In late April, 2015, the National Security Agency (NSA) will release over 52,000 pages of historical material relating to the career of William F. Friedman. On this page you will find a small sampling of those documents.

Considered the dean of American Cryptology, William F. Friedman (1891-1969) was a pioneer in the field as one of the first to apply scientific principles to the making and breaking of codes. His most well-known accomplishment was leading a small team which broke Japan’s “Purple” diplomatic cipher prior to the Pearl Harbor attack, but through his lectures, textbooks, and mentorship Friedman also trained several generations of American cryptologists, thus laying the foundation for the 20th century U.S. signals intelligence community.

NSA's William F. Friedman Collection consists of materials created or collected by Mr. Friedman over the course of his government career and comprising his official working files. The Collection was augmented by documents related to Friedman's work and contributions to cryptology subsequently compiled by NSA historians and archivists. Covering almost 60 years, the records shed light on both the career of this legendary cryptologist and the history of American signals intelligence.

This collection, composed of over 52,000 pages in more than 7,600 documents (along with some sound recordings and photographs), has been preserved in the NSA Archives for its historic significance and value. The bulk of the material dates from 1930-1955 and represents Mr. Friedman's work at the Signals Intelligence Service, the Signal Security Agency, the Armed Forces Security Agency, and NSA.

Please Note: The following historical documents are scanned images of formerly classified carbon paper and letters that have been declassified and saved as PDFs. Due to the age and poor quality of some of the images, a screen reader may not be able to process the images into word documents. In accordance with Sections 504 and 508 of the Rehabilitation Act of 1973, as amended, individuals may request that the government provide auxiliary aids, alternate formats, or services to ensure effective communication of the substance of the documents. For such requests, please contact the Public Affairs Office at 301-688-6524.

1. Certain Aspects of “Magic” In the Cryptological Background of the Various Official Investigations Into the Attack on Pearl Harbor
2. Conversation Between William Friedman and Col. Sadtler on Pearl Harbor
3. Examination - Thesis Submitted by W.F. Friedman; the Duties of the Officer-in-charge of the Signal Intelligence Service, GCHQ
4. Final Report and Papers of the U.K.-U.S. Conference on the Communications Security of the NATO Countries (USCIB 23/65); Agenda Item for USCIB’s 88th Meeting, 10 July 1953
5. Final, Lecture No. 1, Introduction to Cryptology by William F. Friedman; Introductory Remarks and General Introduction of the Subject
6. Friedman TDY Trip to London, Apr-Jun 1943; Diary - Daily Activities
7. Friedman's Contributions In the Fields of Communications Security and Communications Intelligence, 1930-1945
8. Friedman's Diary - TDY Trip to Europe, Oct 1946; Itinerary, Daily Activities
9. Friedman's Original Worksheets of Hebern Solution, 11 Nov 1936
10. Handwritten Notes for Introduction to Cryptology by William F. Friedman, Lecture No. 5
11. Important Contributions to Communications Security, 1939-1945; Summary of Contributions Made by Mr. Friedman
12. Introduction to Cryptology - IV, Draft, Cryptology In the Civil War by William F. Friedman
13. Introduction to Cryptology-VI by William Friedman; Handwritten Draft of Lecture Deals with Cryptology from the End of WWI to End of WWII, No. 6, 1st Draft
14. Japanese Broadcast of Office Chief's Code; Circular #2353 Translation Revised 26 Sept 44
15. Japanese Broadcasts In Office Chief's Code; Circulars # 2353 and #2354
16. Japanese Office Chief's Coded Broadcasts
17. Job Descriptions - Special Assistant to the Director and Cryptologic Research Advisor; Plus Others; Duties and Responsibilities
18. Lecture 2, Final Version, Introduction to Cryptology by William F. Friedman; Historical Information About Cryptology
19. Lecture 3, Introduction to Cryptology, Draft, William F. Friedman; Deals with the Cryptosystems Employed by the British Regulars and the Colonials During the Period of American Revolution
20. Lecture on Code Work Given to the Naval Academy Graduating Class at Annapolis in 1922

21. Mr. Friedman's Appointments, 1954 and 1955; Notebook Listing Daily Appointments

22. Report on Temporary Duty, ETO, by Mr. Friedman; Copy of Orders; Account of Movements and Duty on Trip

23. SCAG Conference, 31 May 1951

A week ago I phoned General Sanford, Director of NSA, to request he give consideration to my being permitted to publish this brochure, minus the classified portions. My reason: the "revisionists" literature, including the books by Adm. Theobald and Adm. Konrad, etc. Sanford said then he was dubious about the advisability of making over the dead embalms, etc., that the Theobald charges were balderdash + not worthy of serious attention. But he said he'd consider my request + would let me know.

[Signature]

[8 May 1957]
they did not think it would be advisable to publish the brochure at all— for the reasons he gave. I told him immediately I accepted his decision without question. He thanked me, I thanked him for asking me.
CERTAIN ASPECTS OF "MAGIC" IN THE CRYPTOLOGICAL BACKGROUND
OF THE VARIOUS OFFICIAL INVESTIGATIONS
INTO THE ATTACK ON PEARL HARBOR

by

William F. Friedman
Certain Aspects of "Magic" in the Cryptological Background of the Various Official Investigations into the Attack on Pearl Harbor

INDEX

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td>1</td>
</tr>
<tr>
<td>2. The Real Essence of the Problem</td>
<td>11</td>
</tr>
<tr>
<td>3. A New Look at the Revisionists Allegations of Conspiracy to Keep Kimmel and Short in the Dark</td>
<td>18</td>
</tr>
<tr>
<td>4. Was MAGIC Withheld from Kimmel and Short and, if so, why?</td>
<td>35</td>
</tr>
<tr>
<td>5. The &quot;Winds Code Messages&quot;</td>
<td>49</td>
</tr>
<tr>
<td>6. The Question of Sabotage</td>
<td>53</td>
</tr>
<tr>
<td>7. Conclusions</td>
<td>65</td>
</tr>
<tr>
<td>8. Epilogue</td>
<td>68</td>
</tr>
</tbody>
</table>

APPENDIX 1: "Pearl Harbor in Perspective," by Dr. Louis Morton, United States Naval Institute Proceedings, Vol. 81, No. 4, April 1955; pp. 461-468

1. INTRODUCTION

More than 15 years have passed since the Japanese, with unparalleled
good luck, good luck that now seems astounding, and with a degree of
skill unanticipated by the United States, executed their surprise attack
on Pearl Harbor during the morning hours of 7 December 1941. It was an
attack that constituted a momentous disaster for the United States; it
made our Navy's Pacific Fleet, for all practical purposes, hors de combat
for many months. In the view of Mark S. Watson, in a volume written for
the Army series on the history of the U. S. Army in World War II, Chief
of Staff: Prevar Plans and Preparations (1950), the disaster was the
result of a "fateful series of mischances" among which he listed those
which he considered the most important. He did not list them all; to
do so would make the disaster partake of the character of an enormous,
and almost incredible Greek tragedy—so many big and little things went
wrong to make the disaster possible and to prevent its being averted with
little or no damage.

The Battle of Pearl Harbor is still being fought but the adversaries
this time are all Americans; and though the battle is bloodless, because
the weapons are now words, not bullets or bombs, it is quite acrimonious
and intense, as internal or civil wars generally are. This time the
battle is intended to capture, by a sort of literary "brainwashing," the
minds of a large segment of the American people who more or less dimly
feel that the truth, the whole truth, has not yet been told. Many
Americans, I am sure, are still undecided in regard to who or what was

1
responsible for this most momentous and most humiliating naval disaster in our history.

Fifteen million words, more or less, have been written concerning, explaining, or attempting to assess and fix responsibilities for the Pearl Harbor disaster, and to show why the U. S. forces at Honolulu were caught napping in the early hours of what President Roosevelt referred to as that "day of infamy" when he appeared before Congress on 8 December 1941 to declare war on Japan. The Report and Hearings Before the Joint Committee on the Investigation of the Pearl Harbor Attack (79th Congress, 2d Session, Government Printing Office, Washington, 1946), hereinafter referred to as PHR, alone contain 15,000 transcript pages; the over-all final report of the Committee comprises some ten million words and fills 40 volumes of closely printed text. Thus far, in addition to this vast amount of material there must be at least five million words in the writings of private individuals. Some of them defend the Findings, Conclusions, and Recommendations of the Majority in the PHR; others defend the Findings and Conclusions of the Minority in the PHR; still others disagree and violently attack both what the Majority and the Minority said. Even representative Keefe, a Republican who signed the Majority Report found it necessary to add to that report some additional views of his own where he could not agree with those of the Majority. It is obvious that in this brochure it will be impossible to deal with all that has been written on the subject. Even to list by title the books, brochures, articles (not to mention the thousands of newspaper accounts, letters to editors, etc.) which have something to add to the
story would be a fairly large task. A bibliography covering the items on Pearl Harbor in my private collection will be found in the "Subject file" now in the NSA Library. But it is a strange, indeed, it is a remarkable fact that not a single new item of information having a direct bearing upon attempts to explain why the Pearl Harbor attack could have come or did come as a complete surprise to the U. S. has been turned up since 1946, when the Joint Congressional Committee completed its task. One may well assume, therefore, that since no new facts have come to light it must be something else that is keeping the Battle of Pearl Harbor going. The assumption is true: the facts developed in the various investigations of 1944, 1945, and 1946 are being scrutinized now through different sorts of spectacles and by different observers; this results in new "interpretations" of the old, well-known facts.

It is the purpose of this brochure to make a few observations and comments on the current Battle of Pearl Harbor. They are directed at the writings of certain historians who call themselves or are known as "revisionists," and who find much support in two recently published books, both by high-ranking officers of the U. S. Navy. These charges are very serious—indeed they are tantamount to imputing at least very questionable behavior by persons of such stature as the late President Franklin D. Roosevelt, the Army's Chief of Staff, General George C. Marshall, and the Navy's Chief of Naval Operations, Admiral Harold R. Stark. The charges are really not new; their antecedents, or nuclei of them or carefully veiled hints at them, can be found in some of the early writings of the more rabid Roosevelt-haters, and even in some parts of the
reports made by various official U. S. investigating bodies appointed to look into the matter during the last phases of World War II or soon after that war had been won.

In another section of this report will be found an attempt to explain the genesis of the suspicions which aroused the Roosevelt haters and which kept them "needling" the President and his Administration for an explanation of how it was possible that the U. S. was taken so completely by surprise when the Japanese attacked Pearl Harbor; to introduce the explanation at this point I think would be confusing. All that can logically be said right here is that the President, his Administration, and the Chiefs of the two military services simply could not afford to permit the true explanation to be broadcast while the war was still in progress.

A very impartial bibliographical survey of the principal items in the literature of the subject has been prepared by a historian of recognized standing, Dr. Louis Morton, Chief of the Pacific Section of the U. S. Army's Office of Military History. His survey, entitled "Pearl Harbor in Perspective," was published in the April 1955 issue of the United States Naval Institute Proceedings (Vol. 81, No. 4, Whole No. 626, pp. 461-488). A copy of Dr. Morton's survey forms Appendix I to this brochure.

A second recapitulation of the Pearl Harbor story and also a source of material which may interest the reader in what the present brochure aims to do is found in an article by Robert H. Ferrell, Assistant Professor of History at Indiana University, published also in 1955, in The Historian, under the title "Pearl Harbor and the Revisionists"
It was perhaps inevitable that after the second World War, as after the war of 1914-18, there should appear in the United States a school of historians questioning the purposes of the war and the motives of the wartime statement. The cost of both world wars, in human lives and in physical resources, was very high; and it was only natural that some individuals should question such expenditure. Yet the new school of "revisionism" appearing after the second World War has undertaken a line of investigation which, if successful, will force the rewriting of an entire era in American history. The revisionists hope to prove that in 1941 President Franklin D. Roosevelt purposely exposed the Pacific Fleet at Pearl Harbor, and goaded the Japanese into attacking it, thus bringing the United States into the war on the side of the Allies. As Professor Harry Elmer Barnes has put the case, in rather plain English, "The net result of revisionist scholarship applied to Pearl Harbor boils down essentially to this: In order to promote Roosevelt's political ambitions and his mendacious foreign policy some three thousand American boys were quite needlessly butchered. \[...\]

Professor Ferrell follows this extract from Professor Barnes with the following words (in a footnote):

"Of course, they were only a drop in the bucket compared to those who were ultimately slain in the war that resulted, which was as needless, in terms of vital American interests, as the surprise attack on Pearl Harbor." H. E. Barnes, ed., Perpetual War for Perpetual Peace (Caldwell, Idaho, 1953), Ch. 20, "Summary and Conclusions," p. 651.

Strong language, isn't it? Very strong, I think, coming from a well-known historian such as Barnes. What substance is there to the strident claims of those professional historians, some of them very well-known and able men, who are the spokesmen for the revisionists? What is it that they wish to prove from their study of the facts concerning the Pearl Harbor disaster? First, they wish to prove that there was no need at all, "in terms of vital American interests," for the U. S. to enter into World
War II as one of the belligerents. Some of them no doubt believe that we fought on the wrong side, with the wrong allies! With this phase of the subject I shall not concern myself in this brochure, since I make no pretence whatsoever of being a historian competent to deal with such an important subject. Next, some of the revisionists claim or believe that they have proof that the disaster at Pearl Harbor was no "accident," that it was brought about deliberately by President Roosevelt. They believe that what they call our "back-door" entry into the conflict was based upon an erroneous view, held by him and his Administration, as to what the U. S. role should be in world affairs; also, they want us to believe that our entry into World War II was for the personal political advantage of President Roosevelt and his followers in the Administration. They contend, in fact, that he goaded the Japanese into making the attack, that he enticed them into doing so by using the U. S. Pacific Fleet as a "lure;" that he knew from the so-called "MAGIC", the Japanese secret communications which Army and Navy cryptanalysts had solved, the exact time the attack would be made and the exact place where they were going to make it; that the President sensed that such an attack was the only thing which would unify American opinion and bring the people of the United States to a pitch of excitement and resentment sufficiently high to lead them to accept with equanimity U. S. entry into World War II on the side of the British and the French, thereby, as Roosevelt felt and as turned out to be the case, assuring the complete defeat of the Axis powers; that President Roosevelt should and could have avoided the disaster at Pearl Harbor but deliberately chose not to do so, for the
reasons cited above; and that he purposely withheld MAGIC intelligence from Admiral Kimmel, Commander-in-Chief of the U. S. Pacific Fleet, and General Short, Commanding General of the Hawaiian Department, the two highest-ranking commanders in Hawaii who should have been but were not given this information and who, therefore, were permitted by him to be deliberately misled as to the real situation, misled to the point, in fact, that when the attack came they were entirely unprepared even to meet it, let alone repulse it. In withholding this information, one of the proponents of this theory, a retired admiral of the regular U. S. Navy, Rear Admiral Robert A. Theobald, implies in his book, The Final Secret of Pearl Harbor (New York: The Devin-Adair Co., 1954), that to make it quite certain that the Japanese attack would be a complete surprise, so far as General Short and Admiral Kimmel were concerned, the President had to have and did have as reluctant partners in his conspiracy, or what was tantamount thereto, General Marshall, the Chief of Staff of the Army, and Admiral Stark, the Chief of Naval Operations, both regular officers of highest integrity and repute. And although Admiral Kimmel in his own book Admiral Kimmel's Story (Chicago: Henry Regnery Co., 1955) does not go quite so far as does Admiral Theobald as to make charges tantamount to conspiracy, he does go quite a long distance along the same route. There is a degree of confusion in regard to this point, however. The following, for example, appears on the inside flap of the dust cover:

Admiral Kimmel sticks to his own end of the story. He tells us about the material he was denied, the warning messages he didn't get. He impugns no motives, he makes no deductions from unproved hypotheses. "Is this a slap at Theobald?" But the book is
sufficient to nail down the inescapable point: the blame for the loss of the Pacific Fleet battleships rests squarely on Washington not on the men at Pearl.

But on the back of the dust jacket, repeated from the last chapter of his book (p. 186), Admiral Kimmel says:

Again and again in my mind I have reviewed the events that preceded the Japanese attack, seeking to determine if I was unjustified in drawing from the orders, directives and information that were forwarded to me the conclusions that I did. The fact that I then thought and now think my conclusions were sound when based upon the information I received, has sustained me during the years that have passed since the first Japanese bomb fell on Pearl Harbor.

When the information available in Washington prior to the attack was finally disclosed to me long after, I was appalled. Nothing in my experience of nearly forty-two years service in the Navy had prepared me for the actions of the highest officials in our government which denied this vital information to the Pearl Harbor commanders.

If those in authority wished to engage in power policies, the least that they should have done was to advise their naval and military commanders what they were endeavoring to accomplish. To utilize the Pacific Fleet and the Army forces at Pearl Harbor as a lure for a Japanese attack without advising the commander-in-chief of the fleet and the commander of the Army base at Hawaii is something I am wholly unable to comprehend.

While I am still able to do so, I feel that I must tell the story so that those who follow may fully realize the imperative necessity of furnishing the naval and military commanders at the front with full and clear information. Only in this way can the future security of our country be preserved.

Dr. Morton in commenting upon Admiral Kimmel's Story says (p. 461):

Admiral Kimmel's case rests upon the allegation that he was deliberately denied information available in Washington. Had he had this information, he says, he would have known the Japanese intended to strike Pearl Harbor and could have adopted measures to meet the attack and minimize the losses. These measures, which he outlines, are of considerable interest, though one wonders to what extent they are guided by hindsight.

Dr. Morton continues as follows: (p. 462)
To support his case, Admiral Kimmel draws on the evidence presented during the investigations of the Pearl Harbor attack. This evidence, he claims was not only obscured at the time but was evaluated to produce a desired result. Inconsistencies in the testimony were ignored, and important questions raised during the hearings left unanswered. He charges bias on the part of investigating officers and a deliberate effort to white-wash the administration and block an impartial search for the truth. "The Congressional investigation," Kimmel declares, "was governed by the majority party, the Democrats. The huge volumes of testimony in that inquiry served to confuse the public mind as to the significance of the facts and to smother testimony damaging to the administration."

Responsibility for Pearl Harbor, Kimmel charges, rests squarely upon the shoulders of his superiors in Washington and ultimately on the Commander-in-Chief, President Roosevelt. "Until this day," he writes, "I have kept silence on the subject of Pearl Harbor ... Now, however, I deem it my duty to speak out. What took place in Washington must be so clearly placed on the public record that no group of persons in administrative power will ever dare again to invite another Pearl Harbor and place the blame on the officers in the fleet and in the field."

The charges that Admiral Kimmel makes are not new and were being circulated even before the end of the war. The Japanese attack on December 7 had unified the country and ended temporarily the debate between the "Isolationists" and the "Interventionists" which had marked the prewar years. All classes and parties closed ranks for the duration of the struggle. But even during the war, there had been a recognition of the political implications involved in the question of responsibility for Pearl Harbor, and the administration had taken steps to preserve the record. Six investigations had been conducted even while the conflict raged, all but one of them by the Army and Navy. As a result, a large volume of testimony and documents that might otherwise have been lost was assembled. But the requirements of wartime security and a unified national effort made public debate impossible.

The war over, partisan differences reappeared, and critics of President Roosevelt began to challenge openly the views so widely held during the war years. The cooling of passions and disillusion with the postwar world raised further questions about American participation in the war. Historians and publicists, as they have done after every war, sought to reassess the causes of the war and to place Roosevelt's policy in the larger perspective of American history. Thus, in the years following the end of the conflict, a new interpretation of the events that had preceded the war and of the conduct of the war itself emerged.
The foregoing final paragraph of the extract from Dr. Morton's article brings us directly to the principal revisionist contention which will be examined in the present brochure. The contention, as noted above, was first stated in 1945 by John T. Flynn, one of the early and most vitriolic revilers of President Roosevelt, in a pamphlet entitled The Final Secret of Pearl Harbor, in which he revealed the fact that U. S. cryptanalysts had solved the Japanese diplomatic codes and ciphers before the Pearl Harbor attack. His contention was that the intelligence derived or derivable from the solved and translated messages, the so-called MAGIC, told exactly where and when the Japanese were going to strike; that this priceless information Roosevelt deliberately kept from Admiral Kimmel and General Short, with the result that the Japanese were able to make their attack with complete surprise; and that the loss of men and ships that resulted therefrom, however unfortunate it was for the U. S. and a few American families, unified the country. That, claims Flynn, was Roosevelt's aim. At any rate, as Dr. Morton indicates, the Japanese attack on Pearl Harbor ended the debate between the "isolationists" and the "interventionists."
2. THE REAL ESSENCE OF THE PROBLEM

Distilled down to its essence, therefore, the first question is: Did MAGIC really contain clear and unequivocal indications as to exactly where and when we would be hit by the Japanese in the war which Roosevelt knew, or was expecting, or at least felt was in the offing?

Much has been written on this basic question; hundreds of thousands—not millions of words, in fact—have been published on the question in an attempt to answer it either affirmatively or negatively. If some Americans now scoff at the whole business and say that all that could be said on the point was said years ago—why not stop flogging a dead horse?—let them note that in as staid and unsensational a newspaper as The Wall Street Journal there appeared a long review of Admiral Kimmel's Story in the issue for 14 January 1955, accompanied by a lengthy editorial entitled "Pearl Harbor" in the same issue; let them note, too, another lengthy editorial entitled "Myth of the broken code" in the issue of the same newspaper for 21 January 1955; let them read also the baker's dozen "Letters to the Editor" in the issues for 21 January, 31 January, 4 February, and 6 February 1955, all commenting upon the two editorials and the book review mentioned above. The question therefore can by no means be said to be "dead and buried;" in fact, even to this day references to the "MAGIC" that was available and was not used at the time of Pearl Harbor keep popping up in the daily newspapers, in periodicals, and in books.

For instance, there are two "Letters to the Editor" in the Washington Post on Pearl Harbor as recently as 31 December 1956 and 4 January 1957. And
as I write this brochure word has just come that the Chicago Tribune is about to publish another (revisionist, no doubt) article on the subject.

Let me therefore repeat the question: Did MAGIC really contain clear and unequivocal indications as to exactly where and when we would be hit by the Japanese in the war which Washington knew, or was expecting, or at least felt was probably soon to come?

In this brochure I shall attempt to dispose of this basic question in a rather simple and, in my opinion, a definitive manner by attacking it in what may seem to be a round-about way. But just before getting right down to it I will place before the reader a short extract from a book published late in 1956 by a recently-deceased and a highly-respected (by certain Americans who knew him) Japanese whose words were such— he died in prison—as to indicate that he had no particular reason for hiding the truth. I refer here to the book written by Shigenori Togo, the man who was Japanese Minister of Foreign Affairs at the time of the attack on Pearl Harbor and across whose desk there certainly must have passed the most important of the messages to and from the Foreign Office and Japanese ambassadors, ministers, and consuls abroad.¹

It is to be noted, and indeed emphasized, before going into this phase of the subject, that at the time of the attack the only cryptographic systems which the U. S. cryptanalytic agencies had solved and were able to read were not the Japanese military or naval systems; they were only the systems used by the Foreign Office. Whatever intelligence the U. S. authorities were able to obtain from MAGIC therefore must have been and

was clearly derived from Japanese diplomatic communications. With this fact in mind let us take a look at an item of much interest in Togo's book (pp. 118-119 and 197):

It is not difficult to conceive the extent of the tyranny of the military power from the fact that on the eve of the Pacific War such a fundamental datum as the total tonnage of Japanese naval vessels—not to speak of the displacement of the gigantic battleships Yamato and Musashi, or the plan to attack Pearl Harbor—was vigilantly withheld from the knowledge of the civilian cabinet ministers. General Togo even told me in Sugamo Prison that it was only at the IMFFE that he had first learned that the Japanese task force which carried out the attack on Pearl Harbor had assembled at Hitokappu Bay on 10 November, and weighed anchor for Hawaii on the morning of the 26th! The high command did not divulge its secrets even to the full general who was Premier and Minister of War; it is easy to conceive how other ministers were treated.

The war decision was thus made, and various problems which would arise with the opening of the war were submitted to meetings of the Liaison Conference. One thing which—needless to say—was not discussed in the Liaison Conference was operational aspects of the impending hostilities. It was disclosed at the IMFFE that the naval task force under Admiral Nagumo had sailed from Hitokappu Bay on 26 November under orders to strike Pearl Harbor, and in its judgment the tribunal made the absurd finding that the scheduled attack was freely discussed at the meeting of the Liaison Conference on 30 November. We had, of course, no knowledge of the plan; it was the invariable practice of the high command not to divulge to civilian officials, such as us, any scrap of information bearing on these highly secret operations, and anyone familiar with the system will readily understand our total lack of knowledge of them. (This condition is sufficiently well illustrated by the fact, which I have mentioned elsewhere, that Tojo told me that it was only at the IMFFE trial itself that he first learned any operational details of the Pearl Harbor attack; a mass of additional evidence was adduced at the trial showing that the civilian members of the Cabinet had no prior knowledge even of the existence of the plan to attack Hawaii.)

It is a fair and logical deduction to conclude that if Togo was telling the truth, i.e., that the civilian members of the Japanese Cabinet, including Prime Minister Tojo and the Foreign Minister himself, had no
prior knowledge of the plan, including of course the exact date on which
the Pearl Harbor attack was to take place (as set by the Japanese high
command) then the MAGIC messages themselves in the communications from
and to the Foreign Office could not possibly have contained any definite
information, let alone a clear-cut statement, on this very important
point. And if the MAGIC messages did not contain this information or
statement how could President Roosevelt or any members of his immediate
official family, or the heads of U. S. Army and U. S. Navy intelligence
staffs know from the MAGIC messages exactly where and when the attack
was coming? But this question does arise: did Togo tell the truth in
his book? If he did, how are we to explain certain of the MAGIC messages
the records of PHR contain?

After re-reading the hundreds of MAGIC messages that were exchanged
between the Foreign Ministry and its offices abroad in the year 1941 it
seems fantastic, it strains our credulity, to believe that Togo did not
know what was being planned. To mention only one set of messages, the
"dead line" messages—after which "things are automatically going to
happen"—how could Togo not know what was being planned? How are we to
explain them, if he didn't know that the U. S. was going to be attacked?
But let it be remembered that we are now re-reading the messages from the
vantage point of hindsight. There is not a single message that can be
said to contain categorical evidence proving that Minister Togo must have
known that Pearl Harbor was to be the target. In 1946, and even now
when we re-read those messages in Part 12 of the PHR, I realize that it
is fantastic that somebody in U. S. Intelligence did not or could not
see that the blow was being prepared against Pearl Harbor. But if we
believe Togo was an honorable man and was telling the truth, then we must conclude that he and his closest associates in the Foreign Office were no better at intelligence than our own intelligence authorities! They knew or only guessed that something was going to happen after 29 November 1941, but they didn't know exactly where or when! Or shall we assume that somebody in the Japanese Foreign Office, some subordinate of Togo, the Foreign Minister, was "in on the secret"—and it was he that took care of all the messages that pointed to Pearl Harbor? Could be! Could easily be! How many messages going out of any one of our own large executive departments and signed by the Secretary thereof are actually seen by the Secretary? But I do not wish to belabor the point. Let us merely say that it is quite possible that Togo saw none of the crucial messages or, what is more probable, that he saw them but, not being "in on the secrets" of the Japanese high command, did not draw the correct deductions—that the U. S. was to be attacked, without warning, at Pearl Harbor in the early hours of 7 December 1941, and that the object of the attack was to destroy the U. S. Pacific Fleet if possible. But let us also remember that reading the MAGIC messages in 1946 or in 1956 is analogous to reading the final chapter of a detective tale—before the preceding chapters, with their false and purposely misleading clues injected by the author to evoke the reader's interest. In reading such a detective story in the normal manner the final chapter often makes the reader feel inferior, even silly, that he could not see the truth, the real elements of the mystery right from the beginning. The Japanese were getting intelligence reports—call them if you will, "ordinary spy reports" from several U. S. military bases
besides Hawaii, such as the Philippines, Panama Canal, Seattle, and San Francisco. It is true that Japanese interest in Pearl Harbor seemed to be and actually was much greater than at any other base; but one could also say that this greater interest stemmed from a perhaps justifiable fear by the Japanese that the U. S. Pacific Fleet might sortie some dark night and strike the first blow at Japan. They, as well as the U. S., did not want to be taken by surprise! Perhaps an intelligence specialist with the proper kind of imagination might have hit upon the real reason for the greater Japanese interest in Pearl Harbor, but who can be certain of this? All that can safely be said in regard to the Togo statement is this: Both he and Prime Minister Tojo may have been told, or they may have guessed, that Japan was going to strike—but not exactly where and when. These two very important elements the Japanese high command kept to itself even after the task force left Japanese waters. And for those revisionists who think the U. S. note of 27 November 1941 was an ultimatum and that it was that note which triggered off the attack on Pearl, let them ruminate on the fact that the Japanese task force which attacked Pearl left Japanese waters the day before that note was sent off by Secretary of State Hull. His note may have constituted an ultimatum—but it did not bring on the attack. The attack was planned very carefully, months before that, and, to repeat, was already launched to the point of having departed from Japanese waters.

But there is another revisionist prop, and a very important one, I must emphasize, which I wish to undermine, for it should be greatly weakened when consideration is given to another argument which is so obvious
and simple that it has been a source of astonishment to me that the revisionists themselves have not thought of it. (Parenthetically I want to preface the argument by saying that any hesitancy I might have in stating it melts away when I find that several very able naval historians with whom I have discussed it expressed astonishment that it had not hitherto been mentioned. One of them said of it in a recent personal letter: "In retrospect I realize that some of the ideas you mentioned about the events leading up to the attack on Pearl Harbor (like Columbus' egg trick!) are startling in their simplicity and obviousness—which is probably why no one has heretofore recognized their importance." My contention, I think, warrants taking a new look at a certain phase of the Pearl Harbor mystery—if indeed there is any mystery about the factors entering into our being taken by surprise.
3. A NEW LOOK AT THE REVISIONISTS ALLEGATIONS OF CONSPIRACY TO KEEP KIMMEL AND SHORT IN THE DARK

The revisionists' argument, which I hesitate to repeat (since it has already been stated in this brochure; but its repetition may make what I have to say crystal clear) runs as follows: President Roosevelt desperately needed a good reason for justifying America's entry into World War II. He needed it in order to save the British from utter defeat by Germany; France was already down and out! Britain was next on Hitler's list—and then the United States. (The revisionists deny this most vehemently, but everything that Hitler had done thus far was strictly in accordance with the plans he outlined in Mein Kempf. In this connection, and as I write this, there has just come out a book which must be regarded as authoritative and which is called The German Weapons and Secret Weapons of World War II, by Rudolf Lusar. Lusar was head of the Technical Arms Department of the Wehrmacht. He discloses that Germany was also building the Heinkel 314, a bomber capable of reaching the United States and returning without refuelling. Several of the planes were ready at the end of the war. The book also says that it was originally planned to stage the first air raid on the United States in May 1945. So much for the revisionist contention that the benign Herr Hitler had no designs whatsoever on the United States; for it is very clear that he planned to bomb this country just as soon as he had finished off England.) The President wanted to get the U. S. into the conflict not only to save Britain but, ultimately, also to save the U. S. Timely action was needed. He had goaded Hitler by several unneutral acts in the Atlantic, as well as in establishing certain U. S.
logistical relations with Britain ("lend-lease," the transfer of 50 U. S. destroyers, etc.); but Hitler was too clever to be pushed to the point where Germany would have to declare war on America prematurely or where German action would justify an American declaration of war on Germany before Germany was ready for such action. Hitler realized, as well as President Roosevelt, that what American did held the answer to Germany's problem. President Roosevelt knew that the America people were not at all anxious to be drawn into the European war; but he felt that it was absolutely necessary that something be "engineered," so to speak, in order that the U. S. would, willy-nilly, be drawn into the conflict. This, the revisionists contend, as I have reiterated, Roosevelt felt was necessary to save England; it was incidentally also intended, they contend, to divert attention from the failure of the New Deal to bolster the badly sagging economy as a result of defective monetary policies and other internal difficulties. U. S. participation was also a Democratic objective, they say, for Roosevelt's reelection; and, of course, it was desirable to preserve the Rooseveltian prestige. The long-drawn out arguments with the Japanese might, in view of the Tri-partite pact of the German, Italian, and Japanese Axis, and despite Hitler's canny strategy of not succumbing to American provocation in the Atlantic, serve his purpose. Americans did not like the Japanese anyhow and were distrustful of these Orientals. Japanese ambitions in the Far East and distrust of the Japanese kept popping up everywhere in the American press and public opinion. But Roosevelt felt that there was one sine qua non to getting into a shooting war with the Japanese. In the words of Mr. Stimson, his
Secretary of War, unfortunate words one must now admit, it was all a matter of how the Japanese "could be maneuvered into the position of firing the first shot," otherwise the American people would be lukewarm about a war with them. MAGIC, that is, the secret intelligence which the solution of the Japanese diplomatic communications made available to the Roosevelt Administration in great abundance, provided a golden opportunity—so the revisionists, including Admiral Theobald, fervently believe. I have already and more than once stated in this brochure that the revisionists are convinced that MAGIC told the President exactly when and where their attack was going to be launched: in the early hours of the morning of 7 December 1941, at Pearl Harbor. By withholding from the U.S. commanders at Pearl Harbor this private knowledge which President Roosevelt gained from MAGIC—the horse's mouth, so to speak—enabled the President to accomplish his heart's desire. With this highly secret information he could maneuver the Japanese so that they would fire the first shot; he realized, they concede, that there would be some losses of men and ships, of course, as so callously stated in the extract from Professor Barnes which was quoted above, but these losses, they contend, he would regard as justified in the long run by saving England, France, and, later on, America from the Axis Powers—and it would incidentally save his own prestige and insure his reelection.

The important element in the foregoing argument, let it be noted, is that, to quote from Secretary Stimson's diary a bit, Japan was to be "maneuvered into a position of firing the first shot." The maneuver, according to the revisionists, included using the ships of the U.S.
Pacific Fleet as a lure; that is why, they argue, Roosevelt insisted on having that fleet based on Pearl Harbor instead of on the west coast of the U. S., as Admiral Richardson, Kimmel's predecessor, wished. But let be noted that Admiral Richardson's objections stemmed from purely logistical considerations, such as easier maintenance and repair; and morale of the sailors entered into the picture—Hawaii was a long way from "home" for the men and officers of the fleet. (Admiral Richardson had not the slightest idea that keeping the fleet at Pearl would deter the Japanese from doing what they wished to do in the Far East. In fact, he thought keeping the fleet on the West Coast would be more effective. Well, the President, the Commander-in-Chief, didn't agree with Admiral Richardson—and that's all there was to it. It turned out, unfortunately, that Admiral Richardson's view was more nearly correct than the President's—but does that mean that the President had ulterior motives in keeping the fleet at Pearl? I don't think so at all.)

And now for my counter argument on this score.

If we assume for the moment that the revisionists' argument is valid, why don't they go just one step further? If all that President Roosevelt thought necessary for his purposes, if all that he was seeking, was "to maneuver the Japanese into firing the first shot," and if MAGIC contained all that the revisionists claim it contained, would it not have been possible, by means of that very MAGIC to accomplish his purpose without such a terrible loss of American lives and, without loss of any of the ships that constituted the apple of the President's eye, the Navy's big battleships? If Roosevelt was so clever a politician and so machiavellian
in his strategy as to think up a way of maneuvering the Japanese into a
different position wherein they would be enticed or maneuvered into firing the first
shot, should one doubt that he lacked the intelligence to have gone one
step further in his thinking and saying something like the following to
himself: 'Eureka! I've got it. MAGIC will provide the golden opportuni-
ty I've sought for so many months. I've hit upon a perfectly marvelous
idea and opportunity! An absolutely and amazingly wonderful opportunity!
The Japanese have to come to Pearl Harbor to make their surprise attack,
an attack clearly indicated by these MAGIC messages. They have to travel
several thousand miles, in fact, to get to Hawaii from Japanese waters.
If we caught them red-handed, so to speak, near Hawaii and preferably
just before the attack, nobody could possibly claim they were on a simple,
harmless reconnaissance mission—or on maneuvers. Why, with Japanese-
American relations so tense, even if they were caught as many as 500 miles
from Pearl Harbor every unbiased critic would say that they really fired
first! So I'll bring Kimmel and Short fully into the picture—I'll tell
them the story MAGIC is telling us. I'll secretly order them here right
away (November 26th, for example) and I'll have Marshall and Stark come
in. I'll show Kimmel and Short the crucial messages. Then I'll tell
them something like this: Look, my boys, you see now, don't you, what
your're in an excellent position to do to the Nips? You see, don't you
that this inside and absolutely authentic information says that they are
coming from Japan to attack Pearl Harbor by surprise at seven o'clock on
the morning of 7 December; they're coming with a task force which will
certainly be a pretty big one, you may be sure. It will comprise several
aircraft carriers; they'll have maybe as many as 350 aircraft, including
dive bombers, etc., of course. Now as Commander-in-Chief, I direct you
to do everything that will be necessary to meet them when or preferably
just before they arrive to launch their attack. I direct you to destroy
them; knock out the whole task force, carriers, planes, and all, just
before they reach Oahu if you can. I direct you, Kimmel, to get all your
battleships and, of course, your carriers out of their berthing positions
at Pearl Harbor some time during the night, so that there won't be any
ships there for them to bomb. And I want all your planes, including
those on your carriers, the Lexington and the Enterprise, up in the air
before seven o'clock; you'd better get off messages at once to Halsey,
Newton, and Brown to alert their task forces; if they're not at Pearl get
them back as soon as you can; maybe you'll want to get the Saratoga back
from the West Coast to join your other carriers if there's still time,
and that's OK with me. Short, I want all your anti-aircraft batteries on
shore to be fully manned and with live ammunition at hand, ready for use;
I know you don't have too much in the way of fighter and bomber planes but
I want you to wipe out as many of their aircraft as possible with what you
have. Forget that screwy message you sent about being prepared for
sabotage—in view of these messages that's an absurd notion. You can see
that the Japs are after our fleet and the protection of the fleet while
at Pearl is your job, you know. Be sure your radar is working properly—
24 hours a day. I want you, Kimmel, to get your carriers and battlewagons
out where they can destroy the Japanese carriers and escort ships while
their aircraft are being shot down just before they reach Pearl. This,
my lads, if done well will go down in history as the most thrilling and
important battle of all time. Even much more important is the fact that
if you knock off their task force and assuming we'll have minimal losses
we'll come out far ahead in naval strength because right now our Pacific
Fleet is no match for the Japanese Combined Fleet—they've got more
ships, faster ships, and with longer-range guns than we have, I'm sorry
to say. Now I don't want you to tell anybody I've alerted you because of
what MAGIC is telling us. We're reading their most secret diplomatic
codes and ciphers, which are all that count now anyhow right now, and it's
very important that they don't get suspicious about the security of their
Foreign Office communications. I want them to continue using those
cryptographic systems because the information we're getting out of them
now is priceless and will be even more so in the war which will without
question ensue when you've destroyed their task force for Pearl. They
won't get suspicious if you will act exactly as though your operations
and maneuvers are a routine matter—training—but I want you to be on
Alert No. 1. Don't forget that on 17 June 1940, when we thought the Japs
and the Germans were about to gang up on us, we sent messages directing
our commanders to put our forces at Pearl on a full alert, and you did
so; that time, fortunately, nothing happened. We were probably jumping
at conclusions then, but now it's different—now we've got this MAGIC.
You'll have to go at this carefully, of course, so as not to alarm the
Japs and lead them into calling the whole thing off, which they still can
do, as we understand their plan. But the important thing is to keep from
doing anything that will alarm them and make them call the whole thing off.
I want them to fire the first shot. I'm sure you can think up ways to work up to a condition of full alert so that they'll not get suspicious. That might precipitate an "incident" and give the Japs an excuse to say that we committed the first overt act. Besides we don't want to alarm the civil population, of course. Everybody knows that relations between Japan and ourselves are very tense right now, so that exercises and maneuvers of a defensive type will certainly be regarded as only logical and the natural thing to do. Now I suggest that you get back to your posts as fast as you can—you've got only a few days to prepare a real surprise for the surprise they think they're going to spring on us.

Let's see how well you can knock 'em off. Give 'em hell! So long, and the best of luck to you. About 150 million Americans will probably never know how much they will owe you two for what I'm sure you'll be able to do, even with what little you have. I wish you had more—but you know what the trouble is. I don't have to tell you. It's enough merely to remind you that the Selective Service Act was extended in the House just a few months ago by a majority of just one vote."

On 3 December the President (in this imaginative account) sends a message to Kimmel and Short telling them that we've deciphered a long message from the Japanese Consul, Kita, in Honolulu to Tokyo. "Kita is the Jap whose been giving them the dope about ships in harbor; he's the one whose been sending Tokyo the detailed story of what ships are anchored where. But from this 3 December message it's clear that somehow Kita has figured out, or maybe somebody in Tokyo has figured out, that it would be a terrible denouement to come all the way from Japan to make their surprise
attack only to find that the "birds had flown the coop." So Kita has figured out a plan whereby he and his spies in and around Pearl can send last word to the Japanese Attack Force Commander that everything is OK, that the important elements of the U. S. Fleet are still in their berthing positions, and haven't suddenly departed just a few hours before the attack is scheduled to commence." (See Message from Kita to Tokyo, 3 December 1941, p. 267 of Part 12, PHR, a message which by the way was not processed until 31 December 1941 but which if there really was a conspiracy would certainly have been done before 7 December.) "Kita doesn't even have the slightest inkling, of course, that I'm telling you, Kimmel and Short, about the set-up he has prepared to make sure to get word to the Japanese task force that the birds haven't flown the coop. You arrange with Naval Intelligence, Army Intelligence and the FBI at Honolulu to grab Kita and Kita's spies on Saturday and hold them in cold storage until after the planned for attack has come off—and has, of course, failed, because it will fail, if you've done your part."

If any reader of this brochure thinks that the foregoing fanciful, imaginative, or conjectural account of what might have happened is too bizarre for serious consideration let me call his attention to what Admiral Kimmel says he could and would have done—if only he'd been "let in on" MAGIC, or at least had been told what was in those messages. Let me quote from his book (pp. 87-88):

No one had a more direct and immediate interest in the security of the fleet in Pearl Harbor than its commander-in-chief. No one had a greater right than I to know that Japan had carved up Pearl Harbor into sub-areas and was seeking and receiving reports as to the precise berthings in that harbor
of the ships of the fleet. I had been sent Mr. Grew's report earlier in the year with positive advice from the Navy Department that no credence was to be placed in the rumored Japanese plans for an attack on Pearl Harbor. I was told then, that no Japanese move against Pearl Harbor appeared "imminent or planned for in the foreseeable future." Certainly I was entitled to know when information in the Navy Department completely altered the information and advice previously given to me. Surely, I was entitled to know of the intercepted dispatches between Tokyo and Honolulu on and after September 24th, 1941, which indicated that a Japanese move against Pearl Harbor was planned in Tokyo.

Knowledge of these intercepted Japanese dispatches would have radically changed the estimate of the situation made by me and my staff. It would have suggested a re-orientation of our planned operations at the outset of hostilities. The war plans of the Navy Department and of the Pacific Fleet, as well as our directives and information from Washington prior to the attack, indicated that the Pacific Fleet could be most effectively employed against Japan through diversionary raids on the Marshalls when the Japanese struck at the Malay Barrier. Knowledge of a probable Japanese attack on Pearl Harbor would have afforded an opportunity to ambush the Japanese striking force as it ventured to Hawaii. It would have suggested the wisdom of concentrating our resources to that end, rather than conserving them for the Marshall Islands expedition.

Admiral Kimmel cites instance after instance, message after message, which contained information which, he says, would have been of vital importance to him and would have prevented the disaster if only he had been given the information which he should have received as Commander-in-Chief of the U. S. Pacific Fleet. Maybe, maybe he's right in his contention. His proximity to the scene might have led him to make the imaginative jump that was necessary in order to reach the correct solution to the astounding story that MAGIC was unfolding.

Imagination boggs down when one considers what such a picture as I have conjured up might have been painted from what the Japanese messages were saying—or what the revisionists claim they clearly said.
It is true that in Hawaii there were fewer fighting aircraft, both Army and Navy, than were released from the Japanese carriers when the attack was launched. But the aircraft on the U. S. Navy carriers Lexington and Enterprise, had these carriers been positioned on the basis of the information the revisionists claim President Roosevelt had, would have made up for the lack of aircraft on Hawaii at the time of the attack.

In Admiral Kimmel's story the Admiral makes a few comments on the question of whether his account represents action that he might have taken. But let it be remembered that what he says is based on hindsight; and the Admiral freely admits this point. He contends that had he had the benefit of the intelligence which was in the MAGIC messages and which he never received the story would have been very different (pp. 109-111):

The question will arise in your minds, as it has in mine: Would the receipt of this information have made a difference in the events of December 7? No man can now state as a fact that he would have taken a certain course of action years ago had he known facts which were then unknown to him. All he can give is his present conviction, divorcing himself from hindsight as far as humanly possible, and re-creating the atmosphere of the past and the factors which then influenced him. I give you my views, formed in this manner.

Had I learned these vital facts and the "ships in harbor" messages on November 28th, it is my present conviction that I would have rejected the Navy Department's suggestion to send carriers to Wake and Midway. I would have ordered the third carrier, the "Saratoga," back from the West Coast. I would have gone to sea with the fleet and endeavored to keep it in an intercepting position at sea. This would have permitted the disposal of the striking power of the fleet to meet an attack in the Hawaiian area. The requirements of keeping the fleet fueled, however, would have made necessary the presence in Pearl Harbor from time to time of detachments of various units of the main body of the fleet.

On December 4, ample time remained for the Navy Department to forward to me the information which I have outlined,
and in addition the following significant facts, which the Navy Department learned between November 27 and that date:

1) Japan had informed Hitler that war with the Anglo-Saxon powers would break out sooner than anyone dreamed;

2) Japan had broadcast her winds code signal using the words "east wind rain," meaning war or a rupture of diplomatic relations with the United States.

Assuming that for the first time on December 5 I had all the important information then available in the Navy Department, it is my present conviction that I would have gone to sea with the fleet, including the carrier "Lexington" and arranged a rendezvous at sea with Halsey's carrier force, and been in a good position to intercept the Japanese attack.

At some time prior to December 6, 1941, the commanders of Hawaii could have been informed of the promise of armed support as detailed by the War Department in London to Air Marshal Brooke-Popham in Singapore. This vital information was denied to them.

On December 5, fifteen hours before the attack, ample time still remained for the Navy Department to give me all the significant facts which I have outlined and which were not available to me in Hawaii. In addition, the Navy Department could then have advised me that thirteen parts of the Japanese reply to the American proposals had been received, that the tone and temper of this message indicated a break in diplomatic relations or war with the United States, and that the Japanese reply was to be formally presented to this government at a special hour soon to be fixed. Had I received this information on the afternoon of December 5, it is my present conviction that I would have ordered all fleet units in Pearl Harbor to sea, arranged a rendezvous with Halsey's task force returning from Wake, and been ready to intercept the Japanese force by the time fixed for the outbreak of war.

Even on the morning of December 7, four or five hours before the attack, had the Navy Department for the first time seen fit to send me all this significant information, and the additional fact that 1:00 P.M., Washington time, had been fixed for the delivery of the Japanese ultimatum to the United States, my light forces could have moved out of Pearl Harbor, all ships in the harbor would have been at general quarters, and all resources of the fleet in instant readiness to repel an attack.

For some years I, too, have wondered to what extent Kimmel's statements as to what we could or might have done, had he had or had he been given the information in MAGIC, are guided by hindsight. But having
read his book carefully I feel that it is quite possible that he is
warranted in making his statements. The defense of Pearl Harbor was not
his responsibility, of course—it was General Short's. But between
Kimmel and Short, both capable officers, their closeness to the situation
and the greater amount of time they had to think about their duties and
responsibilities with respect to safeguarding the Pacific Fleet might
have led them to a safe conclusion: that they had better take all precau-
tions to avoid a sudden attack on Pearl Harbor.

One further comment: if, as a result of the inside information the
revisionists say we got from MAGIC, all the submarines, destroyers,
carriers and battleships in a large task force of the U. S. Pacific Fleet,
or even the whole of the fleet had been lying in wait for the Japanese
task force sent to make the attack on Pearl Harbor there would have been
strength enough, I think, to wipe out the whole Japanese task force. It
is true that the Japanese task force included only two battleships, but
it had six carriers, two heavy cruisers, a light cruiser, eleven destroyers
and a number of submarines, about five, some of which carried midget sub-
marines. (Capt. Harley Cope, USN in "Climb Mount Mitaka," U. S. Naval
Institute Proceedings, Vol. 72, No. 12, December 1946.) I say this on
the assumption that Admiral Kimmel would have timed his counter-move so
that the Japanese task force would not have had the protection of the
aircraft of its carriers, because if Kimmel and Short had operated on the
basis of information the revisionists claim was clearly in MAGIC the
Japanese 361 planes would already have departed on their mission. This
I regard as a point of considerable importance. There is reason to
believe that had only a task force of the U. S. Pacific Fleet gone out to engage the Japanese task force in battle on the high seas, the U. S. task force would probably have fared very badly because of the fact that the Japanese not only did have six carriers to our two but also their battleships were faster and had longer range guns. Also, if even the whole U. S. Pacific Fleet had gone out, on the basis of MAGIC—as MAGIC is conceived by the "revisionists"—to meet the Japanese task force which was to attack Pearl Harbor, and had the two navies met on the high seas, with the Japanese carriers still sailing with their entire complement of airplanes, the U. S. Pacific Fleet would probably have suffered a terrible, humiliating and ignominious defeat, because the Japanese task force because of what I have already said—they had six carriers to our two, their first-line battleships were speedier and had longer-range guns than any of our own battleships had. Not only would there have been a great loss of American lives, but also none of our battleships or carriers could have been raised and repaired. As it was, and quite fortuitously, there were no carriers at Pearl on 7 December; and with one exception the battleships damaged or sunk at Pearl Harbor were soon back in commission, thanks to an obvious strategic error made by the Japanese high command—they could have but they failed to destroy the dry docks, machine shops, and the repair facilities at Pearl! Why the Japanese overlooked this rather obvious point is not too clear; it shows them to be not too good as naval strategists. Only one Japanese naval officer has thus far tried to explain this strategic error. They, or at least Admiral Yamamoto had the imagination to realize that with the U. S. Fleet in being in the Pacific
their plans for conquest could not be carried to completion very easily; therefore it was necessary to destroy the U. S. Fleet. Dr. Louis Morton in his article "The Japanese decision for war" (U. S. Naval Institute Proceedings, Vol. 80, No. 12, December 1954, p. 1329) says:

Against the almost unanimous opposition of the naval planners, Admiral Yamamoto remained adamant. Unless the American Fleet could be destroyed at one blow at the start of the war, he insisted, the Japanese would probably fail in their effort to seize the Netherland Indies and Malaya. And even if they were successful, he predicted that they would be unable to hold any of their gains for long. ... A determined effort by the Pacific Fleet might well result in disaster. ... The Japanese believed it necessary to destroy or neutralize the American Fleet at Pearl Harbor and to deprive the United States of its base in the Philippines.* America's line of communications across the Pacific was to be cut by the seizure of Wake and Guam.

But that was as far as imagination of Japanese Navy strategists carried them: the only thing they thought necessary was to destroy the U. S. Pacific Fleet. On the other hand, although the U. S. war plans elaborated in the first half of 1941 (in May of that year) took into account the possibility that the Japanese might, (as they had three times before and successfully) begin a war on an enemy without a preceding declaration of war, that is, by a surprise attack, and although this possibility was placed first on the list of contingencies, with Pearl Harbor as the focal point of the attack, and although the war plans even envisioned that such an attack could come from aircraft flown from carriers, it is an almost inexplicable fact that all this was simply forgotten by the end of the same year. The U. S. high command in Washington certainly forgot this

* Some American naval historians and strategists disagree with Dr. Horton on this point; they insist that the Japanese Navy needed a spectacular victory—the Army was getting too much publicity, and that is why Yamamoto insisted on the Pearl Harbor attack. It was not necessary for their plans to take all that could be taken in Southeast Asia.
contingency; and the two principal commanders in Hawaii, by December 1941, also apparently forgot it—or did they lack the imagination that the January to May 1941 war planners used in thinking up the things that the Japanese might do? In Washington they were thinking only of deterrents to Japanese expansion in the Far East. They imagined that as long as the U. S. Pacific Fleet remained intact in the Pacific it would serve as a deterrent to Japanese moves toward conquest in Southeast Asia. The Japanese attack Pearl Harbor, our greatest overseas bastion? How absurd! Washington, by December 1941, just simply could not imagine that the Japanese would be foolhardy enough to attack Pearl Harbor and try to destroy the ships of Pacific Fleet in their berthing positions in that harbor. Except here and there among the junior officers of the Navy the possibility of a surprise air attack on the Fleet was kept in mind. "A group of the younger officers (on the West Virginia) . . . anticipating an air attack on the Fleet, had discussed among themselves what to do in case it came, and knew exactly how to act." (Morison, S. E. The rising sun in the Pacific, Vol. III of History of United States Naval Operations in World War II, Little Brown and Co., Boston, 1953, p. 103). Their foresight, says Prof. Morison, saved the West Virginia. To repeat, it is true that this contingency about which I have already said a good deal, was explicitly stated in war plans—but apparently nobody seriously believed that it could be done, or that the Japanese would be so foolish as to try it. Indeed, Prof. Morison says of the attack on Pearl Harbor: (P. 132)
Thus, the surprise attack on Pearl Harbor, far from being a "strategic necessity," as the Japanese claimed even after the war, was a strategic imbecility. One can search military history in vain for an operation more fatal to the aggressor. On the tactical level, the Pearl Harbor attack was wrongly concentrated on ships rather than permanent installations and oil tanks. On the strategic level it was idiotic. On the high political level it was disastrous.
4. WAS MAGIC WITHHELD FROM KIMMEL AND SHORT AND, IF SO, WHY?

We come not to another very important question which has been raised in revisionist circles: Why did not the commanders at Pearl Harbor get MAGIC; why did they not have the machines and facilities for deciphering the Japanese highest level diplomatic communications, the so-called "Purple" crypto-system? Prof. Ferrell says: "The British and General MacArthur received the Purple decoding machines from Washington; why not the commanders at Pearl Harbor? (p. 225) This is a good question, and not as foolish as it might be made to appear by the usual answer that the authorities in Washington couldn't prevent the Pearl Harbor attack, even with the code, so what would Kimmel and his Army opposite at Hawaii, Lieutenant General Walter C. Short have done with it."

Let us agree that the question raised is not a foolish one but let us consider it in two parts. First, as to why the British got the Purple system. In the autumn of 1940 U. S. military and naval authorities on the highest level agreed that there should and could be some exchange of intelligence between the U. S. and the U. K. Included in the material to be exchanged was communication intelligence. It was ascertained that the U. K. communication intelligence experts had not succeeded in solving the highest-level Japanese diplomatic crytosystem and the machine which was involved in enciphering and deciphering the messages in that system.

Nor, parenthetically, had the German experts. Cryptanalysts of the U. S. Army's Signal Intelligence Service, however, had accomplished this task and were reading the Japanese messages in that crytosystem, which
they had named, for brevity as well as for disguise, the "Purple" system, its predecessor, also a machine system, having been named the "Red" system. On the other hand, it had been ascertained that the U. K. cryptanalysts, although they had been unsuccessful with the "Purple" system, had been quite successful with certain German and Italian diplomatic cryptosystems the study of which had only recently been undertaken by U. S. cryptanalysts. It therefore seemed that both the U. S. and U. K. could profit by some sort of exchange. A team of four cryptanalysts, two from the Army and two from the Navy, was sent to London in January of 1941 to discuss the technical aspects of an exchange of material. The U. S. team took with it a recently-completed "Purple" machine and the data necessary to use it in deciphering the Japanese messages. It is very important to understand that the British had not only extensive facilities for intercepting and forwarding Japanese diplomatic traffic to London but they also had a corps of very competent cryptanalysts and Japanese translators—without whom possession of the "Purple" machine would have been of little or no value. The British also were able to read and translate other systems carrying Japanese diplomatic traffic—and they did so not only in London but also at Singapore and Hong Kong, and possibly in one or two other strategic spots under the British Crown.

In the exchange of the "Purple" machine and informational details concerning the Purple system for specific technical data on certain German and Italian cryptosystems (principally diplomatic) both the U. S. and the U. K. gained advantages of inestimable value. On this point there never has been any doubt on either side. Moreover, this exchange paved the way
to a later complete U. S. - U. K. collaboration in cryptanalytic opera-
tions after the U. S. entry into World War II as one of the belligerents.
The value of this collaboration can hardly be overestimated but this
brochure will not deal with this aspect.

As long as we are dealing with the question about the U. S. delivery
to the British of a "Purple" machine and the cryptosystem which used it,
we may well go into a related question concerning which little has been
said in the torrent of words about the Pearl Harbor disaster. The British
acquired the "Purple" in January 1941, and were able from the very first
to use it—no strings were attached to this usage, except that the secret
would be treated with the care that it deserved in order to keep from
enemy knowledge the fact that we had solved it. (There have always been
very detailed and strict regulations governing the handling of communica-
tions intelligence and in time the U. S. and U. K. regulations became
identical). The reason for mentioning that there were no strings attached
to the U. S. gift to the British is to forestall a revisionist allegation
that President Roosevelt must have permitted the gift to be made only on
condition that no information coming from "Purple" would be used by the
British in a manner that would interfere with his conspiracy to withhold
from the two commanders at Pearl Harbor whatever intelligence they might
obtain which would prevent the Japanese taking them by surprise. Such an
allegation would, of course, be absurd on its face—but then the revisionists
do not always argue in a logical manner. Exactly why the British
would, even if they could have agreed, to keep "Purple" intelligence from
Short and Kimmel is hard to understand. In the first place, although there
was no direct communication between these commanders and the British, certainly, there was communication between British and American intelligence authorities in the Far East. In the second place, let it be noted that the British had been able to read and were reading Japanese diplomatic systems other than Purple; in fact, many of the messages which the revisionists claim most definitely indicated that a surprise air attack was to be made at Pearl Harbor were in cryptosystems other than Purple. For example, the so-called "bombing plot" message was not in "Purple" at all but in a system held by consulates, a system designated by us as J-19; and several other messages related to the bombing plot message were in the same system.

What has all the foregoing to do with the British? Simply this: is it conceivable that the British, too, would have participated in a conspiracy of silence so as to let the Japanese destroy the U. S. Pacific Fleet, the fleet that was their principal protection against Japanese aggression in the Far East? Hardly. Is it not clear that the various messages in Purple and in the other Japanese systems conveyed to the British no definite statement as to an impending attack on the American bastion in the Hawaiian area? The British, let us remember, were then supposed to have the finest and most carefully trained intelligence experts in the world. Is it likely that the detailed story of an impending attack, if revealed by MAGIC, would have been completely overlooked by their experts? Is it conceivable that they would, if they saw the outlines of the story, have kept it to themselves? That they would have kept it from their U. S. friends? That they would have seen to it that no word of it
leaked to Short and Kimmel? The British were counting upon the U. S. to protect British interests in the Far East.

In the foregoing paragraphs it was stated that certain Japanese messages were long-delayed in their processing into plain English by the Army and Navy cryptanalytic units. These delays were caused by several things: (1) there were so many messages to be forwarded from U. S. intercept stations that U. S. radio facilities were then not equal to the task of carrying them all; many had to be sent by air mail pouch or even by ordinary U. S. Mail pouch; (2) there were so many messages and so few persons capable of processing them in Washington—let us not forget that a few dozens of persons in Washington were trying to keep up with what hundreds, perhaps thousands, of Japanese were doing in Japanese message centers in Japanese embassies, legations, and consulates all over the world; (3) there were many times when it was impossible to solve a new key until a sufficient amount of traffic had accumulated; (4) there were many cases when decrypting a message was stymied by errors in transmission or interception; (5) there were only a handful of persons in both the Army and the Navy cryptanalytic units who could translate Japanese—and no pool in the U. S. from which trained and trustworthy Japanese translators could be selected, as is the case in other foreign languages such as French, German, Spanish, etc.; and until the Japanese was converted into English, the messages containing useful intelligence about Japan might just as well be filed in the waste basket.

While we dwell upon the foregoing elements in the story it might be a good place to point out that a conspiracy to withhold information in
order that an attack might be carried out could hardly afford to risk certain contingencies. For instance, it would be essential, would it not, that a high degree of priority in processing be accorded all Japanese Government messages going to or coming from Honolulu, so that the alleged conspirators themselves might not be caught napping? But it is a fact that several very important messages having a direct bearing on the situation were not processed until several days after the attack. The very fact that the processing of all messages to and from Honolulu was not given the highest or even a high priority itself constitutes an argument against the alleged conspiracy being objective—and not completely subjective.

Let us now take up the question about the withholding of MAGIC from Admiral Kimmel and General Short—as viewed by the highest level authorities in Washington. First of all it is easy to admit the fact that the critical MAGIC messages of the early autumn of 1941 and up to the day of the attack were withheld from them; there can be no question whatever about this fact. But the important point is why? The revisionists say that it was necessitated by the Roosevelt-Marshall-Stark conspiracy to bring about the attack on the Fleet at Pearl Harbor. A dispassionate view, however, must take into consideration quite different and more logical factors. First, as the Purple messages continued to be read in Washington the strategic value of our solution of that cryptosystem became increasingly apparent. This is a good place to insert what General Marshall had to say on the subject of the value of MAGIC, which he described in detail in a highly secret letter he wrote to Governor Dewey, a
Republican, who had learned about MAGIC (nobody knows how or from whom).

Marshall had learned that Dewey was proposing to use this highly explosive
information in the 1944 Republican Presidential campaign against a fourth
term for Roosevelt. The war was not over! Here it is, in extenso:

Extracted from CONGRESSIONAL INVESTIGATION PEARL HARBOR ATTACK,
Part 3, pp. 1132-1133.

For Mr. Dewey's eyes only.

27 September 1944.

My dear Governor: Colonel Clarke, my messenger to you of yester-
day, September 26th, has reported the result of his delivery of my
letter dated September 25th. As I understand him you (a) were unwill-
ing to commit yourself to any agreement regarding "not communicating
its contents to any other person" in view of the fact that you felt
you already knew certain of the things probably referred to in the
letter, as suggested to you by seeing the word "cryptograph," and
(b) you could not feel that such a letter as this to a presidential
candidate could have been addressed to you by an officer in my posi-
tion without the knowledge of the President.

As to (a) above I am quite willing to have you read what comes
hereafter with the understanding that you are bound not to communi-
cate to any other person any portions on which you do not now have
or later receive factual knowledge from some other source than myself.
As to (b) above you have my word that neither the Secretary of War
nor the President has any intimation whatsoever that such a letter
has been addressed to you or that the preparation or sending of such
a communication was being considered. I assure you that the only
persons who saw or know of the existence of either this letter or my
letter to you dated September 25th are Admiral King, seven key
officers responsible for security of military communications, and
my secretary who typed these letters. I am trying my best to make
plain to you that this letter is being addressed to you solely on
my initiative, Admiral King having been consulted only after the
letter was drafted, and I am persisting in the matter because the
military hazards involved are so serious that I feel some action is
necessary to protect the interests of our armed forces.

I should have much preferred to talk to you in person but I
could not devise a method that would not be subject to press and
radio reactions as to why the Chief of Staff of the Army would be
seeking an interview with you at this particular moment. Therefore
I have turned to the method of this letter, with which Admiral King
concurs, to be delivered by hand to you by Colonel Clarke, who, incidentally, has charge of the most secret documents of the War and Navy Departments.

In brief, the military dilemma is this:

The most vital evidence in the Pearl Harbor matter consists of our intercepts of the Japanese diplomatic communications. Over a period of years our cryptograph people analyzed the character of the machine the Japanese were using for encoding their diplomatic messages. Based on this a corresponding machine was built by us which deciphers their messages. Therefore, we possessed a wealth of information regarding their moves in the Pacific, which in turned was furnished the State Department—rather than as is popularly supposed, the State [29375] Department providing us with the information—but which unfortunately made no reference whatever to intentions toward Hawaii until the last message before December 7th, which did not reach our hands until the following day, December 8th.

Now the point to the present dilemma is that we have gone ahead with this business of deciphering their codes until we possess other codes, German as well as Japanese, but our main basis of information regarding Hitler's intentions in Europe is obtained from Baron Oshima's messages from Berlin reporting his interviews with Hitler and other officials to the Japanese Government. These are still in the codes involved in the Pearl Harbor events.

To explain further the critical nature of this set-up which would be wiped out almost in an instant if the least suspicion were aroused regarding it, the battle of the Coral Sea was based on deciphered messages and therefore our few ships were in the right place at the right time. Further, we were able to concentrate our limited forces to meet their naval advance on Midway when otherwise we almost certainly would have been some 3,000 miles out of place. We had full information of the strength of their forces in that advance and also of the smaller force directed against the Aleutians which finally landed troops on Attu and Kiska.

Operations in the Pacific are largely guided by the information we obtain of Japanese deployments. We know their strength in various garrisons, the rations and other stores continuing available to them, and what is of vast importance we check their fleet movements and the movements of their convoys. The heavy losses reported from time to time which they sustain by reason of our submarine action, largely result from the fact that we know the sailing dates and routes of their convoys and can notify our submarines to lie in wait at the proper points.
The current raids by Admiral Halsey's carrier forces on Japanese shipping in Manila Bay and elsewhere were largely based in timing on the known movements of Japanese convoys, two of which were caught, as anticipated, in his destructive attacks.

You will understand from the foregoing the utterly tragic consequences if the present political debates regarding Pearl Harbor disclose to the enemy, German or Jap, any suspicion of the vital sources of information we possess.

The Roberts' report on Pearl Harbor had to have withdrawn from it all reference to this highly secret matter, therefore in portions it necessarily appeared incomplete. The same reason which dictated that course is even more important today because our sources have been greatly elaborated.

As another example of the delicacy of the situation, some of Donovan's people (the OSS) without telling us, instituted a secret search of the Japanese Embassy offices in Portugal. As a result the entire military attache Japanese code all over the world was changed, and though this occurred over a year ago, we have not yet been able to break the new code and have thus lost this invaluable source of information, particularly regarding the European situation.

A further most serious embarrassment is the fact that the British government is involved concerning its most secret sources of information, regarding which only the Prime Minister, the Chiefs of Staff and a very limited number of other officials have knowledge.

A recent speech in Congress by Representative Harness would clearly suggest to the Japanese that we have been reading their codes, though Mr. Harness and the American public would probably not draw any such conclusion.

The conduct of General Eisenhower's campaign and of all operations in the Pacific are closely related in conception and timing to the information we secretly obtain through these intercepted codes. They contribute greatly to the victory and tremendously to the saving in American lives, both in the conduct of current operations and in looking towards the early termination of the war.

I am presenting this matter to you in the hope that you will see your way clear to avoid the tragic results with which we are now threatened in the present political campaign.

Please return this letter by bearer. I will hold it in my most secret file subject to your reference should you so desire.

Faithfully yours,  

(Sgd) G. C. MARSHALL.
It seems to me that the foregoing letter goes a long way toward answering the question as to why MAGIC was withheld from Kimmel and Short. Stated briefly, the authorities in Washington were fearful that if MAGIC continued to be sent them the secret that we were able to read all their diplomatic cryptocommunications, including "Purple", their most secure system, would soon find its way to the Japanese. The whole of the island of Oahu had thousands of Japanese nationals, among whom it was natural to assume there were—there must have been—plenty of spies. The Army and Navy authorities in Washington felt that it was becoming too dangerous to the continued secrecy of the fact that we had solved and were reading messages in Purple to send any more of the messages to Kimmel and Short. Of course they could have been sent some gists—as had been done in the first half of 1941—but General Sherman Miles, the then Assistant Chief of Staff for Military Intelligence, stated before the Joint Congressional Committee that sending even gists would have been dangerous, by overloading the radio circuits; and he went on to say that while the Navy cryptosystems could have been used, because they were more secure than the Army's, even that would not remove the danger altogether. I will interject at this point the statement that General Miles was not too well-informed on these practical matters, because the Navy had adopted and was using an Army cryptosystem and a machine invented by Army personnel. Both the Army and the Navy's cryptosystems could and would have stood up under the strain of sending all the important MAGIC messages to Kimmel and Short and in extenso.
But, insist the revisionists, the Navy furnished a MAGIC machine and information on how to use it to the Commander of the 16th Naval District—the Philippines. Why not to Kimmel and Short? There were very good reasons for this; but at this point we shall merely ask: did possession of MAGIC prevent General MacArthur from being taken by surprise and losing all his planes at one fell swoop more than 12 hours after the General knew of the Japanese attack on Pearl Harbor? General MacArthur blames his chief of the Army Air Corps forces in the Philippines, General Brereton, for being caught napping; and Brereton blames MacArthur. Possession of the Purple machine alone obviously was not sufficient—the interpretation, appreciation, and evaluation of MAGIC is just as important. It might be useful to quote what General Willoughby, MacArthur's G-2, said on this latter point in an affidavit dated 8 May 1945 (PHR, Part 35, p. 87) in protecting the Navy's monopoly of MAGIC:

In 1941 the Navy obtained and maintained a highly efficient crypto-analytical service, specializing in Japanese material; though the Army had notably participated in the development of this subject, the Navy appears to have obtained a lead; consequently, it can be said that the Navy enjoyed on almost monopolistic privilege. In an otherwise meritorious desire for security (though every modern nation knows that crypto-analysis is going on), the Navy has shrouded the whole enterprise in mystery, excluding other services, and rigidly centralizing the whole enterprise. At this date, for example, this same system is still in vogue: as far as SWPA is concerned, the crypto-analysis is made in Melbourne, forwarded via 7th Fleet D.N.I.; the Melbourne station is under direct orders of Washington, is not bound by any local responsibilities, forwards what they select, and when it suits them. The possibility of erroneous or incomplete selection is as evident now as it was in 1941. The only excuse the Navy has is that its field is primarily naval intercepts, but there is a lot of Army traffic or other incidental traffic. This collateral traffic is not always understood or correctly interpreted by the Navy, in my opinion.
The solution to this vexing and dangerous problem is a completely joint, inter-locking intercept and crypto-analytical service, on the highest level, with the freest interchange of messages and interpretation.

The sequence of messages referred to, had they been known to a competent intelligence officer, with Battle Order and tactical background, beginning with November 14th, would have led instantly to the inescapable conclusion that Pearl Harbor naval installations were a target for attack, with November 25th or November 29th as the deadlines, suggesting irresistibly that elapsed time was involved, for some sort of naval seaborne sortie.

C. A. Willoughby,
C. A. Willoughby,
Major General, G. S. C.,
Asst. Chief of Staff, G-2,
General Headquarters, SWPA.

The fact is that skilled cryptanalytic help and skilled Japanese translators were not in sufficient supply to permit either the Army or the Navy to maintain many such people anywhere outside the U. S.—they were badly needed in Washington. And besides, nobody thought or even imagined that they were so badly needed at Pearl Harbor as at Manila—the Japanese would never be so foolhardy as to attack Pearl! The U. S. Navy authorities believed that the Philippines might be cut off—but not Hawaii. Manila needed MAGIC much more than Pearl! That explains why there was a Purple machine in Manila, more than anything else. The Navy communications personnel at Pearl were assigned the mission of trying desperately to solve the important Japanese naval cryptosystems and to get what information could be gleaned from traffic analysis of Japanese communications; the Army had no signal intelligence or cryptanalytic personnel at all in Hawaii after 1939—the very small unit it did have in Honolulu was brought back to Washington after but one year's operations there—because the few trained persons of that unit were thought
to be much more useful in Washington. Hawaii seemed to be the last place the Japanese would try to attack! Why keep the few trained cryptanalytic personnel there when they could be so much more useful in Washington? What the Army had, therefore, was simply an intercept unit directed to listen in on certain assigned Japanese circuits and to forward the traffic to Washington for study.

In this decision to bring back to Washington that small Army cryptanalytic unit (two or three persons at most!) I am quite sure that the Chief Signal Officer consulted no higher authority—and, I am sure too, the Commanding General of the Hawaiian Department at that time, General Short's predecessor, was glad to get rid of the unit—its maintenance caused him difficult logistical problems. The secrecy of its operations certainly was a source of irritation to him and his staff—they never got to see the results. The trained Signal Corps officer the Signal Intelligence Service in Washington sent to Hawaii in 1940 performed no signal intelligence functions; by direction of the local commander he was soon given "more necessary" duties, such as devising and supervising the laying of communication cables in and around Honolulu. And with this decision I can take no exception—the Commanding General on the spot knew best what he needed. I know for a fact that when the Signal Corps sent a very small unit to Corregidor it was only with the greatest difficulty that the Commanding General there was finally persuaded to let the unit do what it was sent out to do—but only for a short time. The members of any Signal Intelligence unit (Signal Corps personnel) were badly needed for ordinary Signal Corps functions. Washington could do
very little about this—the local commander decided. In all that I have said above, however, the most important point by far was, so far as concerned both the Philippines and Hawaii, that an attack by the Japanese was too fantastic to warrant much thought, so preparations for a possible attack were somewhat neglected.
5. THE "WINDS CODE MESSAGES"

Many thousands of words have been expended in discussing and writing the story of the so-called "Winds Code Messages," and, in particular, whether there were any authentic "Winds Code Execute" messages.

There were two "Winds Code" set-ups, which were intended, for reasons peculiar to the Oriental mentality, to give a certain kind of warning but just exactly what kind of a warning is unclear because both of these "set-ups" were, to say the least, impractical, indeed quite foolish, because they were so susceptible of being confused with ordinary weather and news broadcasts. And, indeed, this is exactly what did happen with regard to the one of most interest to the U. S. A weather broadcast—now termed the false "Winds Code Execute" message was intercepted—and for a few hours at any rate was taken to be the real thing. But it wasn't "the real McCoy"—it resembled what the Execute message might have been but when carefully scrutinized it just didn't meet all the conditions specified in the code instructions. The alarm it set off subsided as soon as the discrepancies with what a real Execute should be were recognized.

I think that one thing was established conclusively after exhaustive investigation by several of the Pearl Harbor boards, including that of the Joint Congressional Committee: the Japanese never did send out an authentic "Winds Code Execute" message which clearly indicated that Japan was going to attack the U. S. If indeed the Foreign Ministry intended to transmit such a message it was forgotten at the last moment; and even if
it had not forgotten, the most the message could have conveyed was that there was going to be a break in relations between Japan and the country signified by the particular "Winds Code Execute" message. The other thing which seems to be certain is that having forgotten to send out the "Execute" meaning a break between Japan and the U. S., somebody seems to have remembered to send out after the attack on Pearl Harbor a "Winds Code Execute" signifying that Japan was breaking relations with Britain but not with the U.S.S.R. Even this one the Japanese who were interrogated after the surrender of Japan denied having transmitted but all the evidence I have examined indicates that they were not telling the truth. One might say, if they didn't tell the truth about that one we should not put any credence in their denial that a "Winds Code Execute" was sent out on 3 December, the one indicating a break in relations (or war) with the U. S. Certain of the Japanese interrogated on the point denied ever setting up the "Winds Code" in the first place. This point is examined in great detail in Appendix E to PER, p. 467-486 and there is consummate skill in this examination. The PER arrived at the following conclusion, which I think represents the last word that can be said on this subject (p. 486):

CONCLUSION: From consideration of all evidence relating to the winds code, it is concluded that no genuine message, in execution of the code and applying to the United States, was received in the War or Navy Department prior to December 7, 1941. It appears, however, that messages were received which were initially thought possibly to be in execution of the code but were determined not to be execute messages. In view of the preponderate weight of evidence to the contrary, it is believed that Captain Safford is honestly mistaken when he insists that an execute message was received prior to December 7, 1941. Considering the period of time that has elapsed, this mistaken impression is understandable.
Granting for purposes of discussion that a genuine execute message applying to the winds code was intercepted before December 7, it is concluded that such fact would have added nothing to what was already known concerning the critical character of our relations with the Empire of Japan.

This conclusion reached in 1946 remains unshaken to this day—nothing has turned up to make a change in it desirable, so far as concerns any "Winds Code Execute" message that might have been transmitted on 3 December, as Captain Safford contended. One could only wish that the conclusion had stated categorically that there was such a message in regard to a break in relations between Japan and the British (and also the Dutch East Indies) because the evidence is clear that such a signal was sent—but then, by that time, 8 December, the attack on Pearl Harbor was finished.

The "revisionists," however, still believe in Captain Safford—the sole person who stuck to his statement that there was a 3 December warning, and that all copies of that message were deliberately destroyed. The interesting thing about this whole tempest-in-a-teapot is that even if there had been an authentic U. S.-Japan execute message it would have not told us nothing whatever that was already known on 3 December. Moreover, and this I think is very important, the attack on Pearl was prepared for with so much secrecy I would doubt very much that the Japanese would take any chance whatever in sending out a message which might "tip their hand". It just doesn't fit in the picture at all.

It is interesting to note that Admiral Kimmel, while he mentions the "Winds Code" affair and cites (p. 100) what the Naval Court of Inquiry said about it—later proved to be wrong—does not press the
matter to seriously. I think the Admiral is very dubious that a real Execute was ever sent out on 3 December as claimed by Captain Safford, although he does say (p. 101): "The findings of the Naval Court of Inquiry on this subject are confirmed by the evidence presented to the joint congressional investigating committee." The Admiral does not state specifically what the "findings" were but the reader is left to conclude that the committee found that there was an Execute transmitted on 3 December and that it was intercepted by us—but the information was not transmitted to him or to other commanders afloat.

Senators Ferguson and Brewster in their Minority Report say (p. 526): "Even if the wind execute message they saw was a false one they believed it true at the time and should have acted accordingly." A good point, and I think, one that should be emphasized; it is too bad it wasn't followed up regardless of any other considerations.
6. THE QUESTION OF SABOTAGE

What led General Short to prepare for sabotage rather than for military action by the Japanese?

In my opinion the reason for General Short's very brief answer to the war warning message sent him after the 26 November 1941 American rejoinder to Japanese proposals for arriving at a modus vivendi was not, as many people believe, utter nonsense. Short said merely that he was prepared for sabotage. The fact is that everybody in Washington and, apparently, also in Honolulu had but two things in mind as to possible or probable Japanese action. First, the Japanese march was certainly to be to the southward (to Malaya, Thailand, Indo-China, Borneo, or the Dutch East Indies; indeed all their actions seemed to point in those directions) and Short was not able to do anything at all about that. Then, secondly, there was incessant talk in America, including in the radio broadcasts and in the writings of columnists, sabotage was what we had to guard against. The generally-held view was that the Japanese were tricky, that attempts to thwart their march would be countered by the various mechanisms of sabotage. This I remember very vividly. And I feel sure that when General Gerow received General Short's message stating that all steps to prevent sabotage had been taken and that he was in liaison with the Navy, General Gerow probably thought "Fine business—Short's on the job." So must have the others in Washington who saw it—General Marshall included. By hindsight Short's message seems entirely unresponsive to the message sent him. But the matter of
sabotage was in the air. That's what we had to look out for. Confirmation of this attitude can be seen in various messages. Even the Navy's strong message beginning "This dispatch is to be considered a war warning" ends with "Continental Districts Guam Samoa directed to take appropriate measures against sabotage." Everybody had forgotten all about the war plan of May 1941 which envisaged as the first and most dangerous contingency a surprise air attack on the Fleet at Pearl Harbor. Parenthetically I may add that those whose memories of World War I included the two great acts of sabotage by German agents in this country (the Black Tom explosion and the Kingsland Fire) before the U. S. became a belligerent in that war will perhaps agree with me that Japanese sabotage was the thing Americans thought was most to be feared in regard to American territory. Let us not forget that this fear quickly expressed itself very clearly and heartlessly in what was done to thousands of Japanese-American citizens (including Nisei) in California the moment we declared war on Japan. Why did they move them out of the port cities? What were the authorities afraid of? Sabotage! For this reason I, for one, find it difficult to criticize General Gerow in his handling of General Short's message in response to the 26 November message from Washington.

But what about the views held by U. S. intelligence authorities on this question of sabotage? Were they the same as those of the average American citizen, "the man-in-the-street"? I think they were—and just as the views of "the man-in-the-street" of those days were wrong, so it seems were the views of our intelligence authorities. Why? Because we never have paid too much attention to intelligence. After several
thousands of years of experience, why do military and naval authorities seem to pay less attention to intelligence than to logistics, for instance? Why does intelligence have to play the role of step-child in the conduct of warfare? What is there about intelligence that makes it less desirable as a career than artillery, for example? The reasons are clear when one looks into the matter.

Admiral Theobald lays great emphasis on Tokyo to Honolulu message number 83 of 24 September 1941 (the so-called "Bombing Plot Message") and says (p. 46):

After studying Tokyo dispatch #83, no military intelligence organization could fail to reach that deduction [that it was to prepare the detailed plan for a surprise attack on the major units of the Fleet moored there].

Here I think is the kernel of the nut—the secret of why the U. S. was taken by surprise. I have underlined the phrase "no military intelligence organization" in the foregoing extract because I think that our military and naval intelligence organizations had serious defects at that time—and I think they still have. (Theobald does not mean just military, U. S. Army Intelligence, but also U. S. Navy Intelligence.)

I think that serious defects in our military and naval intelligence made it possible for the Japanese to take us by surprise at Pearl Harbor. A strong statement? Yes, but I think it is warranted. I will with some diffidence go into this question because I do not know too much about the situation as of 1957. I did know what it was like in 1940-41 and in 1950, four years after the PIR was released. It is clear that the intelligence situation in the U. S. was defective in 1940-41 and in 1950, when the Korean "police action" broke out without warning. Where
were our intelligence services then? What were they doing or thinking about? By 1950 we had CIA. What help was CIA?

Four years after the PRH was released, Major General Sherman Miles, Assistant Chief of Staff for Intelligence of the War Department General Staff, from April 1940 to February 1942, in what some people may regard as an apologia, has many things to say in an endeavor to explain what appear to have been derelections of himself and his staff. It was an attempt to absolve G-2 from its responsibility for the debacle on December 1941. For the most part he does as good a job of this, perhaps, as could be done to exculpate G-2 from its failures, omissions, and lack of the kind of imagination which might have foreseen and forestalled the disaster caused by the Japanese surprise attack. A salient paragraph among many which could be quoted is the following (p. 71):

The plain fact is that the war warnings sent out by the highest military authorities nine days and more before Pearl Harbor were far more authoritative and more definitive of what the Hawaiian commands might expect, and what was expected of them, than any information or interpretations from "magic" that Military or Naval Intelligence could possibly have sent. Complete reliance was placed on the effect those warnings should have had—and did have everywhere except in Hawaii. But Tokyo apparently believed that the incredible might happen and Hawaii be surprised: Washington did not.

General Miles takes it for granted that the warnings sent out by Washington properly alerted all our overseas commands except the one in Hawaii. One wonders about the basis for the General's assumption in this regard. Indeed, in one case, already mentioned, even 12 hours after General MacArthur in the Philippines knew that the Japanese had made the

surprise attack at Pearl Harbor his command was nevertheless taken completely by surprise, when the Japanese destroyed all his planes on the ground, just as they did in Hawaii. General Miles, notwithstanding his statement that (p. 70):

"The Hawaiian commands later complained that this "magic" information was not transmitted to them—this in spite of their failure to react to the authoritative warning orders sent them when the situation was commonly known to be far more critical. By comparison, it may be noted that General MacArthur, who had access to "magic," could not later identify the more important "magic" messages; he apparently took no action on them, but alerted his command for war on Washington's warning orders.

Thus assumes that General MacArthur "alerted his command for war on Washington's warning orders." What does "alerting" mean, anyhow, if a commander loses all his planes by what I think was inattention?

General Miles admits (pp. 70-71) that "there were two "MAGIC" messages ... which have subsequently been held to have been signposts, had we so read them, to Pearl Harbor." The General devotes many words to these two cases and concludes that the signposts pointed to a half-hearted proposal, admittedly discussed in Washington, that the British and U.S. occupy the Netherland Indies before the Japanese did so—and he thus tried to explain away the famous clue contained in a Tokyo message to Berlin telling General Oshima, the Japanese Ambassador to Germany, to tell the Germans: "Say very secretly to them that there is extreme danger that war may suddenly break out between the Anglo-Saxon nations and Japan through some clash of arms, and add that the time of the breaking out of this war may come quicker than anyone dreams." The explanation of Miles (or, better perhaps, the lack of imagination) on the part
of U. S. intelligence agencies appears to me (even by hindsight, of course) to be pretty thin.

Here are two more paragraphs from General Miles’ article, both of which I think are of considerable significance:

The last twenty-four hours in Washington before the bombs fell have come in for much scrutiny. Why did the President, with most of the Japanese final answer before him, conclude that it meant war and then, after a fitful attempt to reach Admiral Stark by telephone, quietly go to bed? Why was he in seclusion the following morning? Why was no action taken on the Japanese reply by the Secretaries of State, War, and Navy when they met on that Sunday morning? Why did they not consult the President, or he send for them? Where was everybody, including my humble self? Why, in short, didn’t someone stage a last-minute rescue, in good Western style?

The picture undoubtedly is one of men still working under the psychology of peace. They were, to quote Secretary Stimson again, "under a terrific pressure in the face of a global war which they felt was probably imminent. Yet they were surrounded, outside of their offices and almost throughout the country, by a spirit of isolationism and disbelief in danger which now seems incredible." They were men who thought they had done their possible to prepare for impending war, and who had no idea that there was an innocent maiden in need of rescue.

I will add another extract that may be helpful in seeing things in what I regard as their proper light. This extract comes from Secretary Stimson’s statement with respect to the report of the Army Pearl Harbor Board, repeated as a footnote (p. 239) to the FHR:

As expressed by Mr. Stimson: "A keener and more imaginative appreciation on the part of some of the officers in the War and Navy Departments of the significance of some of the information might have led to a suspicion of an attack specifically on Pearl Harbor. I do not think that certain officers in the War Department functioned in these respects with sufficient skill. At all times it must be borne in mind, however, that it is easy to criticize individuals in the light of hindsight, and very difficult to recreate fairly the entire situation and information with which the officers were required to deal at the time of the event." See statement of the Secretary of War with respect to the report of the Army Pearl Harbor Board, committee exhibit No. 157.
My own explanation of the failures and derelictions of U. S. intelligence can be stated in few words: I do not think there were no imaginative officers in G-2 or in Naval Intelligence; but more important there was nobody in either the Army or the Navy intelligence staffs in Washington whose most important, if not sole duty, was to study the whole story which the MAGIC messages were unfolding and which played so important a part in our failure to deduce that the Japanese were planning a surprise attack on the U. S. Fleet at Pearl; there was nobody whose responsibility it was to try to put the pieces of the jigsaw puzzle together. Certainly there was nobody in the Army's Signal Intelligence Service who was assigned to or available for this purpose—even if the responsibility for this sort of work had been fixed on that organization, which it wasn't. This was likewise true of the equivalent Navy organization. This important phase of intelligence was a responsibility which in both services was jealously held by the Intelligence staffs. And the distribution of the MAGIC messages was so rigidly controlled that there was nobody in either of these Intelligence staffs whose duty it was to study the messages from a long-range point of view. The persons, officers and civilians, in intelligence, as well as in the White House, had the messages only for so short a time that each message represented only a single frame, so to speak, in a long motion picture film—a film which should have been shown and should have been intently studied as a continuous series of pictures, because they were telling a story. But the film was simply not there to be studied and this was a very serious weakness, I think, in the intelligence organizations of the two Services. It may have been that they
simply did not have the people to devote to such work.

Of course, there are those critics who point to the message which Navy Captain McCollum testified that he thought should be sent to Admiral Kimmel, and to the one which the Army's Colonel Sadtler testified that he thought should be sent to General Short. They, it seemed, sensed that MAGIC was telling a story and was pointing toward a surprise attack, the most likely target being Pearl Harbor. But both efforts came up against stone walls—their superior officers claimed enough had been sent to put Kimmel and Short on full alert: To send more would only confuse them, or worse than that, irritate them. But the latter were obviously wrong—or so it seems to us now—again by the aid of hindsight. Admirals Theobald and Kimmel have made the most of this failure on the part of those above Captain McCollum and Colonel Sadtler to realize how inadequate the warnings that had been sent to Short and Kimmel really were.

The Joint Congressional Committee (Majority Report) clearly felt that what Kimmel and Short were sent by way of information left much to be desired. One thing seems certain, as I have already said: the intelligence arrangements in both Services were inadequate. The Committee reached certain conclusions and made but five major recommendations, the second of which is as follows:

That there be a complete integration of Army and Navy intelligence agencies in order to avoid the pitfalls of divided responsibility which experience has made so abundantly apparent; that upon effecting a unified intelligence, officers be selected for intelligence work who possess the background, penchant, and capacity for such work; and that they be maintained in the work for an extended period of time in order that they may become steeped in the ramifications and refinements of their field and employ this reservoir of knowledge in evaluating material received.
The assignment of an officer having an aptitude for such work should not impede his progress nor affect his promotions. Efficient intelligence services are just as essential in time of peace as in war, and this branch of our armed services must always be accorded the important role which it deserves.

What has been done about this recommendation by the Services? Very little; in fact, I think it can be said that nothing has been done. Of course, we have the Central Intelligence Agency; but is that establishment really responsive to the Joint Committee's recommendation? I hardly think so. The three services no doubt can cite good reasons why they have not made a professional career in intelligence possible or attractive to its officer personnel; no doubt they can cite at length factors and difficulties that would have to be overcome. All I can say is that judging by what the Army has done the attitude toward intelligence seems not to have changed very much, as is indicated by the following editorial which appeared in the Washington Post on 5 December 1955 and which states the case in succinct terms:
Snub to Intelligence

The recent reorganization in the Army General Staff leaves the Military Intelligence Service in an ambiguous and rather humiliating position. Although directors of the other major staff divisions have been designated as Deputy Chiefs of Staff with the rank of lieutenant general, the Chief of Intelligence remains a major general with the subordinate title of Assistant Chief of Staff.

The extraordinary thing about all this is that not long ago the special task force which investigated the intelligence problem for the Hoover Commission strongly recommended that in the case of those units associated with the three armed services their chiefs "be evaluated in the organizational structure to level of Deputy Chiefs of Staff in the Army and Air Force, and Deputy Chief of Naval Operations in the Navy." This was a rather prolix way of saying that they ought to have a little more prestige and influence, along with a little more gold braid, than they now enjoy. Why, in the case of all three services, was this recommendation ignored by the Department of Defense?

The chief function of military intelligence is to collate and interpret the information provided by the attaches abroad and by other agencies, such as the CIA, the FBI and its own counterespionage service. Correct interpretation requires more than the accumulation of relevant facts; it also requires a considerable knowledge of the psychology of the potential enemy, and this in turn requires an extensive study of his language, history, culture, customs and philosophic tradition, since these afford the keys to such an understanding. But all this, together with the secrecy in which their activities are necessarily cloaked, seems to have made intelligence officers somewhat suspect to a certain sort of politician. Even professional military men are often inclined to discount the value of the critical function exercised by intelligence officers in the discussion of pet military projects or plans.

The question raised by the reorganization is whether we can realistically expect to increase the quality of military intelligence by deemphasizing its significance. It is hard to see how a career in intelligence can be made to appeal to capable officers when the importance of intelligence is so obviously downgraded in comparison with other staff functions.
High-level Army authorities obviously don't think that Intelligence is as important as Personnel, Supply, and similar services. How long will it take before it becomes quite clear to them that Intelligence can be of the greatest help in fighting a war? For too many years intelligence in the Army and in the Navy has been a "deadend" for officers who showed an interest in it, or an aptitude for it. Is this to continue indefinitely? Do the Armed Forces think that the Central Intelligence Agency will or can do the job? Of course, CIA representatives can be assigned to the headquarters of military commands—but will that fill the need? I doubt it, I doubt it very much.

The introductory statement of the "Supervisory, Administrative, and Organizational Deficiencies in our Military and Naval Establishments revealed by the Pearl Harbor Investigation" (p. 253) the PHR begins as follows:

The Committee has been intrigued throughout the Pearl Harbor proceedings by one enigmatical and paramount question: Why, with some of the finest intelligence available in our history, with the almost certain knowledge that war was at hand, with plans that contemplated the precise type of attack that was executed by Japan on the morning of December 7—Why was it possible for a Pearl Harbor to occur? The answer to this question and the causative considerations regarded as having any reasonably proximate bearing on the disaster have been set forth in the body of this report. Fundamentally, these considerations reflect supervisory, administrative, and organizational deficiencies which existed in our Military and Naval establishments in the days before Pearl Harbor. In the course of the Committee's investigation still other deficiencies, not regarded as having a direct bearing on the disaster, have presented themselves. Otherwise stated, all of these deficiencies reduce themselves to principles which are set forth, not for their novelty or profundity but for the reason that, by their very self-evident simplicity, it is difficult to believe they are ignored.
It is recognized that many of the deficiencies revealed by our investigation may very probably have already been corrected as a result of the experiences of the war. We desire, however, to submit these principles, which are grounded in the evidence adduced by the Committee, for the consideration of our Army and Navy establishments in the earnest hope that something constructive may be accomplished that will aid our national defense and preclude a repetition of the disaster of December 7, 1941. We do this after careful and long consideration of the evidence developed through one of the most important investigations in the history of the Congress.

What have the Services done to ameliorate the deficiencies mentioned? In my opinion, very little. Maybe it would be correct to say "nothing."

As a colleague said to me recently "Nothing will be done—until war breaks out. Then, of course, intelligence is no longer treated a step-child."

Is that what we want? The chances are that there won’t be time to use intelligence after a war breaks out: maybe the U. S. will be down and out by that time.
7. CONCLUSIONS

After reading some but not all the millions of words alluded to at the beginning of this brochure to what conclusions have I arrived? I will be brief.

First, I must confess, I think that Kimmel and Short were not as culpable as I first thought they were back in 1941-1942, despite all the "warnings" sent them. The Washington authorities were culpable, too—maybe a lot more culpable than were these two officers. Both the Majority and the Minority Reports make good sense. The Report of the Majority contained some very pertinent recommendations—but nobody seems to be doing very much about implementing the second and perhaps the most of these recommendations; nor has much, if anything, been done about following up on the Conclusions of the Minority, Senators Ferguson and Brewater. In 1946 I thought the latter two senators were "hitting below the belt" but today, in 1957, I think they hit closer to the truth than the Majority. I think Mr. Keefe's "additional views" on the Majority Report make good sense—Kimmel and Short, he said, were not the sole culprits. I think that the Intelligence Services came off rather easily—too easily in the fixing of responsibility and pointing out derelictions. I think the intelligence staffs might have used more imagination but this was not because they were staffed with obtuse officers or persons of low-grade intelligence. As a matter of cold fact, I think, they were badly understaffed, because in both the Army and the Navy "intelligence" didn't count—for much at any rate, then. This raises the question: does it
count for much more today in the Armed Services? I think that Kimmel and Short should have been sent more information—even if they were sent only "gists" of MAGIC—to let them evaluate for themselves the significance of what the Japanese were saying. General Miles says that the warning messages sent them were of far more importance than anything they could have got from "Magic". I don't agree. They might have had more time to ruminate; they might even have guessed—as Admiral Kimmel hints—what the Japanese were planning; our commands might therefore have been much more prepared than they were to meet the attack. This, one must admit, could have been done even without their having a Purple machine or a cryptanalytic staff to solve and translate messages in that or in the other Japanese diplomatic systems.

I think that Admiral Stark was wrong in waiting for General Marshall to be found before sending off a message to Kimmel and Short—and to the other overseas commanders—as soon as the last part of the 14-part Tokyo to Washington message became available—especially when he knew from "Magic" that Kurusu and Nomura were told exactly to the minute when to present the whole message to Secretary Hull. (That we knew the contents of the last part of that message "deliver this whole message exactly at 1:00 p.m." before the Japanese Embassy code clerks had them is a credit to the efficiency of Army and Navy cryptanalytic staffs.)

I think that Colonel Edward French, Chief of the Signal Corps Message Center, used very poor judgment when he sent Marshall's message via commercial radio. He could have used Navy radio or FBI radio—but I am sure he thought it was infra dig to ask a "sister" government radio
service (especially the Navy) to do (at a critical moment) something that Army radio couldn't do. Or maybe Colonel French didn't realize the gravity of the situation, or was not told so in impressive enough language.

The Ferguson-Brewster Minority Report does not point the finger at all the high ranking officials who should share the responsibility but it does say (p. 573) "Both in Washington and in Hawaii there were numerous and serious failures of men in the lower civil and military echelons to perform their duties and discharge their responsibilities. These are too numerous to be treated in detail and individually named." I would have liked them to have named the Directors of Intelligence in the Army and in the Navy, specifically, because I think poor intelligence work played such a large part in the debacle.

And, of course, although it is clear that MAGIC was withheld from Kimmel and Short after the summer of 1941, I do not think (and of this I am quite sure) that it was deliberately withheld for the specific purpose of bringing on the attack at Pearl! Except for the most rabid of the revisionists this is too fantastic a thesis; but there is a stronger argument against such a thesis: it is not supported by the facts.
8. EPILOGUE

What was it that so aroused the anti-Rooseveltians, leading them to suspect that it was "skullduggery" and gross negligence in Washington that was responsible for the Pearl Harbor disaster?

Why did the President, his closest associates in the White House, and the officers in the top-level positions in the Army and in the Navy, generate so much suspicion in the minds of the Republicans? Why such reluctance to have an investigation to explain why the U. S. forces were caught by surprise at Pearl Harbor? This is a point which I do not think is explained in the literature and which ought to be. Why did the President and his administration allow so much suspicion to grow up in the minds of the Republicans by the questions which the latter raised after 7 December 1941 and which they continued to raise throughout the war? Could this have been avoided? It is my opinion that it was this refusal to explain, this subjecting to continued "needling" of the President and the Democrats by the Republicans throughout the war that aroused the gravest suspicions that there was indeed gross negligence in the White House and at the highest executive levels, and maybe greater derelictions to be hidden. The adamant resistance the President and the Democratic Administration had to maintain against Republican pressure for Congressional hearings on this point and the reasons therefore were quite obvious: we now know that such hearings would have "let the cat out of the bag"—that the U. S. was reading all the Japanese crypto-communications between the Foreign Office and its embassies, legations, and consulates abroad. The Japanese would have changed their Purple system without delay. It
is inconceivable, the Administration believed, that the secret could have been kept even if all the hearings were in Executive Sessions. They felt and were warranted in feeling that Hearings on the subject would be disastrous during the war: too much vital information on the subject would have leaked out. It is true that the Japanese had been alerted during the war by the Germans; they were told, in fact—and nobody knows to this day just how the Germans found out—that we were reading Japanese diplomatic messages. All this appears in the FBI and makes interesting reading. But it is astonishing that even after they were told the Japanese just simply refused to believe the story and continued to use the Purple system. (Neither, for that matter, did the Germans put much credence in the suspicions, forwarded by Marshal Rommel from Africa, that the British must be reading his messages; Rommel felt that this and only this could account for his continuing defeats in North Africa after 1943! Have these two episodes any lessons for us? Yes, indeed! Cryptographers become ensnared of their inventions and their minds become polarized in a sort of conviction that the systems they have concocted are invincible. It happened to us, too! I can remember the mental shock I had when indubitable evidence was placed before me showing that the Germans were reading the enciphered code system we were using for communications between U. S. Army Observer with the British Expeditionary Forces in North Africa in 1942-3 and Washington! That is why I believe that some body—experts, of course—outside the one that thinks up and produces our own crypto-systems but within NSA should be called in frequently to take a good look at those systems to make sure that some crack in the strong cryptosecurity
edifice the NSA cryptographers think they have erected doesn't exist and that such a crack can not be widened.

William F. Friedman  
WILLIAM F. FRIEDMAN
TO: Director
National Security Agency
Washington 25, D.C.
Attention: Contracting Officer, NSA

In accordance with Article II (Delivery) on Contract No. DA49-170-sc-1739, File No. 69-NSA-55-56-NSA/PR-279, this invoice is submitted for payment

........ 34,000.00

WILLIAM F. FRIEDMAN

CERTIFICATE

I certify that the above bill is correct and just and that payment therefor has not been received.

WILLIAM F. FRIEDMAN
Director  
National Security Agency  
Washington 25, D.C.  
Attn: Chief, Central Office of Reference  

Sir:

Reference is made to Contract No. DA-49-170-SC-1739, File No. 59-354-95,  
56-KA/PS-270, which was entered into as of 1 August 1955 by and between the  
United States of America and the undersigned and which was modified only as  
to date of delivery of all the items called for under said contract. In  
accordance with the provisions of Article II (Delivery) of said contract, I  
am sending you herewith (a) approximately 150 catalog cards supplementary to  
those sent under Project 1, Article 1, paragraph b(1) of said contract; and  
(b) the completed manuscript called for under Project 3 of the same Article,  
viz., a special report originally tentatively entitled The Cryptological  
Background of the Various Official Investigations into the Attack on Pearl  
Harbor. The said tentative title of the item called for under Project 3 is  
now not quite suitable and I have deemed it advisable to amend it by prefacing  
it with the words "Certain aspects of 'Magic'"; making the complete title  
"Certain aspects of 'Magic' in the Cryptological Background of the Various  
Official Investigations into the Attack on Pearl Harbor."

I have adopted a rather informal style which may perhaps make the brochure  
more interesting. Several ideas therein cast a new light, I think, on certain  
aspects of the investigations and the questions raised by a category of historians who have much to say about the attack on Pearl Harbor and who are known as "revisionists." My brochure may therefore be useful in a study  
of the Pearl Harbor disaster, especially for historians who take a more  
realistic view of what happened and why the U.S. forces in Hawaii were  
cought by surprise. It is perhaps unfortunate that I had to use a small  
amount of material which is still classified and therefore the brochure as  
a whole has had to be classified.

I realize only too well that the present brochure can certainly be  
 Improved by further work but the time limit—already twice extended—permits  
of no additional delay in the delivery of this item. Let it be considered,  
in the words of the previous Director of the National Security Agency, as  
"Model No. 1."

Sincerely,

WILLIAM F. FREEDMAN

Enclosures:

a/8
Dec 5 - about 10:00 Noyes called Sedghe t and said "word is in." Fujio has fled to Tokyo over the phone. Noyes said it was one that means "Tokyo" - not "Japan and U.S. acc to Sedghe's recell.

Noyes called again by Sedghe but couldn't get the word. Sedghe said he went to Noyes. Brattin-Knows said it was out.

Dec 4 - War Com Bld

Tony Muto - Rep of 7th Dist - Fox. Told Sedghe - Chinese rep V - Japs would continue neg action to strike.

Sedghe never heard warning of warnings from Australian govt. renewal of job hunt.
ORGANIZED RESERVES
HEADQUARTERS WASHINGTON UNITS
Rooms 3602-18 Munitions Bldg.
Washington, D. C.

November 20, 1934.

SUBJECT: Examination

TO: Major William F. Friedman, Sig-Res.,
Office of the Chief Signal Officer,
War Department, Washington, D. C.

1. Under date of October 16, 1934, you stated in a
1st Indorsement to this Headquarters that pressure of work
had prevented completion of the thesis required in connection
with your examination for promotion, and that the completed
thesis may be expected about October 31st. To date same has
not been received.

2. Information is requested as to the status of this
matter.

W. W. McCALMON,
Colonel, Infantry,
Senior Instructor.

OCSigO 201-Friedman, W.F.
Major, Sig-Res. 1st Ind.

Friedman, W.F., Major, Sig-Res., O.SigO, Washington, D. C., November
24, 1934 - To: Senior Instructor, Organized Reserves, Washington
Units, Rooms 3602-13 Munitions Building, Washington, D. C.

The required thesis in duplicate is being submitted
herewith.

William F. Friedman,
Major, Signal Reserve.

Attached:
Thesis in duplicate.

Approved for Release by NSA on 07-16-2014 pursuant to E.O. 13526
The Duties of the Officer-in-Charge of the Signal Intelligence Service, G3Q.

Thesis submitted by William P. Friedman, Major, Sig-Ras., in connection with examination for Certificate of Capacity for promotion to the grade of Lieutenant Colonel.

<table>
<thead>
<tr>
<th>Paragraph</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introductory note as to sources of data</td>
</tr>
<tr>
<td>Basic authority for Signal Intelligence Service</td>
</tr>
<tr>
<td>Position occupied by Signal Intelligence Service in the G3Q Signal Service</td>
</tr>
<tr>
<td>Relations with Radio Intelligence Company, G3Q Signal Service</td>
</tr>
<tr>
<td>Organization of the G3Q Signal Intelligence Service</td>
</tr>
<tr>
<td>Functions of administrative section</td>
</tr>
<tr>
<td>Functions of enemy documents section</td>
</tr>
<tr>
<td>Functions of cryptographic identification section</td>
</tr>
<tr>
<td>Functions of communications security section</td>
</tr>
<tr>
<td>Functions of secret inks section</td>
</tr>
<tr>
<td>Functions of code and cipher compilation section</td>
</tr>
<tr>
<td>Functions of code and cipher solution section</td>
</tr>
<tr>
<td>Relations with other branches of Signal Intelligence Service</td>
</tr>
<tr>
<td>Duties of the officer-in-charge of the G3Q Signal Intelligence Service</td>
</tr>
</tbody>
</table>

Appendix I

1. Introductory note as to sources of data - 5. In preparing this thesis the writer has had access to the files of the Chief Signal Officer, including those of current as well as historical information. Among many other documents, the following may be mentioned:

   (1) Tables of Organization, Signal Intelligence Service
   (2) Technical Papers of the Signal Intelligence Section,
       War Plans and Training Division, Office of the Chief
       Signal Officer.
   (3) Army Regulations pertaining to codes and ciphers.
   (4) Letters pertaining to the work of the Signal Intelligence Service.

2. In addition, files pertaining to the World War, as contained in the World War Records Division of The Adjutant General, have also been studied. Among the latter were the following:

   (1) Final report of the Officer-in-Charge of the Radio
       Intelligence Section, General Staff, G3Q (G-2 - A6)
   (2) Final report of the Code Solving Subsection (G-2 - A5)
   (3) Final report of the Cipher Solving Subsection (G-2 - A5)
   (4) Final report of the Cryptographic-subsection (G-2 - A5)
   (5) Final report of the Security Subsection (G-2 - A5)
   (6) Final report of the Administrative Subsection (G-2 - A5)
   (7) Final report of the Main Intelligence Office, Rear 1st Fl., N.Y.
2. Basic authority for the Signal Intelligence Service. — a. Basic authority for the establishment of the Signal Intelligence Service is given in AR 105-29, March 15, 1933, as amended by Changes No. 1, August 21, 1934.

Par. 2 & thereof now reads as follows:

"2. Duties of the Chief Signal Officer. — In addition to such other duties as may be prescribed, the Chief Signal Officer will have immediate charge, under the direction of the Secretary of War, of the following:

* * * * *

b. The preparation, publication, revision, storage, accounting, and distribution of all codes and ciphers required by the Army, and in time of war the interception of enemy radio and wire traffic, the geocentric location of enemy radio stations, the solution of intercepted enemy code and cipher messages, and laboratory arrangements for the employment and detection of secret inks.

* * * * *

3. Unit signal officers. — a. A chief signal officer will be detailed for every expeditionary force and a Signal Corps officer as unit signal officer will normally be detailed for each corps area and every tactical unit larger than a brigade containing Signal Corps troops. When no unit signal officer is assigned, the Signal Corps officer present for duty with the command will act as such. The unit signal officer will be a member of the staff of his commanding officer. He will be charged, under the direction of his commanding officer, with the command, in so far as relates to operations, of signal troops not assigned or attached to subordinate units. The unit signal officer is also charged with specific duties as follows:

* * * * *

(3) Preparation, publication, storage, accounting, and distribution of codes and ciphers.

* * * * *

(3) Supervision of the installation, maintenance, and operation of the signal communications system, including the message center, of the unit.

(7) Supervision of such activities pertaining to the meteorological, signal intelligence, pigeon, and photographic services as affect the unit."

* * * * *

b. Based upon the foregoing authority, we may now study the following extracts from a directive given the Chief Signal Officer by the Secretary of War, in a letter dated April 27, 1930, dealing specifically with the Signal Intelligence Service:

"5. Upon mobilization the various activities of this service will operate at the following headquarters:

- 2 -
a. Under the War Department:

(1) The preparation of all means of secret communication employed by the Army in peace and war including secret inks, except that, upon its organization, G\&S will begin the preparation of field codes and ciphers required for current replacement for subordinate units.

(2) The interception of enemy communications by electrical means, including the necessary goniometric work incident thereto.

(3) The detection and solution of secret or disguised enemy communications including those written in code, cipher, secret ink or those employing other means for disguise.

b. At General Headquarters:

(1) The preparation of field codes and ciphers for employment by subordinate units to replace those previously prepared under the War Department during peace time.

(2) The interception of enemy communications by electrical means.

(3) The location of enemy radio transmitting stations by goniometric means.

(4) The detection and solution of secret or disguised enemy communications including those written in code, cipher, secret ink or those employing other means for disguise.

c. At Headquarters of Field Forces:

(1) The interception of enemy communications by electrical means.

(2) The location of enemy radio transmitting stations by goniometric means.

(3) The solution of intercepted enemy code or cipher messages by the assistance of cipher keys and solved codes as furnished by the service at General Headquarters.

3. Position occupied by the Signal Intelligence Service in the GHQ Signal Service. — a. Coming now directly to the manner in which the Signal Intelligence Service fits into the organization of the GHQ Signal Service, we find a graphic picture of the latter organization in T\O 507-W shown in Appendix 1.
4. The Radio Intelligence Company, GHQ Signal Service, as given under a and b above are performed by a similarly organized Radio Intelligence Company, Army Signal Service; the data obtained are furnished to the Signal Intelligence Service, Headquarters Army Signal Service. This must be mentioned for reasons which will become apparent subsequently.

5. Organization of the GHQ Signal Intelligence Service. — a. Coming now directly to the GHQ Signal Intelligence Service, we find a graphic picture of its organization in T/0 507-8, shown in Appendix I. As shown in the table, this service consists of the following sections:

(1) Administrative
(2) Army documents
(3) Geostatic identification
(4) Communications security
(5) Secret links
(6) Cops and other compilation
(7) Cops and higher compilation
b. Since T/O 509-W was approved the Signal Corps has been assigned the additional responsibilities of publishing, storing, distributing, and accounting of cryptographic publications. Although these added duties can be allocated to one of the sections of the code and cipher compilation section, it will be noted, nevertheless, that the additional work thus imposed upon the GS Signal Intelligence Service is of very great importance and will necessitate some expansion of the present authorized organization.

2. Each of the foregoing sections will be taken up in turn, the duties set forth, the relations with other sections, and all details connected with its efficient operation discussed.

6. Functions of administrative section. - 2. The administrative section comprises the following subsections, the duties of which will be described presently:

1. Headquarters subsection
2. Correspondence subsection
3. Production and tabulating machinery subsection
4. Files subsection
5. Communications subsection
6. Guard subsection
7. Liaison subsection
8. Library and current information subsection

2. The headquarters subsection handles all matters relating to the general policies of the service, the obtaining and administration of personnel, quarters, office equipment and supplies for the service. The officer-in-charge of the GS Signal Intelligence Service maintains his office in this subsection.

3. The correspondence subsection comprises the necessary stenographic and typing personnel for conducting the large volume of correspondence of the whole GS Signal Intelligence Service. It is deemed best to have a fairly large stenographic and typing pool so that the work may be centralized.

4. The reproduction and tabulating machinery subsection makes copies of texts, tables, etc., required for the various sections. This will include micrographing, multigraphing, and other methods of reproducing copies. In addition, there will be needed certain machines usually employed for stenographic purposes, but easily adaptable to cryptographic and cryptanalytic work. The use of such machines very greatly reduces the amount of time and labor involved in code compilation and in making statistical studies in cryptanalytic work.
6. The liaison subsection is a central agency for maintaining the files and records of the entire G-2 Signal Intelligence Service.

7. The communications subsection may have direct telegraph wires to Army Signal Intelligence Service headquarters, to outlying intercept stations, and to other places (for example, Navy Signal Intelligence Service headquarters), for the purpose of avoiding all delays in the transmission and receipt of messages relating strictly to the technical work of this service, especially that of the solution section, where time is of the utmost importance.

8. The guard subsection has supervision of the special sentries assigned to patrol the quarters occupied by the Signal Intelligence Service at all hours of the day and night. It is felt that these special guards are necessary in order to prevent the surreptitious operation of enemy agents in the vicinity of the quarters where most of the vitally secret work is carried on.

9. The liaison subsection maintains the necessary contacts with the Signal Intelligence Services of Field Armies, with other arms, with branches of the General Staff, with the Navy Signal Intelligence Service in case of joint action, and with the Signal Intelligence Services of Allied Governments, if any. In other words, the section serves as a central agency for coordination of work with other Signal Intelligence organizations, or with other agencies concerned in the results obtained.

10. The library and current information subsection maintains a small but fairly comprehensive library of books having a bearing on signal intelligence activities and of books likely to be necessary as sources of information for particular use of the solution section. Files of certain newspapers may be necessary if they are not readily accessible at G-2. Reference books of special types are also required for cryptanalytic work that may not be available at the library of G-2.

11. Functions of enemy documents section. — This section is the depository for documents relating to the signal service of the enemy in all its phases, but primarily as regards his signal intelligence organization, its agencies, operations, systems, and devices.
A small unit of translators is essential if the language of the enemy is different from our own. These persons must have some technical knowledge in signal intelligence in order to translate properly such documents in form suitable for our ready use.

The translators may also be called upon to assist personnel of the code and cipher solution section and for this reason also they must have a certain amount of training in cryptanalysis.

The importance of rapid forwarding of captured documents such as codes, cipher keys, files of cryptographed messages with their translations, to the Signal Intelligence Service is apparent. For this reason a special subsection is deemed advisable, the duties of which are to see that no time will be lost in bringing back captured documents and placing them in proper form for study by various interested personnel of the Signal Intelligence Service.

Functions of geoniometric identification section. The work of this section is primarily of interest to the Battle Order Section of C-2, and to the code and cipher solution section of the Signal Intelligence Service. It consists in enabling the latter to sort intercepted messages properly according to the enemy units from which they emanate and for which they are intended, since tactical messages rarely carry addresses and signatures in plain text, and externally carry few indications from which it may be determined whether two messages are in the same code, in the same cryptographic system, or in the same key.

This section works in close liaison with the Radio Intelligence Company assigned to GIN. The latter intercepts the messages and records on them the location of the transmitting stations, as found by intersection from the radio-compass bearings taken on the emitted waves. The geoniometric identification section records the locations and call signs of these stations on a suitable map, and from a study of intercommunicating stations, establishes the probable enemy radio nets. These nets are then analyzed with the point of view of identifying the units which the transmitting and receiving radio stations serve and this in turn, by noting the groupings and intercommunicating stations form, furnish valuable information concerning enemy order of battle.

---
6. Having identified the units in this manner, it is then possible to indicate on the intercepted messages the unit from which and to which they are coming and going, their location, the larger units to which they belong, etc. Thus, the messages can be sorted so as to isolate messages in the same cryptographic system, key, or in the same code. This is, of course, of primary importance to, and constitutes an essential preliminary step in solving the messages.

7. From the point of view of furnishing information concerning enemy order of battle, the work of this section is also of great value, since this information may be obtained at comparatively little expense, without entailing the loss of lives, and, moreover, in contrast to similar information obtained from prisoners or spies, is not subject to psychological, or purposive distortion of the facts.

9. Functions of communications security section. - 2. The work of this section is exclusively that of furnishing data for the supervision of our own signal communications from the point of view of their protection and the maintenance of security and secrecy in signal communication.

b. Its duties include the following:

(1) Study of our own messages to insure that the regulations governing cryptographic security are being observed. This involves analyzing radio messages transmitted by our own forces. The messages for this purpose are obtained by the Radio Intelligence Company assigned to G13 and are forwarded to the Communications Security Section of the Signal Intelligence Service. The latter, of course, has the codes or ciphers and deconstructs the messages, devoting special attention to violations of the regulations essential to cryptographic security.

(2) Switchboard facilities are provided so that personnel of this section may cut in on important telephone lines and listen in on conversations for the purpose of noting inadvertent or missed errors. Particular attention is devoted to listening for the repetition of unit designations, plans of operation, troop movements and the like. It must be assumed that the enemy will attempt to intercept
and record such conversations by placing agents at strategic points suitable for this purpose. Direct tapping of the telephone wires is, of course, not necessary because by suitable apparatus the electrical currents may be detected by induction, amplified, and led away to a place where the conversations may be recorded with ease.

d. The personnel of this section should include a stenographer of considerable ability, so as to be able to record the conversations as rapidly as they are spoken, otherwise the evidence obtained might not be considered valid. All the listening-in personnel must be carefully selected for their discretion and integrity.

d. When serious violations are observed, one of two procedures may be followed. Under the first procedure a letter may be drafted, calling attention to the irregularities, and forwarded through the Adjutant General to the commanding officer of the organization concerned. If the violations continue and are of a serious nature, an inquiry may be held by the Inspector General's Department. Under the other procedure, it has been contemplated that an officer to be known as the Communications Security Officer would be designated in each large unit, whose duties would include the supervision of communications from the point of view of security. If this is the case, the liaison between the GH Communications Security Section and the unit security officer would be more direct. This would expedite the correction of irregularities leading to insecurity in communication by radio or other means.

10. Functions of secret inks section - a. This section maintains and operates a laboratory for the preparation and detection of invisible writing fluids, and for the detection of other means of transmitting information to elude censorship, as for example, microscopical writing.

b. The subsection for preparation of secret inks functions only intermittently, when the G-2 section of GH desires to send out secret agents into enemy territory and must provide these agents with means for sending back information in a form that will escape detection by enemy censorship.

c. The subsection for detection functions continuously and is furnished its material by the censors' bureau. Documents suspected of containing invisible writing are passed through the various chemical tests, and if secret
writing is discovered the results of the examination are forwarded to G-2 for action.

4. This section works in closest liaison with the censorship agency, and also with the larger laboratory at the War Department, where better facilities and more personnel are available for research.

II. Functions of code and cipher compilation section. — 4. This section comprises the following subsections, the duties of which will be briefly discussed in turn:

1. Headquarters subsection
2. Code compilation subsection
3. Cipher compilation subsection
4. Publication subsection
5. Storage subsection
6. Distribution subsection
7. Accounting subsection

b. The headquarters subsection has charge of the administrative details relative to assignment of work to personnel, the use of the equipment, and the issue of supplies to the individual members of the section. All correspondence pertaining to the production, distribution, and accounting of codes and ciphers is initiated in the subsections and then passed through this office before going to the administrative section of the Signal Intelligence Service for signature and transmittal.

g. The code compilation subsection compiles new editions of authorized codes, as are required by field forces, principally for the Division Field Code, Air-Ground Liaison Code, Radio Service Code, and War Coordinate Code. Special codes adapted for special usage or entirely new codes the need for which is determined by the Commanding General, GHQ may be compiled.

§. The cipher compilation subsection prepares cipher tables, cipher keys, or cipher alphabets as may be required for use in connection with the various authorized codes, cipher systems and devices. It also has as one of its responsibilities the technical supervision and coordination of such automatic cryptographic machinery as may be employed for short intercommunication among the highest headquarters of field forces.

- 10 -
9. The publication subsection has charge of the details pertaining to
the printing and physical reproduction of copies of codes, cipher,
tables, and cipher keys. If practicable, it should have facilities for
printing or lithographic reproduction entirely under its own control, in
order that proper safeguards may be established over this phase of secret
communication facilities. However, if this is not practicable the printing
and reproduction facilities of the Adjutant General, G-2, or of the Engineer
Reproduction Plant, G-2, will have to be employed. The subsection is also
responsible for all proofreading of galley and page proofs.

10. The storage subsection is the receiving office for printed crypto-
graphic publications and is responsible for their safeguarding while in
storage. It is necessary to provide it with suitable storage facilities,
safe being preferable, and also with armed sentries to patrol the quarters
at all hours during the day and night.

11. The code and cipher compilation section will make the most use of
the automatic machinery referred to under par. 6 g. Without such machinery
the section could either have to have much more personnel or else codes would
have to be replaced less frequently.

12. Functions of code and cipher solution section. - a. This section
comprises the following subsections:

(1) Headquarters subsection
(2) Distribution and records subsection
(3) Codes subsection
(4) Ciphers subsection
(5) Research and training subsection

b. The headquarters subsection has charge of the administrative details
relative to the assignment of work to the personnel of the section, the use of
the equipment, and the issue of supplies to the individual members of the
section. All correspondence pertaining to the work of the section, material
furnished it for solution, the results accomplished, and liaison with other
branches and agencies pass through this office before going to the Administra-
tive Section for signature and transmittal. It also prepares daily, weekly,
or monthly reports on cryptanalytic activities, which reports are intended
for the G-2 section of the G-2 staff and must be forwarded to that section for
evaluation, coordination and distribution to all concerned. -
g. The distribution and records subsection distributes manuscript sheets, copies of messages, documents, etc., as received from the reproduction subsection of the Administrative Section direct to the personnel working upon the particular code or cipher concerned. Its personnel also are employed in indexing, tabulating, making frequency studies, etc., for the cryptanalytic staff.

d. The codes subsection studies and solves enemy code systems, attempts to reconstruct the codes as completely as possible, and decodes enemy messages so far as the reconstruction of the codes up to that moment will permit.

e. The ciphers subsection does the same type of work except on cipher systems.

f. The research and training subsection has the following duties:

1. To investigate such new code and cipher systems, apparatus, and devices as are submitted to the Signal Officer, G3s, for consideration for use by field forces.

2. To conduct a school for the training of enlisted and officer personnel assigned to duty in the Signal Intelligence Service of G3s or Army. Such training will be essential for personnel obtained from sources other than the Chief Signal Officer because no other agency exists in the military service for training in signal intelligence activities.

13. Relations with other branches of Signal Intelligence Service. — a. The G3s Signal Intelligence Service must maintain close liaison with the following other branches of the Signal Intelligence Service of the military establishment:

1. Army Signal Intelligence Service. The signal intelligence service at the headquarters of each field army serves as a sort of forward echelon of the G3s Signal Intelligence Service. Its personnel are trained only so far as will enable them to decipher and decode enemy messages for which the keys have been worked out by G3s Signal Intelligence Service. The purpose here is to permit of speed in utilizing the results that may be obtained from solutions of enemy messages intercepted within the radius of action of the field army.
At the same time, the Army Signal Intelligence serves as a source of material for work by GHQ Signal Intelligence Service, since the messages which are intercepted by the Radio Intelligence Company assigned to Army and which cannot be solved by Army Signal Intelligence Service are forwarded for solution to GHQ Signal Intelligence Service. The officer-in-charge of Army Signal Intelligence Service should have had adequate training and experience in the GHQ Signal Intelligence Service. His assistants do not require such thorough training, but obviously the more they have the better will be their work.

(2) Far Department Signal Intelligence Service. The largest unit of the Signal Intelligence Service and the one best equipped to work with the more complicated enemy codes and ciphers should be located at the Far Department in Washington. Here the non-military codes and ciphers of the enemy government are studied, as well as the codes and ciphers of enemy commercial houses, agents, etc. It may be that the GHQ Signal Intelligence Service is in a better position to intercept such material than is the Far Department Signal Intelligence Service, in which case the former should spend no time trying to solve this non-military traffic but should merely forward it to Washington. On the other hand, the enemy's field ciphers may be so complicated as to be beyond the ability of personnel at GHQ Signal Intelligence Service, in which case the Far Department Signal Intelligence Service may be called upon for cooperation and assistance.

(3) Corps Area and Department Signal Intelligence Services. If branches of the Signal Intelligence Service are established at the headquarters of corps areas and departments, liaison may be necessary between them and GHQ Signal Intelligence Service, for purposes of coordination, cooperation, and avoidance of duplication of effort.
b. It must also act in close liaison with the following:

(1) Censorship representative, GHQ. The censorship bureau will undoubtedly have offices in the Theater of Operations. Matters requiring cooperation between the Signal Intelligence Service and Censorship authorities in this region will require close liaison.

(2) Navy Signal Intelligence Service. The Theater of Operations may be located in such an area that direct liaison with Navy Signal Intelligence Service Afloat or Ashore is more conducive to good cooperation with GHQ Signal Intelligence Service than indirect liaison through the War Department Signal Intelligence Service, such direct contact should be established.

(3) Signal Intelligence Services of allied governments. During the World War, the liaison that existed between the Radio Intelligence Section, CG-2, GHQ, AEF, and the same service of French GHQ and British GHQ was most conducive to cooperation and elimination of duplication of effort. In case our government is engaged in a war conducted with Allies against a common enemy, such liaison may again be essential.

c. It will be seen from the foregoing that the activities of the Liaison Subsection of the Administrative Section, GHQ Signal Intelligence Service (par. 64 (7) above) are quite important and necessary for achieving the best results possible from coordinated efforts to solve all kinds of enemy communications.


a. It is the responsibility of the officer-in-charge of the GHQ Signal Service to administer the service under his charge in such a way that the functions of each section of his office, as outlined above, are efficiently conducted and that the service as a whole fulfills the mission assigned to it. He cannot be expected to be an expert cryptographer or an accomplished cryptanalyst, but he should know enough about these subjects to recognize the limitations that abound in practical work in these fields. He must realize first of all that the personnel assigned to him or selected by him are assigned to possess basic technical qualifications for the work and that if success does not come their efforts or if it seems to him to come only too
slowly, this is inherent in the work itself; "supermind performances" are not the forte of cryptanalytic personnel, popular concepts to the contrary notwithstanding. It cannot be too strongly emphasized that cryptanalytic studies require a great deal of patience on the part of its working personnel; on the part of its directing and administrative personnel a similar degree of patience must be forthcoming. It is only rarely that spectacular situations and successes arise in the course of the work.

2. The last statement leads quite directly to a point which is touched upon with a certain amount of hesitancy but which nevertheless must be mentioned. As said before, signal intelligence is a specialty and its successes are rarely of a spectacular nature. They are, in this respect, quite different from the notable achievements which are much more frequently brought to light on the battlefield by brilliant tactics, resolute action, courage and fortitude. To those who have the good fortune to succeed on the battlefield, recognition and advancement come quickly, and this is of material importance toward the establishment and maintenance of a high stage of morale. But the successes of signal intelligence personnel, even when they do come (and they come only infrequently, very slowly, and most often as the result of long, hard labor), must usually be kept secret or, at the least, confidential. Consequently, those successes never can meet with popular acclaim and never can be accorded even recognition until long afterward. If, under these circumstances, promotion and advancement come more slowly than they do in other fields of action, the result is apt to be detrimental to the morale of the plodders in the signal intelligence field. It therefore is incumbent upon the officer-in-charge of the signal intelligence service to see that his personnel in accorded recognition for efficient, conscientious work in the same degree and with the same benefits as is accorded deserving personnel in the combat zone.

2. Finally, it is extremely important that the officer-in-charge realize that a vital factor in attaining success in signal intelligence work is the fostering of a competitive spirit among all personnel concerned but at the same time repressing to the utmost spirit of professional jealousy, and my
attempts to deprive others of credit due for good work, merely for the sake of personal advancement of the offender. The officer-in-charge of each branch of the Signal Intelligence Service, wherever located, must be constantly on guard to prevent such destructive forces from gaining a foothold among his subordinates for the good and sufficient reason, aside from the one of fair play, that whereas the spirit of competition on a purely scientific basis is conducive to the production of results, will spur on his subordinates to do their very best, and will bring about a good state of morale, the corroding spirit of professional jealousy based merely upon avidity for personal distinction and advancement will not only disrupt a good organization but will prevent the establishment and maintenance of real cooperation. It may be stated that in signal intelligence work, especially in that of cryptanalysis, cooperation and coordinated effort are absolutely essential. The efforts of even a good many individuals, if each works alone, will avail very little; only good teamwork will produce results and will bring success in the assigned mission.
The CHAIRMAN opened discussion on this item by inviting comments by the Chairman of the U.S. Delegation, Mr. Friedman.

MR. FRIEDMAN expressed his opinion that the conference report spoke pretty well for itself, and added that he thought the report should be approved as rendered. At a meeting on 6 July he said the Executive Committee approved the conclusions and recommendations of the report with exception of the CIA member who reserved his position on one or two points.

CAPTAIN TAYLOR replied that the CIA position had been circulated to the Members of the Board as USCIB 23/69.

MR. FRIEDMAN went on to say that there are some loose ends remaining to be tied up by a sub-committee or an ad hoc committee. He suggested that an ad hoc committee composed of some members of the U.S. delegation constitute such a group. He added that specific points to be worked out are the preparation of certain appendices and schedules of the communications security technical details, for which a small group should be set up in Washington. Also he said there were certain other matters to be considered, such as what might be done with regard to improvements in commercial machines which might interfere with our future work. He further stated that he was prepared to try to answer questions that might be raised by Members of the Board.

The CHAIRMAN suggested that USCIB 23/69 be taken up since some question had been raised by the CIA representative, and asked Mr. if he would like to speak on that.
The CHAIRMAN said he thought there was some strength in the CIA position and that until negotiations have been concluded with the French it will be difficult to tell just what the best procedure would be. He inquired if it would be agreeable to approve the report and to have another look at the question of the best method of proceeding with the other NATO powers, after we conclude with the French. He asked Mr. Friedman if he had any comment on that point.

MR. FRIEDMAN said he thought the important thing to do is to start and see how the French react, and if the French react favorably we could then consider the other countries one by one.

The CHAIRMAN said that CIA would not be estopped by this action from raising the question of other possible means of procedure.

MR. KEAY said he thought that was inherent in the report and he believed that the approach to the French was on the basis of further NATO approaches.

MR. FRIEDMAN said the French had already approached with the statement that they were very much concerned about the insecurity of the communications of certain NATO countries.

The CHAIRMAN said he thought the report is approved unless there was any other comment.

CAPTAIN ROEDER said that the Navy approved the report. He added that they felt that since five years have elapsed since the problem was first presented that it might be desirable to agree at this time to vote a deadline on when the problem would be re-examined rather than let it go on for another few years. He suggested the time limit of one year if that was agreeable and added that the problem could then be re-examined to see what progress has been made.

The CHAIRMAN inquired of Captain Taylor if there was any objection to Captain Roeder's proposal.
CAPTAIN TAYLOR replied in the negative.

The CHAIRMAN then stated the proposal was approved.

The CHAIRMAN stated that the first matter for implementation was the appointment of the cognizant U.S. authority. He asked for suggestions.

MR. FRIEDMAN stated that in the deliberations of the conference, the conferees had originally definitely suggested that the Department of State and the Foreign Office be made cognizant authorities for making an approach to the French. He added that the specific reference was taken out at the suggestion of the CIA delegate who thought it was presumptuous of the conference to try to tell LSIB and USCIB whom to appoint.

MR. suggested the Department of State.

MR. ARMSTRONG said that the State Department was perfectly willing to undertake it on the part of USCIB. He added that he assumed that LSIB would appoint the Foreign Office. He added that he understood this to be the case and that the actual person to approach in the Foreign Office had been agreed in the early stages.

MR. FRIEDMAN agreed and added that it was Mr. Parodi.

The CHAIRMAN inquired if there were any other nominations and added that the job requires a high degree of diplomacy and skill. He said he would look to the State Department for that diplomacy. He added that he hoped Mr. Armstrong would take a personal interest in the matter.

MR. ARMSTRONG said he would indeed. He said he would see that the Ambassador, upon whom we would have to rely very heavily, would be fully briefed on the matter as to how and when, etc.

The CHAIRMAN inquired if the matter would be handled in Paris or London.

MR. ARMSTRONG replied that Paris would be best because it would prevent the French from having to communicate and it could be done with less attention drawn to it in Paris than London.

The CHAIRMAN stated that that would mean getting into higher diplomatic circles.

MR. ARMSTRONG said he thought we should start at the top. The first approach, he said, presumably would be to the Minister who would raise it in the inner-Cabinet level forthwith for approval per se.
The CHAIRMAN stated that if there were no other nominations, the designation of the State Department as the Cognizant U.S. Authority is approved. He pointed out to Mr. Friedman that he thought the U.S. element of the Combined Working Group would be the State Department and technicians from NSA.

MR. ARMSTRONG stated that with respect to paragraph 32b, the State Department would have to rely very heavily upon NSA and the others.

The CHAIRMAN noted that paragraph 32e stated that "Agreement on the terms and composition of the Combined Working Group to be set up in Washington to facilitate coordination of this action" is required.

MR. FRIEDMAN said that was referred to in the last sentence of paragraph 24. He then proceeded to read this sentence, and added that he assumed that the Group would assist the State Department and the U.S. members of this Combined Working Group.

The CHAIRMAN said it could be left up to the Cognizant U.S. Authorities to see that the Combined Working Group is set up.

MR. FRIEDMAN said he thought that many of these details could be worked out by the Executive Committee.

CAPTAIN TAYLOR asked if it was the sense of the Board that the initial action on the Combined Working Group will be referred to the Executive Committee by the Cognizant U.S. Authorities.

MR. ARMSTRONG replied that it was his understanding that it would be.

The CHAIRMAN stated that the above action was approved.

The CHAIRMAN suggested that the Executive Secretary advise the British of the action taken at this meeting.

CAPTAIN TAYLOR said he would prepare a suitable document.

DECISION: (10 July 1953) USCIB approved the final report and papers of the US/UK conference on Allied (NATO) communications security as a basis for negotiations with the U.K. and agreed that U.K. authorities would be so notified.

It was agreed, further, that:

(1) The Department of State would be the "Cognizant U.S. Authority".
(2) As "Cognizant U.S. Authority" the Department of State would take action as necessary and appropriate to refer to the Executive Committee the problem of initial action in the establishment of the Combined Working Group in Washington.

(3) No member would be estopped from raising the question of desirability of using other than NATO channels after negotiations with the French have been undertaken.

(4) That this problem will be reviewed by the Board at approximately one year from date.
From the Files of the Special Consultant - Friedman
Final Version of Lecture No. 1 - 24 pages (carbon copy), No. 2 - 24 pages, No. 3 - 19 pages and 1 page of notes. UNCLASSIFIED
The objective of this series of lectures is to create an awareness of the background, development, and manner of employment of a science that is the basis of a vital military offensive and defensive weapon known as CRYPTOLOGY, a word that comes from the Greek kryptos, meaning secret or hidden, plus logos, meaning knowledge or learning. Cryptology will be specifically defined a little later; at the moment however, I'm sure you know that it has to do with secret communications.

Let me say at the outset of these lectures that I may from time to time touch upon matters which are perhaps essentially peripheral or even irrelevant to the main issues of cryptology, and if a defense is needed for such occasional browsing along the by-ways of the subject while travelling along the main highways of the science, I'll say that long preoccupation with any field of knowledge begets a curiosity the satisfaction of which is what distinguishes the dedicated professional from the person who merely works just to gain a livelihood in whatever field he happens to find himself a job. That's not much fun, I'm afraid. By the way, a British writer, James Agate, defines a professional as the man who can do his job even when he doesn't feel like doing it; an amateur, as a man who can't do his job even when he does feel like doing it. This is pretty tough on the gifted amateur and I for one won't go all the way with Agate's definition. There are plenty of instances where gifted amateurs have done and discovered things to the chagrin and red-facedness of the professionals.
Coming back now to the main thoroughfare after the foregoing brief
jaunt along a by-way, I may well begin by telling you that the science of
cryptology has not always been regarded as a vital military offensive and
defensive weapon, or even as a weapon in the first place. Here I am
reminded of a story in a very old book on cryptography. The story is
probably apocryphal, but it's a bit amusing, and I give it for what it's
worth.

It seems that about two thousand years ago there lived a Persian
queen named Semiramis, who took an active interest in cryptology. Whether
it was because of that interest or for other unnatural reasons, such as
curiosity about what people call "secrets", the record doesn't say, but
anyhow it is reported that she met with an untimely death. Presumably
she went to Heaven, or perhaps to the other place, but she left instructions
that her earthly remains were to be placed in a golden sarcophagus within
an imposing mausoleum on the outside of which, on its front stone wall,
there was to be graven a message, saying:

Stay, weary traveller!
If thou art footsore, hungry, or in need of money--
Unlock the riddle of the cipher graven below,
And you will be led to riches beyond all dreams of avarice!

Below this curious inscription was a cryptogram, a jumble of letters
without meaning or even pronounceability. For several hundred years the
possibility of sudden wealth served as a lure to many experts who tried
very hard to decipher the cryptogram. They were all without success, until
one day there appeared on the scene a long-haired, be-whiskered, and be-
spectacled savant who, after working at the project for a considerable
length of time, solved the cipher, which gave him detailed instructions
for finding a secret entry into the tomb. When he got inside, he found
an instruction to open the sarcophagus, but he had to solve several more
cryptograms the last one of which may have involved finding the correct
combination to a 5-tumbler combination lock— who knows? Well, he solved
that one too, after a lot of work, and this enabled him to open the
sarcophagus, inside which he found a box. In the box was a message, this
time in plain language, and this is what it said:

O, thou vile and insatiable monster! To disturb these poor bones!
If thou had'st learned something more useful than the art of
deciphering,
Thou would'st not be footsore, hungry, or in need of money!

I'm frank to confess that many times during my 45-year preoccupation
with cryptology, and generally near the middle and the end of each month, I
felt that good old Queen Semiramis knew what she was talking about. How-
ever, earning money is only a part of the recompense for working in the
cryptologic field, and I hope that most of you will find out sooner or later
what some of these other recompenses are and what they can mean to you.

If Queen Semiramis thought there are other things to learn that are
more useful than the art of deciphering, I suppose we'd have to agree, but
we are warranted in saying, at least, that there isn't any question about
the importance of the role that cryptology plays in modern times: all of

-3-
us are influenced and affected by it as I hope to show you in a few minutes.

I will begin by reading from a source which you'll all recognize--TIME magazine, the issue of 17 December 1945. I will preface the reading by reminding you that by that date World War II was all over--or at least V-E and V-J days had been celebrated some months before. Some of you may be old enough to remember very clearly the loud clamor on the part of certain vociferous members of Congress who had for years been insisting upon learning the reasons why we had been caught by surprise in such a disastrous defeat as the Japanese had inflicted upon us at Pearl. This clamor had to be met, for these Congressmen contended that the truth could no longer be hushed up or held back because of an alleged continuing need for military secrecy, as claimed by the Administration and by many Democratic senators and representatives. The war was over--wasn't it?--Republican senators and representatives insisted. There had been investigations--a half dozen of them, but all except one were TOP SECRET. The Republicans wanted, and at last they got what they desired--a grand finale: Joint Congressional Investigation which would all be completely open to the public. No more secrets!

It was spectacular! Not only did the Congressional Inquiry bring into the open every detail and exhibit uncovered by its own lengthy hearings, but it also disclosed to America and to the whole world everything that had been said and shown at all the previous Army and Navy investigations. Most of the
information that was thus disclosed had been and much of it was then still TOP SECRET; yet all of these precious secrets became matters of public information as a result of the Congressional Investigation.

There came a day in the Congressional Hearings when the Chief of Staff of the United States Army at the time of the Pearl Harbor Attack, 5-star General George C. Marshall, was called to the witness stand. He testified for several long, long days, eight of them in all. Toward the end of the second day of his ordeal he was questioned about a letter it had been rumored he'd written to Governor Dewey in the Autumn of 1944, during the Presidential Campaign. The letter was about codes. With frozen face, General Marshall balked at disclosing the whole letter. He pleaded most earnestly with the Committee not to force him to disclose certain of its contents, but to no avail. He had to bow to the will of the majority of the Committee. Here's a picture of General Marshall and Governor Dewey. I will now read from TIME a bit of information which may be new to many of my listeners, especially to those who were too young in December 1945 to be following into periodical literature or to be reading any pages of the daily newspaper other than those on which the comics appear.

Said TIME, and I quote:

"U.S. citizens discovered last week that perhaps their most potent secret weapon of World War II was not radar, not the VT fuse, not the atom bomb, but a harmless little machine which
cryptographers had painstakingly constructed in a hidden room in Washington. With this machine, built after years of trial and error, of inference and deduction, cryptographers had duplicated the decoding devices used in Tokyo. Testimony before the Pearl Harbor Committee had already shown that the machine known as 'Magic' was in use long before December 7, 1941, and had given ample warning of the Japs' sneak attack if only U.S. brass hats had been smart enough to realize it. Now, General Marshall continued the story of 'Magic's' magic.

1. "It had enabled a relatively small U.S. Force to intercept a Jap invasion fleet, win a decisive victory in the Battle of the Coral Sea, thus saving Australia and New Zealand.

2. "It had given the U.S. full advance information on the size of the Jap forces advancing on Midway, enabled our Navy to concentrate ships which otherwise might have been 3,000 miles away, thus set up an ambush which proved to be the turning-point victory of the Pacific war.

3. "It had directed U.S. submarines unerringly to the sea lanes where Japanese convoys would be passing.

4. "By decoding messages from Japan's Ambassador Oshima in Berlin, often reporting interviews with Hitler, it had given our forces invaluable information on German war plans." End quote.
TIME goes on to give more details of that story, to which I may later return but I can't leave this citation of what cryptology did toward our winning of World War II without telling you that the account given by TIME of the achievements of MAGIC makes it appear that all the secret intelligence gained from our reading Japanese messages was obtained by using that "harmless little machine" which TIME said was used in Tokyo by the Japanese Foreign Office. I must correct that error by telling you that the secret information we obtained that way had little to do with those portions of the MAGIC material which enabled our Navy to win such spectacular battles as those of the Coral Sea and Midway, and to waylay Japanese convoys. The naval parts of MAGIC were nearly all obtained from Japanese naval messages by our own very ingenious U.S. Navy cryptanalysts. At that time, I may tell those of you who are new, that the Army and Navy had separate but cooperating cryptologic agencies and activities; the United States Air Force was not yet in existence as an autonomous and separate component of the Armed Forces, and work on Japanese, German, and Italian air force communications was done by Army cryptanalysts admirably assisted by personnel of what was then known as the Army Air Corps.

It is hardly necessary to tell you how carefully the MAGIC of World War II was guarded before, during, and after the war until the Congressional Inquiry brought most of it out in the open. Some remaining parts of it are still very carefully guarded. Even the fact of the existence of MAGIC was
known to only a very few persons at the time of Pearl Harbor—and that is an important element in any attempt to explain why we were caught by surprise by the Japanese at Pearl Harbor in a devastating attack that crippled our Navy for many months. Let me read a bit from page 261 of the Report of the Majority of the Joint Congressional Investigation of the attack:

"The Magic intelligence was pre-eminently important and the necessity for keeping it confidential cannot be overestimated. However, so closely held and top secret was this intelligence that it appears that the fact that the Japanese codes had been broken was regarded as of more importance than the information obtained from decoded traffic."

TIME says, in connection with this phase of the story of Magic during World War II:

"So priceless a possession was MAGIC that the U.S. high command lived in constant fear that the Japs would discover the secret, change their code machinery, force U.S. cryptographers to start all over again."

Now I don't want to over-emphasize the importance of communications intelligence in World War II, but I think it warranted to read a bit more of what is said about its importance in the Report of the Majority. The following is from p. 232:

-8-
"... all witnesses familiar with MAGIC material throughout the war have testified that it contributed enormously to the defeat of the enemy, greatly shortened the war, and saved many thousands of lives."

General Chamberlin, who was General MacArthur's operations officer, or G-3, throughout the war in the Pacific, has written: "The information G-2, that is, the intelligence staff, gave me in the Pacific Theater alone saved us many thousands of lives and shortened the war by no less than two years." We can't put a dollar-and-cents value on what our possession of COMINT meant in the way of saving lives; but we can make a dollar-and-cents estimate of what communications intelligence meant by shortening the war by two years, and the result of that estimate is that it appears that $1,000 spent for that sort of intelligence was worth $1,000 spent for other military activities and materials.

In short, when our commanders had that kind of intelligence in World War II they were able to put what small forces they had at the right place, at the right time. But when they didn't have it--and this happened, too,--their forces often took a beating. Later on we'll note instances of each type.

I hope I've not tried your patience by such a lengthy preface to the real substance of this series of lectures, so let's get down to brass tacks. For those of you who come to the subject of cryptology for the first time, a few definitions will be useful, in order that what I shall be talking about
will be understood without question. Agreement on basic terminology is always desirable in tackling any new subject. In giving you the definitions there may be a bit of repetition because we will be looking at the same terms from somewhat different angles.

First, then, what is cryptology? Briefly, we may define it as the doctrine, theory, or branch of knowledge which treats of hidden, disguised, or secret communications. You won't find the word cryptology in a small dictionary. Even Webster's Unabridged defines it merely as "secret or enigmatical language"; and in its "Addenda Section", which presumably contains new or recently-coined words, it is defined merely as "the study of cryptography". Neither of these definitions is broad nor specific enough for those who are going to delve somewhat deeply into this science.

Cryptology has two main branches; the first is cryptography, or, very briefly, the science of preparing secret communications; and the second is cryptanalysis, or the science of solving secret communications. Let's take up cryptography first, because as a procedure it logically precedes cryptanalysis: before solving anything there must be something to solve.

Cryptography is that branch of cryptology which deals with the various means, methods, devices, and machines for converting messages in ordinary, or what we call plain language, into secret language, or what we call cryptograms. Here's a picture of one of the most famous cryptograms in history. It was the solution of this cryptogram which resulted in bringing America
into World War I on the side of the Allies on 6 April 1917, just about six weeks after it was solved. I'll tell you about it later in this series.

Cryptography also includes the business of reconverting the cryptograms into their original plain-language form, by a direct reversal of the steps followed in the original transformation. This implies that the persons involved in both of these bits of business, those at the enciphering and sending end, and those at the receiving and deciphering end, have some sort of understanding as to what procedures, devices, and so on, will be used and exactly how down to the very last detail. The what and the how of the business constitutes what is generally referred to as the key. The key may consist of a set of rules, alphabets, procedures, and so on; it may also consist of an ordinary book which is used as a source of keys; or it may be a specialized book, called a code book. That cryptogram I just showed you was made by using a book—a German codebook.

To encrypt is to convert or transform a plain-text message into a cryptogram by following certain rules, steps, or processes constituting the key or keys and agreed upon in advance by the correspondents, or furnished them by higher authority.

To decrypt is to reconvert or to transform a cryptogram into the original equivalent plain-text message by a direct reversal of the encrypting process, that is, by applying to the cryptogram the key or keys, usually in a reverse order, employed in producing the cryptogram.
A person who encrypts and decrypts messages by having in his possession the necessary keys, is called a cryptographer, or a cryptographic clerk.

Encrypting and decrypting are accomplished by means collectively designated as codes and ciphers. Such means are used for either or both of two purposes: (1) secrecy, and (2) economy. Secrecy usually is far more important in diplomatic and military cryptography than economy but it is possible to combine secrecy and economy in a single system. Persons technically unacquainted with cryptology often talk about "cipher codes", a term which I suppose came into use to differentiate the term "code" as used in cryptology from the same term as used in other connotations, as, for example, the Napoleonic Code, a traffic code, a building code, a code of ethics, and so on. Now, in cryptology, there is no such thing as a "cipher code". There are codes and there are ciphers, and we might as well learn right off the differences between them so that we get them straightened out in our minds before proceeding further.

In ciphers, or in cipher systems, cryptograms are produced by applying the cryptographic treatment to individual letters of the plain-text messages, whereas, in codes, or in code systems, cryptograms are produced by applying the cryptographic treatment generally to entire words, phrases, and sentences of the plain-text messages. More specialized meanings of the terms will be explained in detail later but in a moment I'll show you an example of a cryptogram in cipher and one in code.
A cryptogram produced by means of a cipher system is said to be in cipher and is called a cipher message, or sometimes, simply, a cipher. The act or operation of encrypting a cipher message is called enciphering, and the enciphered version of the plain text, as well as the act or process itself, is often referred to as the encipherment. A cryptographic clerk who performs the process serves as an encipherer. The corresponding terms applicable to decrypting cipher messages are deciphering, decipherment, and decipherer.

A cryptogram produced by means of a code system is said to be in code, and is called a code message. The text of the cryptogram is referred to as code text. This act or operation of encrypting is called encoding, and the encoded version of the plain text, as well as the act or process itself, is referred to as the encodement. The clerk who performs the process serves as an encoder. The corresponding terms applicable to the decrypting of code messages are decoding, decodement, and decoder. A clerk who encodes and decodes messages by having in his possession the pertinent code books is called a code clerk.

Technically, there are only two distinctly different types of treatment which may be applied to written plain text to convert it into a cipher, yielding two different classes of ciphers. In the first, called transposition, the letters of the plain text retain their original identities and merely undergo some change in their relative positions, with the result that the original text becomes unintelligible. Here's an authentic example of a
transposition cipher; I call it authentic because it was sent to President Roosevelt and the Secret Service asked me to decipher it. Imagine my chagrin when I had to report that it says "Did you ever bite a lemon?" In the second, called substitution, the letters of the plain text retain their original relative positions but are replaced by other letters with different sound values, by symbols of some sort so that the original text becomes unintelligible.

Nobody will quarrel with you very hard if you wish to say that a code system is nothing but a specialized form of substitution; but it's best to use the word code when a code book is involved, and to use substitution cipher when a literal system of substitution is used.

It is possible to encrypt a message by a substitution method and then to apply a transposition method to the substitution text, or vice versa. Combined transposition-substitution ciphers do not form a third class of ciphers; they are only occasionally encountered in military cryptography. Applying a cipher to code groups is a very frequently-used procedure and we'll see cases of that too.

Here's an example of a substitution cipher, and a very simple one. It was found on a German spy in World War II. Here's the cipher alphabet; here's the plain text which happened to be in German; and here's the cipher text or encipherment.
Now for an example of a cryptogram in code. Here's a plain-text message in the handwriting of President Wilson, to his special emissary in London, Colonel House. Here's the cryptogram after the plain text was encoded, by Mrs. Wilson. The President then himself typed out the final message on his own typewriter, for transmission by the Department of State. It would appear that President Wilson lacked confidence in the security of the Department of State's methods—and maybe with good reason, as may be seen in the following extract from a letter dated 14 September 1914 from the President to Ambassador Page in London: "We have for some time been trying to trace the leaks, for they have occurred frequently, and we are now convinced that our code is in possession of persons at intermediary points. We are going to take thorough-going measures." Perhaps one of the measures was that the President got himself a code of his own. I must follow this up some day.

A cipher device is a relatively simple mechanical contrivance for encipherment and decipherment, usually "hand-operated", or manipulated by the fingers, as for example, a device with concentric rings of alphabets, manually powered. Here's an example—a cipher device with such rings. I'll tell you about it later. A cipher machine is a relatively complex apparatus or mechanism for encipherment and decipherment, usually equipped with a typewriter keyboard and generally requiring an external power source. Modern cryptology, following the trend in mechanization and automation in other fields, now deals largely with cipher machines, some highly complicated. Here's a picture of a modern cipher machine with keyboard and printing mechanism.
One of the expressions which uninformed laymen use but which you must
never use is "the German code", or "the Japanese code", or "the Navy cipher",
and the like. When you hear this sort of expression you may put the speaker
down at once as a novice. There are literally hundreds of different codes
and ciphers in simultaneous use by every large and important government or
service, each suited to a special purpose; or where there is a multiplicity
of systems of the same general nature, the object is to prevent a great deal
of traffic being encrypted in the same key, thus overloading the system and
making it vulnerable to attack by methods and procedures to be mentioned in
broad terms in a few moments.

The need for secrecy in the conduct of important affairs has been
recognized from time immemorial. In the case of diplomacy and organized
warfare this need is especially important in regard to communications. How-
ever, when such communications are transmitted by electrical means, they can
be heard or, as we say, intercepted, and copied by unauthorized persons,
usually referred to collectively as the enemy. The protection resulting from
all measures designed to deny to the enemy information of value which may be
derived from the interception and study of such communications is called
communication security, or, for short, COMSEC.

In theory, any cryptosystem except one, to be discussed in due time,
can be attacked and "broken", i.e., solved, if enough time, labor, and skill
are devoted to it, and if the volume of traffic in that system is large
enough. This can be done even if the general system and the specific key
are unknown at the start. You will remember that I prefaced my statement
that any cryptosystem can be solved by saying "in theory", because in
military operations theoretical rules usually give way to practical considera-
tions.

That branch of cryptology which deals with the principles, methods, and
means employed in the solution or analysis of cryptosystems is called
cryptanalysis. The steps and operations performed in applying the principles
of cryptanalysis constitute cryptanalysis. To cryptanalyze a cryptogram is
to solve it by cryptanalysis. A person skilled in the art of cryptanalysis
is called a cryptanalyst, and a clerk who assists in such work is called a
cryptanalytic clerk.

Information derived from the organized interception, study, and analysis
of the enemy's communications is called communication intelligence, or, for
short, COMINT. Let us take careful note that COMINT and CONSEC deal with
communications. Although no phenomenon is more familiar to us than that of
communication, the fact of the matter is that this magic word means many
things to many people. A definition of communication that is broad enough
for our purposes would be that communication deals with intelligent messages
exchanged between intelligent beings. This implies that human
beings, and human operators are involved in the preparation, encryption,
transmission, reception, decryption, and recording of messages which at some
stage or stages are in written form and in some stage or stages are in
electrical form as signals of one sort or another. But in recent years
there have come into prominence and importance electrical signals which are
not of the sort I've just indicated. They do not carry "messages" in the
usual sense of the word; they do not convey from one human being to another
an intelligible sequence of words and an intelligible sense. I refer here
to electrical or electronic signals such as are employed in homing or
directional beacons, in radar, in telemetering or recording data of an electrical or
electronic nature at a distance, and so on. Information obtained from a study
of enemy electronic emissions of these sorts is called electronic intelligence,
or, for short, ELINT. The particular or specialized study of enemy radar
signals is called RADIINT. All these, COMINT, ELINT, RADIINT comprise SIGINT,
that is, signal intelligence. Cryptology is the science which is concerned
with all these branches of secret signalling.

In this series of lectures we shall be concerned only with COMSEC and
COMINT, leaving for others and for other times the subjects of ELINT, RADIINT,
and so on. This means that we shall deal with communications or messages.

Communication may be conducted by any means susceptible of ultimate
interpretation by one of the five senses, but those most commonly used are
seeing and hearing. Aside from the use of simple visual and auditory
signals for communication over relatively short distances, the usual method
of communication between or among individuals separated from one another by
relatively long distances involves, at one stage or another, the act of
writing or of speaking over a telephone.
Privacy or secrecy in communication by telephone can be obtained by using equipment which affects the electrical currents involved in telephony, so that the conversations can be understood only by persons provided with suitable equipment properly arranged for the purpose. The same thing is true in the case of facsimile transmission (i.e., the electrical transmission of ordinary writing, pictures, drawings, maps). Even today there are already simple forms of enciphered television transmissions. Enciphered facsimile is called CIFAX; enciphered telephony, CIPHONY; and enciphered television, CIVISION. However, these lectures will not deal with these electrically and cryptanalytically more complex forms of cryptology. We shall stick to enciphered or encrypted writing—which will be hard enough for most of us.

Writing may be either visible or invisible. In the former, the characters are inscribed with ordinary writing materials and can be seen with the naked eye; in the latter, the characters are inscribed by means or methods which make the writing invisible to the naked eye. Invisible writing can be prepared with certain chemicals called sympathetic or secret inks, and in order to "develop" such writing, that is, make it visible, special processes must usually be applied. Here's an interesting example—the developed secret-ink message that figured in an $80,000,000 suit won by two American firms against the German Government after World War I sabotage was proved. There are also methods of producing writing which is invisible to the naked eye because the characters are of microscopic size, thus
requiring special microscopic and photographic apparatus to enlarge such
writing as to make it visible to the naked eye. Here's an example—a code
message in a space not much larger than the head of a pin. A simple
definition of secret writing would be to say that it comprises invisible
writing and unintelligible visible writing.

There is one additional piece of basic information which it is wise
to call to your attention before we proceed much further, and I'll begin by
stating that the greatest and the most powerful instrument or weapon ever
forged and improved by man in his long struggle for emancipation from utter
dependence upon his own environment is the weapon of literacy—a mastery of
reading and writing; and the most important invention, the one that made the
weapon of literacy practical, was the invention of the alphabet. It is
therefore a rather striking anomaly that we should now come to the study
of another weapon—a counter-weapon to the weapon of literacy—the weapon
of secrecy, the basic intent of which is to thwart the weapon that man
struggled so long to forge. Secrecy is applied to make writing more difficult
and the reading of the writing very difficult, if not impossible.

Perhaps this is a good place to do a bit of theorizing about this matter
of secrecy and what it implies.

Every person who enciphers a piece of writing, a message, or a text of
any kind, for the purpose of hiding something or of keeping something secret,
does so with the idea that some other person, removed from him in distance,
or time, or both, is intended to decipher the writing or message and thus uncover the secret which was so hidden. A person may possess a certain piece of knowledge which he does not wish to forget but which he is nevertheless unwilling to commit to open writing, and therefore he may jot it down in cryptic form for himself to decipher later, when or if the information is needed. The most widely known example of such a cryptogram is found in Edgar Allan Poe's romantic tale The Gold Bug. That sort of usage of cryptography, however, is unusual. There are also examples of the use of cipher writing to establish priority of discovery, as did the astronomers Galileo and Huygens. Here's a slide which shows both examples. I suppose I should at least mention another sort of cryptic writing famous in literary history, the diaries of persons such as Samuel Pepys and William Byrd. These are commonly regarded as being "in cipher", but they were actually written in a more or less private shorthand and can easily be read without the help of cryptanalysis. Here's a picture of a page of Pepys diary.

Now there can be no logical reason, point, or purpose in taking the time and trouble to encipher anything unless it is expected that some other person is to decipher the cipher some time in the future. This means that there must exist some very direct, clear-cut and unambiguous relationship between the enciphering and deciphering operations. Just what such a relationship involves will be dealt with later but at this moment all that it is necessary to say is that in enciphering there must be rules that govern or
control the operations, that these rules must admit of no uncertainty or ambiguity and that they must be susceptible of being applied with undeviating precision, otherwise it will be difficult or perhaps impossible for the decipherer to obtain the correct answer when he reverses the processes or steps followed in the encipherment. This may be a good place to point out that a valid or authentic cryptanalytic solution cannot be considered as being merely what the cryptanalyst thinks or says he thinks the cryptogram means, nor does the solution represent an opinion of the cryptanalyst. Solutions are valid only insofar as they are objective and susceptible of demonstration or proof employing scientifically acceptable methods or procedures. It should hardly be necessary to indicate that the validity of the results achieved by cryptanalytic studies of authentic cryptograms rests upon the same sure and well-established scientific foundations, and are reached by the same sort of logic as are the discoveries, results, or "answers" achieved by any other scientific studies, namely, observation, hypothesis, deduction, induction, and confirmatory experiment. Implied in what I have just said is the tacitly understood and now rarely explicitly stated assumption that two, or more, equally competent and, if necessary, specially qualified investigators, each working independently upon the same material, will achieve identical or practically identical results.

Cryptology is usually and properly considered to be a branch of mathematics, although Francis Bacon considered it also a branch of grammar and
what we now call linguistics. Mathematical and statistical considerations play an ever-increasing and prominent role in practical cryptology, but don't let my statement of this point frighten those of you who have not had much formal instruction in these subjects. We have excellent cryptologists who have never studied more than arithmetic, and some of our best ones would hide if you were to go searching for mathematicians around here. What is needed is the ability to reason logically as the mathematician sometimes does and this ability is found in the most curious sorts of persons and places. So those of you who are frightened by the words mathematics and statistics take heart—you're not nearly so bad off as you may fear.

But now to return to the main theme as to the place mathematics occupies in cryptology, let me say that just as the solution of mathematical problems leaves no room for the exercise of divination or other mysterious mental or psychic powers, so a valid solution to a cryptogram must leave no room for the exercise of such powers. In cryptologic science there is one and only one valid solution to a cryptogram, just as there is but one correct solution or "solution set" to any problem in mathematics. But perhaps I've already dwelt on this point too long; in any case, we'll come back to it later, when we come to look at certain types of what we may call pseudo-ciphers.

In the next lecture I'm going to give you a brief glimpse into the background or history of cryptology, which makes a long and interesting story that has never been told accurately and in detail. The history of communications
security, that is, of cryptography, and the history of communications
intelligence, that is, of cryptanalysis, which are but opposite faces of
the same coin, deserve detailed treatment but I am dubious that this sort
of history will ever be written because of the curtain of secrecy and
silence which officially surrounds the whole field of cryptology.

Authentic information on the background and development of these vital
matters having to do with the security of a nation is understandably quite
sparse.

But in the succeeding lectures I'll try my best to give you authentic
information, and where there's conjecture or doubt I'll so indicate. I must
add, however, that in this series I'm going to have to omit many highly-
interesting episodes and bits of information not only because these lectures
are of low classification but also because we won't and can't go beyond a
certain period in cryptologic history for security considerations. Neverthe-
less, I hope you won't be disappointed and that you'll learn certain things
of great interest and importance, things to remember if you wish to make
cryptology your vocation in life.
William F. Friedman
％US Military Attaché
American Embassy,
London, England

3932 Military Road,
Washington, D.C.

"Entia non sunt multiplicanda praeter necessitatem"
=William of Occam

Approved for Release by NSA on
01-23-2015 pursuant to E.O. 13526
Friday, April 23, 1943

Left National Airport on a C-54 at 11:18 p.m. (instead of 7:30 a.m.) 26 passengers, crew of 8. Nice passage to Gander. No turbulence. No wind pressure, no flaps, when due to land. Circled field 3 times, made good landing at 11:45 p.m. 1350 miles. Good supper. Played ping pong. Left Gander 12:15 p.m. (local time) in single hop to Prestwick (2:22 a.m.) Landed 10:40 a.m. Very cold at 16,000 ft but had use oxygen. Then down to 1500 ft. Quite rough. Was nauseated. Several times Customs etc at Prestwick. After about 15 minutes boarded shuttle plane to London. Arrived Heathrow at 2:30 p.m. (local time)

Bus from Airport to 48 Audley St,酱, 25 mins. Was assigned room at Park Lane Hotel, June Shopping and from shop to arrive Heathrow 25 hrs. Flight 21 hrs.

Nice dinner at hotel, good room, with Taylor at 18/plus 3/6 for buffet.

To bed at 11:30 p.m. (London) slept hard through our alarm at 12:30 a.m. Feel tired but more rested and very comfortable.

Sunday April 25 - Reported in at A.S.O. office. Phoned George Burley, met him at ETOUSA HQ. With Ernie Swenson, Grand Tour, and lunch with them at Officer's Mess. Left for London. We were introduced to given membership (me thru courtesy of Col. Fyman). Spent evening at George's with George, Ernie and Fyman at table. Spent evening at Ernie's room, talking. Back to bed at 11:30 p.m.

Monday April 26 - Ate 9:30 a.m. Breakfast hotel. Reported to 41 A. + met" Hen Pauling. Lunch at Club. Spent pm again with George. Tour through his rooms. Talked with Johnson, met Col. Black. In ETOUSA Dinner with George as our guest. Walked
Hyde Park. Evening at George's hotel. 

Must have discussion before 12. FS for US 7.30 am inside continuous session. Ahead. Dinner at 7.15 am. 

Breakfast. Our guide, Frank. 

Tuesday April 27 - Breakfast in room at 10.30. To HQ to pass on letter to 

Jan Rumbough. Made date for us 

to call on p.m. In C to Chase hall. 

to open account for us at Gunners. 

Our place. 4:30 pm called on Jan. R and had nice visit. 

George this a.m. with info for trains made good 

opening for us. Called him later. 

on special line from George's office. 

Cordial welcome. Dine at 7.15 

p.m. for dinner. (Commander's table. 

Bottles from Gunners for occasion. 

It was good thing that train at 

door so we were coming in. Very 

cordial greeting up to my room. 

*see note 5 pg 5

When had fairly good preliminary 
talk. I suggested his arranging for 

meeting this p.m. with M. We 

agreed good thing to do despite it 

being departure from our until re 

going home. Jan Davidson first I had 

heard phone if OK. Lunch at Off base. 

Back to hotel. Rested 30 min. Called 

it took us to fall on M. Spent 1½ hrs. 

with him. Very dapper & pleasant. 

General welcome. We will proceed with 

preparations. Mention of Dutch men 

30. 

If we are 1st they I machines. I notice 

expected Verkhov had more variety it 

with Jan Whigger. MA offered so welcome to 

go then the works. I took me back to 

hotel. Handed over bags out on 

our gadgets & Rap cont. will not be 

arranged until we come then as they 

have. Dinner. Goodby to guests. Jan 

Rumbough. Running me back to hotel 

and to bed.
Sunday, April 29 — Up at 7:30. Breakfast at 8:00. Goodbye to Hotel. We leave at 10:30 and go to airport. We are met by our luggage. Check in 2:00. We meet hotel. We go to hotel at 3:00. To New York. To New York. To New York. To New York.

Monday, April 30 — Up at 7:30. Breakfast at 8:00. Goodbye to Hotel. We leave at 10:30 and go to airport. We are met by our luggage. Check in 2:00. We meet hotel. We go to hotel at 3:00. To New York. To New York. To New York. To New York.

Wednesday, April 24 — Up at 8:00. Goodbye to Hotel. We leave at 10:30 and go to airport. We are met by our luggage. Check in 2:00. We meet hotel. We go to hotel at 3:00. To New York. To New York. To New York. To New York.

Friday, April 27 — Up at 7:30. Breakfast at 8:00. Goodbye to Hotel. We leave at 10:30 and go to airport. We are met by our luggage. Check in 2:00. We meet hotel. We go to hotel at 3:00. To New York. To New York. To New York. To New York.

Saturday, April 28 — Up at 8:00. Breakfast at 9:00. Goodbye to Hotel. We leave at 10:30 and go to airport. We are met by our luggage. Check in 2:00. We meet hotel. We go to hotel at 3:00. To New York. To New York. To New York. To New York.

Thursday, April 26 — Up at 7:30. Breakfast at 8:00. Goodbye to Hotel. We leave at 10:30 and go to airport. We are met by our luggage. Check in 2:00. We meet hotel. We go to hotel at 3:00. To New York. To New York. To New York. To New York.
REF ID: A60517

Missed reply to C's message & sent telegram to C. Then to Gen. Peabody's office in his car to War Office to call on Gen. Dardengo. Dinner at D'Arcy hotel.


Once Calt to club where we talked semi-still for about hour. We are to give D a schedule on Sunday of what we want to see in the shop. Him to spend weak-end with him at great expense as can be arranged dinner at Club with Eric as our guest. Met Mrs. Jerry & renewed. Wash acquaintance. Dinner & then to our hotel, where played 4-handed rummy. Up to bed at 10:30. Note D told us that M was just not going to work but that T. told him, and Soon!

Sunday May 3. Up at 9. Poor. Slept on for nine hours or more, maybe ten. Weather still rainy. Breakfast hotel then to War office to get paper which came to £52 50 and £13 1/3. What latter I go to hotel to read & had conference with Tayler.
Post on way to train to BP, near to London, do not know to which there were en route there. We arrived at 8:15. We examined sales desk, rooms, lounge, etc. There we met at 11:55 a.m. were met by Col. Fitch (head, Naval Services, incidentally). In Tilton's office car. After few minutes had informed us we were to see all except rear office at gate where we registered (N material). We left naval engineer office in Lounge directly to Tilton's office where (he told us) worked for nothing. To take test. De Tray, Tilton's deputy, a pleasant man of all their construction. A very full looking, small man. We had a few minutes' luncheon (which put he could sleep, for return.) and then we went to Tilton's office for a minute preliminary discussion of general details, during course of which he informed us he was going to wash his clothes on Saturday. He had disposed SS Frame work now is in progress to go alone. In their production office. Some research section on security. Did rather large chart depicting sources was passed by Adlertly when I would show it. Their new material, method of getting it to BP and routing there. This cost to Pabst. If not indicated post office. Stated chart a bit further, if proper bag are not avoidable. Have difficulty in giving us copy. The next varieties to be expected but if it were think not of their shores and seeking very poor to get more than depth, which much better than our own. Then could hardly be solved. To show us the...

[Ref to A, AF, N, ABW]
powned. Fig. 85 shows which ever green good gets over will provide for vertical displacement by some sort. Then called for McCusker & Taylor. They were taken in for private enemy if B3P. They now have 4 oars working there exclusive of maintenance and guard personnel. This means like a terrible looking structure over a rich man's country home. Note if wartime were some still in use. Then abandoned. If Type X, transferring one operation. Wait about 8 or 9 more ballot boxes first. If the arrives at central teleprinter structures. We did not go inside them. As Ti said no time to get marveled at. Some are due to action involved. Do they then come for us? We made sure being read in the section itself a pipe heavily and through their traffic reception. Teleprinters are maintained at B3L. Type X. We were then taken to war where outgoing operated. It has a complement of 3 shifts of 48 WAFTS. They are passed through Type X. About 23 on duty in a shift. Each girl by oldest, most trusted. WAFTS. Taking care of 3 machines. She bases operators machines getting up keep (by
REF ID: A60517
Tuesday May 4 — Today spent mostly at D's shop. Dine at Red Cross place. Dine at our Club Supreme with the McCanns. I was much impressed with amount of work done by so few people. Met several of D's people, Miss Jack, Mr. White, Mr. S., and Mr. Hanley. Spent 2 hours in District Record Section, in charge of Eleanor Smith (who was out today) but actually run today by a French lady of Cambridge named Jutius, who has full assistants in record maintenance. Two old PO women do the teletype and filing (to sections). If the coming thru. After lunch spent in lounge with Mr. White (Gen. Staff - General Sanical) in big suite. Met Col Mervade there. To return for more talk with him tomorrow.

Wednesday May 5 — Up at 8. Breakfast then to PX for Capt. Kenney and weave from (probable) Kellend's. Called on progress on JAC, and requested them to use System of U instead of Special Wages. Also reported our progress to Col. of forthcoming trip to BP. Then to D's shop where we went into details of G. Florence but Miss Patrice Bartley, in charge of G. Section, a most cheery young woman, South W. Fells, Mr. Tomlinson, and other French as D's guests, with Mr. Earle-Sumner (D's Deputy in charge of D's Section), Mr. Hope, head of Commercial Section. Went to Bagatelle Restaurant, delightful conversation with Earle-Sumner and Hope on my night out. Left - Both see Shakespeare.
devotees. Cocktails ("Fun & French") then.

a very nice lunch, after which we returned
to D's place for further discussion on G. We
shared paper on division labor on book
log + an 11 pp. revised draft tomorrow. Met
Mr. Vortleben, dean of art, who is over
75 & has been in power for 50 years. He &
Mr. R's adopted 1-time guest in 1916-17, R F D
had stuff & going back in '96, Austrian
marketers & told R's planters. System all
very simple 1-part ces which remained an
effort for long time & 1st, etc. indep. one
from '93 to '40. V is still quite active
mentally & gets quite excited if reconstruction
2-fits, he doesn't care for "machines," we
left at 5 45, walked to Hans Opera House
where we went directly to the Magic Flute
very good performance & we had good
parts which I purchased at Selfidges
at premium of 1 shilling each card (of
and 10), forever began on 14 May 30.1

found out 7 out of 9 crowds foregoing to
got to London. Before dinner we walked
to hotel & had dinner W. Bought a
bottle of wine (59 o 8 " 1) & we had a
very nice dinner. Up to 10. Went to a better
books to bed Friday the news
re new Andrews death in place circuit.
Scotland. Very nice summer and Kemp
A F 10 USA

Thursday was to stop at 8 Tims had
cold. I went to pick up stock purchased
last Saturday. Cashed 50" new ces & got
beer £ 7/7, 1st & 2nd class. 2/10 sh. vs
plus stamps. To Lindonwy, quitted by a 75
P.O. employee who pointed at places of inter-
est. Then to D's shop where we talked over
with 1 train staff. Were much impressed
with high caliber of cars — practically all
en-American or Gen. — Generals who had
had years of experience + ting in the East
r. Apparently glad to make their way...
Friday May 6th - Up at 8, left at hotel, settled at there & found necessary cash more than checks ($40) so as to settle up & have some left to take along to B/P. Ford & II still well enough to travel. Dined to take all my belongings to B/P & what a bad week Mt. & Easter, pick up some paper & also M. C., with whom went to Easter. She in good, nice ride to Blundell. Car received us & we were welcomed to B/P. Other members of COF were along there & among us to start of Capt. Patmore, Johnson, from Delhi, India, Capt. John Sandford, from Brisbane, Australia, Major Thompson, head of J 법률 at B/P, Capt. Nance, also of J 법률 at B/P, who serving as secretary at Dining Dr. Grey. Mr. C ... at once asked away, Erwin greeted COF in his office with well chosen words of welcome to me as guest of honor, which I replied most suitable for Erwin method.
The people of Long Man projected a time to eat an evening but I declined in favor of a fishman's house later on. We arranged for the usual 27. I don't know. Recovered at 3:30 tomorrow. Took up personally the mutton before us. At 4.50 called and paid. He was very tired, heard about breaking my for the day. I thought then a rather strange but explanation later from him was that he felt the day he purposely looked away from the fact. At another 12:30 stopped to examine anything I could. He was engaged or the paper was involved away so that he was pretty sure. On this note I acquired a car was sent to take me to hotel.

Newport Pagnell, a small town about 8 miles from BPP. "The function" which is a pub, but very clean and quiet, had facilities for laundry or threat, one young woman takes care of all. We are apparently the only guests. We unpacked a lot of their

went for a short walk to see the village. Dinner at 7. The food was excellent. Just system but no napkins. We talked all together until about 10.20. I explaining what distance — broke up my general to the. I felt prettyquite with 10 cold coming on as got into bed with pajamas, my golf shoes, and my washers. Breakfast I got worn in a hurry to fall into very sound sleep until 6:15. When bell went to church arrived at the Saturday morning. And the door Thrush, beautiful tea. 11 a.m. good tea. Can come to field is to BPP, arriving at 10.19 there. Then they wrote but wore much interrupted by call for Tres who wanted to see that we were to be shown there, not to wash. Communication of what he had told us the day before, we were not to be shown anything on that side (at request of our hang!!). He asked me not say anything.
REF ID: AG0517

Back home re many hangar requests this but we could say rarely that we were not shown their part Trans said he frankly did not see why he should bear the obligation for this part of action or wanted it straight as far as I was concerned I then prevailed on where O'Dea of RAF gave data communication facilities for passing the Then had further discussions of SAC. Lunch again for 2 hrs Trans was there, just prior to taking off for US via Bomber. Have his personal wish on table during some good lunch at Spithead. Doubt whether he'd get off from Falmouth because weather has been so bad. SAC has been unreasonably cold, damp, & windy now for several days. After lunch we got down again to more serious detailed discussions re SAC & reached conclusions, some of which were submitted to Falmouth to GH Q & going very smoothly as a most friendly spirit of cooperation. We had no representative from Canada, but nevertheless took cog of their interest. We adjourned at 5 top & Miss Johnson took me to Tidmore home which is close to gate to base. Had a couple were Scotch. Talked then into T for dinner (presumably) very pleasant & multi-course meal of food (soup, meat, hot sausages etc., vegetables, choc pudding). Set around five after dinner (coffee, etc) listened to radio at 9 p.m. re taking off. Under 13 perct. of 10 T had our call for me & take me to Newport-Pagnell, reaching hotel just as it was getting really dark. Talked with W.C. a while—he absolutely amazed by what I've have been beyond all his imaginings. Taylor was already in bed & did not join in conversations. Barrow & I... sure he is just as impressed. Wonder whether everything in Barrow is fine,
REF ID2360517

as well. It is certainly good!" I said. C
told me there was nothing new. I asked
him about his job at the Atomic Energy
Commission. He said it was very well
paid and there was no chance of anyone
taking over the job. He doubted whether C
is smart enough to grasp the significance
of the atomic bomb. The" B" have to work
closely with the "C" on the board. He said
well-wrapped and I had a very fine
time again.

Sunday, May 9 - Up at 8. Breakfast
was excellent and nice tea too. We
got to 8 SP at 10.30. Had a session
with T. Of course, C. was here again.
Wenham and Morgan on the
research section. It was a very
loose-knit affair - composed of all the
men who had worked on the project.

29

primary job is designing "after which they
pass the matter over to specialists like
H. L. D. Simon, then to Morgan, Capt.
Morgan, Mr. Bradley, Mr. Simon. He says the
jobs are now engaged in 11 AE stations on AC as
staff but have other AE problems. We had lunch
with D. at the N. C. Taylor and Mr. E. Bradley
who is Deputy, DEP on administration. He has a
lot of work to do and train the new people. He
sees all the staff to keep in

contact. After lunch at my request D. got
an empty chair and we went through it carefully.
C. was seen in the evening and had a good
afternoon. He worked on the AE, and
went later to C. at the AE. He said the men
were all very happy and the work was
progressing very well. After dinner he
went with D. to see the AE and
with details in their general operation.
Talked to us about the Special Com Un Part
I'm so glad we got to see you last night. I hope the trip was good.

The food was great, and the people too. I think we all had a nice time.

I hope the weather is nice where you are. It's really nice here.

I'll talk to you soon.

Take care!

Love,

[Signature]
and with primitive conditions as to chains, furniture, etc - car came for us late as usual (10:15) so we had plenty of time for breakfast which was some canned tomatoes (excellent) and scrambled eggs. At BP we resumed our IAC conference and practically finished up what we could. Final end to be held on Monday, May 17th at Bug Hames, Chairman of C. R. Thomas (Lunch at BP, then inspection with Mr. Welchman on 6 from 2:15 to 4:30, then the session with Mr. Mitchell & Associates. Dinner at 6:30, and departure at 7:30.)

Dinner with Mr. & Mrs. Ditch at their hotel at Bedford Arms. Mrs. Dudley Smith & young, attractive wife were also guests. We had Irish whiskey - 3 rounds - and a pretty nice dinner. Mr. G. works at BP, so does the D.S. Pleasant evening chatting. Back showed up free from hotel-like type. Slight rain structures were very attractive. B had a car with very pretty ATS clover. Back to Newport Bay at 10:30. Just about dark. Am suffering from lack of light. Facilities at hotel very skimpy.
wasn't any too warm so that to BP at 9.45 & then immediately to my secret pass on E with Marshall major, we & the WT & tea & picture, which is very interesting to see & take down who in a Capt in the 377. We had arranged a schedule for us (Col. War Johnson & self) which called for 1/4 of them but we stayed at least 1/3. We had had to be modified. And will be soon, as I suppose to go slow & get all the plan (he reading them for me) then had practice on theoretical crypt info with Dr. Seaberg 15-20 to 15 lunch. where I met Ennor & Clifford (his relief) at 15 back to Seaberg with 35 then rushed to get to 82 where A & T were just entering car to go to 5th. We waited at 5th for 3/4 the 9th to 9th at 5:10, took Covert of Rumanian who got his nog claus at Carnegie Tech then was attached to Langley Wash for 20 years, now with "Free Run"

in John To Embassy. Several messages for me but no letters than to Park Stonewall. I had a bath at last! Dinner at Chal & straight back to hotel. Read over all my notes, sorted things out & now in bed. Washed socks & loaded. Gave 4 shots to Ed & had just passed. Had nevertheless written letter to E & folks in NY (1st time) now 11:50 p.m. want to bed. PS Notes re C and from A. Adie Private Code about May 4th would have been locked in hold. Code communions. From NA intercept C lackey to BP. NA all in time to save ship only man killed or wounded.

Wednesday May 12 - Turned out lights at 10 30 p.m. last night but soon decided no go - too many things on mind that I wanted to write notes on Bassis. Slept & slept it was 1:30 am. July 14th was a horse long ago. Had not to have to get up early - no engagement for the rest
plapt until 9 A.M. (not too properly) and had breakfast in room with 
T. whose cold is worse and decided to stay in all day. Dresssed and 
showered over to Embassy Letter for me! First one from E. dated April 
27 postmarked 28th via 30 of our 
mail, which arrived in my hands 
only today - 15 days! It must have 
gone by boat, but glad to hear 
from home. The other two partners 
have nothing so far. Worked on 
notes and composing telegram with 
Al, then to lunch at Club on the 
T. Hostman as guest. J ours. Pleasant 
chat + good lunch after which we re-
turned to Embassy to continue working 
I sent a long one to Cont. AI sent 
several, one long + 2 short ones. 
They take time to prepare though 
+ it was 6 P.M. when I finished
business. Spent all day at D's - show going over it method in a detailed manner, under Cathy, head of section. He has been with D since 1935 had several fairly interesting people but on the whole I regard them as practicing amateurs. If they didn't have all the wealth of background material they'd not do so well and their working quarters are a rabbit warren - but somehow they do 1st class work nevertheless. Lived at Red Cross where I was engaged as once again - they are pretty about the place being only for people in uniform. I put in my application a couple of weeks ago but the matter of admitting civilians is being taken up on the high level! While amuse

me a lot next year's contract to RC would be what it was this, so far as I'm concerned. Worked all pot again in T section. Dinner at officer's mess with Swenson & later to his flat where worked on lighter - he & Taylor's Tommy a lighter. Bought my sample one in Wash several years ago for $5. It is the only one around he hasn't really worn all the time, much to the dism. of those who have the expensive $15 dollar ones I used to (maybe) but Eric - no, because we couldn't figure out how to meet the check - even if we had one when we didn't it was going to go to bed at 9 then it was 10 so already so we

scammed home it wasn't pitch dark yet or maybe the moonlight was sufficient to light the way. Went to bed at 7 - played pool again. Woke up many times in the am almost decided to go to the
Friday, May 11

We arrived at my business, feeling pretty dragged out, though I think the cold is working on me. We went to Demain's again around nine at 10:30 looked over the Port & Bank stuff. Mat Exell, head ype who was Botanist at British Museum.

His wife who was also Botanist in work.

Also self-trained something but long.

Also very good. They go on for a detailed study and work themselves than we do.

Also they get some help from direct contact with F.O. which we do not.

Does regularly. Mat also younger.

Cooper, brother of Head of ex-Sen at B.P. Young C has just recently returned from Australia, having been among those chased by the Japs from Hong Kong. Singapore. Jutta's Dev.

Mr. Minton took us to Cunard & Taylor.
Lunch there was bit more discussion at J's office but we could not persu. to go onto another section so we decided to proceed for the day. Returned to Feltmarg where there was a rage for the post. At these still working cables to Clarke but we dragged him out to attend to press repair about St Paul's. Great dedication there but all the desks has been greatly cleaned up. Walked about quite a deal & went into Guildhall which was well demolished except for the hall itself. Stopped in for some beer as a nice pub where I came (opening hour) went to Feltmarg - more minor for me. Dinner (after bath & rest at the Park Lane) at #8 Caxton St where I ate well but not too wisely, judging by the back.
except what we might expect in way of speed. He is off on a weekend leave. I was astonished to learn that people of RCACs get 4 weeks leave with pay at rate of 1 week 4 times/year. Talked with Joe this and he told me it was expected that Civil Service but I think the way they work it it is more or less of a sub rosa thing. Those running RCACs recognize the high pressure wear of the values of these distributed leave weeks or apparently everybody takes their leave. I think it would help us too. We left AE there to ship in a week, he having been up until 130 finishing long tel to Colston which he brought to us at midnight in draft and we suggested changes that I kept him working late—he has sent plans of the home on the E matter. I am very happy I had lunch at RC, where I straightened out matter of my acceptability—somewhat SIMD to be admitted. I quizzed on special concession. Returned to DC's place after good lunch. The DC place is OK in that respect I worked about 1 hour more in FF section where met very attractive young woman—Mrs Hanson. All personnel of FF section woman. Head had been with DC since last war. The number of older men in FF is very striking. Probably the most important factor in the success of RCACs. Joe for hard work and a lot of help being a very pleasant person. To be there next weekend. I had work to do decided to leave the field for this time and not oversee the hospitality on 1st part of 1st day. I had dinner at club. Had an alert in FDR this pm about 5:30—lasted only 10 min. The action. I was told to say that each time there is an alert in FDR the
people

june 16 - Friday

sunday

my uncle's going to dinner so he'll be home late. i think i'm going to go to the library after dinner.

july 9 - wednesday

after dinner we're going to east end. we'll catch the 8 o'clock show. then we'll go to east end to see the 10 o'clock show.

july 16 - saturday

we're going to the movies. we'll see the 8 o'clock show. then we'll go to east end to see the 10 o'clock show.

ref: A60517
Monday, January 7th, 9:00. Another
English teacher's
forceful exhortation
not to waste
away the
morning
led us down
to work—French, De Geer,
German, German,
Science, Science
in addition to
regular morning
work. In German
class, Frau
Schwarz was
also having
great problems
afternoon.
Afternoon,
Bund and
Science. Frau
Reineke was
at the
Chemistry lab,
Bund was
there.
After dinner,
Bund, Science, Frau
Reineke, and
Science. At
the end of
Science, Frau
Reineke was
beaming
with pride.
Score: 90...
ref id: A60517

Finished at 12.45. Lunch with the Jewish crowd. Subsequent meeting finished its work at 3.30. Rest of afternoon on various committee, approved of draft of minutes. At 7 p.m. passing through hotel took by me to AH Cocktail party at the Hotelam, at 6.30, small gathering of several wines. Enzo Jones took us in his car to Western Sands Driver - good soup & fish - and then an hour's conf. with T and McC now ready for bed at 10.30. Hotelam insisted I see the post medics, who gave me some pills & opium. Went to sleep like a log tonight as am very tired after several nights poor sleep. T & H considered what program is for rest of week. I too stay here until Sat. They pro to go in to Sen. tomorrow night or Wednesday. AR said or asked me if I wanted to go home with him next week. I think he was quite nervous. But we pointed out some things he had read which will take more than a week to me. Note: I've not received any word from Cochrane commenting upon my recons that I be allowed to stay as long as I think we should.

Wednesday, May 12. An excellent night's sleep. I heard two alerts - duly in my sleep. There was a fairly heavy raid (No planes) over London on Sunday night which we missed. What it was last night I don't know yet - the weather has been lovely for four or five days now: Brilliant sunshine and mild temperature. Even the English are surprised at it. Bar was a Colonel Light from Falmouth at our table last evening. He comes to Bp every week for a day, representing himself - he knew all about me. In daily

57
The British have descended all AH person alike pretty well. Also the food is not as good as usual. None of us, etc. - I think I gave me pretty good news about what is going on. We shall probably do things on the contrary, however. Let's just go on and see how the controversy develops. We shall probably do things on the contrary, however. Let's just go on and see how the controversy develops.

Wednesday May 15th. - Good sleep up at 8:30. Woke up about 8:30 a.m. with a cold. Yesterday a dear old lady (she is 60) gave me a bottle of cough medicine. But it has been anything but good. This morning she asked me how I was. She replied, "I felt much better." I said, "I just couldn't allow such a lovely patient to be dismissed so soon without a cold."

"To CP" by bus (unintentionally, CP operates its own service, which it had to set up in order to get personnel to work) scattered as they are over the countryside, the service is good. Great day in TIVS. Going over CP at all times. I thought about going to CP and sometimes came with other two. But at night, I went to bed early again at 9:00 p.m. from 8:00 a.m. and...
I don't know who you are or what you're doing, but I'm sorry. I've been through some tough times, and I might have done some things I'm not proud of. But I'm trying to change, and I hope you can give me a chance.

I'm not perfect, and I know I have a lot to learn. But I'm willing to listen and grow. Please don't judge me too harshly. I just want to make things right.

Thank you.
just a handwritten. Yesterday saw
news doubles - very hard - just
counted 70 & station wagons - a dozen
large buses today on station at 12P
perhaps the full complement of transport
but am not sure - my cold is im-
pressing very slowly - this evening my head
well stopped up but otherwise ok. I
think this bathing in bath tub not so
good for me as showed - probably catch
more cold every time no matter how
speedily I make it so have no chance to
use cold water afterwards - glad I
drlected bathing - supply is getting low
though can buy it even at 4P where
it is reserved for females number 1
US press also. Diesel was right when
she suggested BOT as I've had occa-
sion to use failure to do so. Got my
laundry back today - 2 suits, 2 pants
4 underpants, 3 pairs socks, 2 handkerchefs
or borrowed from Al, who assures me he'll pay. The $10 or 20 is not enough to enable us to live at Park Lane - when I spent more & where other things are considerably more expensive, such as to the barring a pint. If I make it on the 9th we shall do very well. Can do it at Webster.

Sounds easily enough, I think, though I am not sure what the cost per day is yet. I got a check from Al for £10 before he left. I will have to use it as I left £15 probably in my folded at the embassy before going up here, failing to realize I would be back here for couple weeks. I shall manage somehow, though I hate the feeling of uncertainty that comes with shortage of funds. I have only $20 I $100 travel checks left & £150 cash at embassy. The £15 mentioned above - saw a farthing of 18 planes flying NW tonight - tomorrow is our 23rd anniversary. Jim
Friday May 21st. - Woke up until 2:15 when decided to take pulse pill. Damn this morning! Guess the long days without physical exercise are responsible for poor sleeping. As I can't figure anything else as cause of course, what I'm doing at 10F or 11F is very thought-provoking. The painting of our set-up is the thing, and what we shall have to do on F or 10F when we do — today is our 21st wedding anniversary, and I'll try to get special work to Elizabeth thru my department but am somewhat embarrassed to ask favor. Writing this while waiting for bus to go to work & am sitting on a stone bench at the corner of Waverly Place, by lamplight to last week's draft, the children going by on way to school — did get nice message off to Elizabeth thru country I'll mention to her all day continuing on. Intrigued of set-up here. Quite complex organization and detailed record keeping to ensure that nothing is overlooked. Checks & cross-checks...
A plan: To move from the coast towards the mountains, gathering resources and building a base. From there, a strategy will be developed to confront the defenses of the dominant power. To ensure survival, cooperation and support among the allies will be crucial. 

Preparations have been made, and the stage is set for the upcoming battle. The roads are clear, and the elements are in our favor. Victory is within reach, and history awaits our triumph.
is just never done. When the booker does
his pitch the crowd — maybe thousands
remain perfectly quiet — an hour be-
dine in which I called it. Not consid-
ered correct to cheer or yell. After a
good play there is restrained applause.
Game is fairly interesting but not nearly
so fast or exciting as baseball. I think
Americans would regard it as deadly dull.
Back home to meet the father-daughter
Margaret — unknown quantity before arrival, her
schoolmate who lives with the D's — Paulyn
Platney — and her D, in uniform—some
hospital aid or other. They are all very
friendly and pleasant. The girls rather perky
here. G with pay how a very nice free-bar
spot good. A couple of gin & bitters & han-
diner at about 8. Lunched to go & look
news, chat with D, re Official riders. D gave me paper of proposed barn of race.

with Taylor, in C & sell our future solutions
in neutral & allied fields. To drive at 11 15,
& a nice bed in the D's big room. He being
a scholarship student at Washington.
apparently a very unusual and good
student, good athlete. Good at tennis.
Sunday, May 22, 1240 at 8 30. Breakfast
of a very fine soft-boiled egg, cereal, tea.
6 45 then in taxi to D's golf club.
Tunnel Road Golf & Country Club. A couple of
friends of D's, uncle to me & D is the
other. A lovely 18 hole game in which D
won by 1 point on the 18th hole. The course
is really very picturesque & quite difficult.
Considering my lack of practice it was
my 1st round of actual that I marked
greenly, when I found I could still hit the
balls fairly well. Played in my ordinary
clothes at 9th hour after having just
hit a bit on 1st drive (remember that Terry
fell flat on his back on 1st drive here)
My driving was usual pretty good but short shots and putting poor, as usual. Anyhow I wasn't a duel & felt pretty good about it - A mug of beer & home to town. I played golf (shuffling - only 3 rounds but turn out in the country - well I guess it is cheaper & that then it would have been at home - Dinner, good food. I was pretty hungry. Read paper a bit & had or tried to have nap from 3 to 4. Then to go into & the girls to tennis court where we met. The girls were watching them play. They pretty good. All of them. The 3 in is a young woman named Caroline who is good at Stanford School. Economics. We had some tables at Stanford 4 coming over to take part in the course there & 4 coming over to Washington to study. Exchange girls - which wouldn't be bad idea. Both - forget to say we had the beef going out to tennis. Dinner at 6 & tea at 8. My feet hurt - not too much at a time - so a good idea. D is a lively man for his age & is apparently good at all games. He could easily turn me at tennis if they had good tennis balls (which are non-removable) the game would be very fast. It is quite fast as it is the young D girl is an excellent player, left-handed. She & Paula are pursuing secretarial course in San & will probably go further. Probably get secretarial work in foreign D. If not for war would have gone to Europe - learned later from J that D had been on international hockey team in his younger days. After tennis lunch + home after a mild rest. It was sunny but where I wanted to be, so, rest for us. Left late again. Missed 10 for 11 dinner, chicken for a first meal. Sat with the folks, helped with - - Cross-word
Puzzle contest, famous woman of 19th and 20th centuries, then dinner or a late meal, and I did the dishes thereafter. The daily routine included picking up things but good D, and I did the dishes there is no such word any longer except among the very wealthy. I suppose. Even the Davidson's, when we were in New York, off in a call, the house was arranged as a rule, too. The D house is arranged. The D house was arranged as a rule, too. The D house is arranged.

About 11, having agreed to stay overnight, the D's family got ready to go on with D in the morning. In the morning, I went back to the hotel. The evening was about 8:45. Listened to radio for a bit, then over to KOP. Didn't sleep well. The absence of noise made the ear seem sensitive.

Every morning, I rose early and with a short addition, I rose early and with a short

About 6:30, much joshing, before going to bed, right before, about his having to be careful, not forget to take a shower. Very well,
to bed very early to escape the rain. The water had no pressure though.
It was very, very quiet outside for over an hour, and we knew it at home. Clean
kitchen felt better after lunch out of day
before, which (as usual), reduced my
"itching" feeling when waiting to eat.
Breakfast of toast, butter, and orange juice was
still raining, so took umbrella to station.
Got into train, still raining, but gently.
Now the train doesn't pull hard
here as it does home. (Right now it's
raining, but you can only feel by looking
out the window—no sound of it.) Am
writing all this on Thursday. P.M. I got to
J's office, left my bag there, walked to
Embassy, saw I.A. J at Eric's, then it was
raining. Need to catch up on
what all. Had telephoned home twice
last time I saw John. Gave him some of
what Lord Levenham gave us and a
few minutes, need to catch up on
what all. A friend telephoned home twice
last time I was there. A friend came for me
from London, going down to London.
He seems very capable man was put up on
Languages (Stefan pop) at Cambridge
has been here about 2 years. - Also had
with Teltow and in New York, waking up at 8
who for next 3 or 4 times here. Brief talk
with here from Johnson. Who's back from Egypt.
other parts. Will probably return to India
via US. - Fin wanted him to stop by to see
us. Chilly wet all day, so slept most of
on back to hotel at 6 30, met
Col. Syrett again up for his Tuesday round
of 12 map. Started him have dinner up here.
set to table at noon, dinner time (7 30). Left
in his one after hearing him and his had
of his Egypt work. He had been back war
over. Things up to did not propose get
- for some years thereafter. Have dinner
after which I immediately went up to
my room to write letter to Mrs. D. and
wrote to Prof Adcock for book.
his clubs plus gift of the 2 golf balls
bought with me from Washington.
...
REF ID: A60517

It took a small pull from Washington but didn't do much good. Another early rise at 7 a.m. Starvation is not at all refreshing. Down this week so very exhausting mentally. S hope to get through with it soon. All quiet again right as far as alerts are concerned. Another thing must ensure relaxation & change. From daily grind has me stayed up, I guess. Am well warmed about a thing in the world, no. It isn't that which is weakening poor sleep [Another funny thing is that I'm past sick. Just on days when I am "tense" I have horrid dreams. I sleep well at night, but when don't have dream, sleep not so good. Have to keep long nights for many days now, will I could, but this mystery of myself S well, no much work.]

Tuesday, May 25th: - Up at 7:30 to have early breakfast & go to RVP in car sent for by Syatt. Got to RVP at 9:15, and started in to arrange the many notes she collected.

This week, Lieutenant not there yet. Syatt & I in talks re. any future activities - where will we be going to Bero Manoe. Sh be much bigger. Syatt wanted to know how some he had it been asked about it - as far as can, in his presence. I was quick to explain. Schedule only made up last evening & intention to consult him not yet able to be carried out. Lieutenant & Maj O'Connor (Eddie Hastings staff) came in & had Chief talk with CC. Seems to be nice chap. Explained situation to Syatt & Bero Manoe to Lieutenant - Birthday & another new had up with Syatt. Plan is for Taylor, McC. & two men myself to make west with Syatt next Tuesday. Weakness further talk with Prof Vincent, who explained it. Nay. Should still preach as those people engage in - it seems a good system. Then to Wing (black) Jones for preliminary outline that 3 or until 1 I suppose. Then to lunch where met Admiral Syatt.
I was called by Mr. Simpson and told that I had to get away as soon as possible. I packed my bag and left immediately. Mr. Simpson arranged for a taxi to take me to the station. It was raining heavily, but I had an umbrella. I arrived at the station just in time to board the train. I was relieved to be on my way to London.

I arrived in London late at night. I went straight to the hotel to get some rest. I had a good sleep and woke up early in the morning.

I spent the day exploring the city. I visited some of the famous landmarks such as Buckingham Palace, the Tower of London, and the British Museum. I also went on a boat tour on the Thames River.

In the evening, I went to a theater show. It was a wonderful performance. I enjoyed the music and the acting. I thoroughly enjoyed the show and would definitely recommend it to others.

I spent the night in the hotel and left early the next morning for my next destination.
REF ID: A60517

probably passed—he has a very much better than yours. Now waiting for 5:30. After I ate the croissants signs there are some of the names: Fanny Stratford, Stony Stratford, Skewley House, Newport Pagnall, Woburn Sands, Woburn Forest, Skewley = funny names, all except London & Stratford. After yesterday’s rain today it is very bright sunshine and warm. The sunshine is too bright for me. I had on my longs yesterday and felt pretty comfortable. So far, so good. Today maybe too warm. Have dinner schedule today through 3:20. Might go out to dinner at 7:30. Here comes the bus = 7:15p. Waiting for dinner. Had a very full day. It can deliver schedule again as 3:20. Finish, but 3 will be late. The schedule is all wrong again. But most interesting stuff.

Just some very interesting chain today. Winding up with a brief German on radar. Lunch today was rather formal affair. "The Chief" appeared rather suddenly in the premises. Something special for lunch I guess. Do say put him at least a table & I on the C's right as guest. Sorry, I was particularly nice to war we had pretty good talk. Re: educating some of our newer allies & dangers that of security measures, possibility of his coming to U.S., poss. of German coming over here. Word about people going away and signs of suspicion & reading (Sp and sq) & pills. Situation = must look into it. He said: "V week after from John dated May 10 and also one from E date May 12. Flash card but one letter from me—V week before. Apparently they've posted in British FO never arrived yet. Doubt if it will. I've written very few letters & hope she understands.
Thursday, May 27 - (Written 26th) Not much to report of unusual nature. Good night’s sleep but not enough — catching up I guess. Worked hard all day until it was then decided to knock it off for couple hours in sunshine as it was lovely out & I had finished up that study. Was to be guest for dinner at Tiltons’, so rested in T’s office in women’s chair, almost fell asleep to T’s house where had nice dinner and pleasant chat, some history on E., until 10:30 when bus was to call for me. When didn’t show up at 10:35, went back to B.P. & searched it but it never left theeli. 11:30: got dark. Arrived hotel at 11:30 steep climb but not dark yet. Turned in soon. For an hour or more could hear planes passing by — must have been big raid on Germany soon. Will be interesting to hear news soon of what part.
REF ID: A60517

Friday, May 28 - up at 7:30 after very good sleep. Wife and I picked prey. T's mother provided breakfast and packed bag as we were going to spend the day after trip to Oxford. Prepared to stay in 2-3 days then return E/P for 2-3 more days. To office where prepared telegram. Condemned re failure to answer one from here at least 10 days old. They seem to be very slow in getting answers across & quite embarrassing to me. Just after preparing draft was notified one was coming in from S.A. so decided hold up mine. But since we are here I had undertaken to make trip to Oxford & car was waiting decided to go on it. Next went to E/P to see what action might be necessary on work return. We left E/P at 11:30 and had a very fine motor trip to Oxford, about 50 miles southwest of E/P. It was a very excellent and the scenery quite very lovely. Saw many very old houses on way. Arrived Oxford where drove up to Mansfield College. Had a stop at pub, Hox's show on compilation Hox met us at door & took us up. Had a brief luncheon chat then took us to walk of about 10 minutes to our hotel. Through most interesting part of Oxford. Hox pointing out places of interest. A lovely city. Too bad not having better chance to stay there for week. But because so much work being done there now in practically all the colleges, no visitors are permitted. Had nice lunch & walk back to Mansfield by different route. Oxford
As I was leaving this morning, we passed the office of the Printer and Publisher, Johnson. He is a man with a large collection of books and a large library. He has just published a new book, and is now working on another. The office is very large and well-organized. The books are arranged in rows, and there is a large collection of old and rare books. Johnson is known for his expertise in the field of printing and publishing. He has been in business for many years and has built a reputation for producing high-quality books. His press capacity is 7,000 books per week. I was told that he is very particular about the selection of paper and the quality of his work. The office is quite spacious, and there are many large bookcases filled with books of all kinds. Johnson is a man of great skill and experience, and his work is highly regarded in the publishing world.
To go back, left at 5:30 and took a different route. Back the lady driver was not familiar with this route & I got lost several times, no street signs or highway markers. All have been taken down & not yet replaced. Saw some more even level, country & old houses, some going back the 15th C. Arrived off at 6:45 & took look at hotel. From Wash. Nothing to get excited about but was amused at tone of superiority at one spot. If Condominium comes over here will learn better. Letter from E. has been originally sent U.S. and correctly addressed but returned to "unknown"!! E. complaining lack of mail but too little meaning.

In new environs on what is called a "Parliamentary Train" it stops at every station, a hangover from a last passed long ago. Figuring plans of all trains, I understand they run at 7:20 and due at Euston Stn at 9:00. Will be too hot to meet. Z. did office's work, as agreed, so will probably get dinner at Park Lane if feel hungry. But I still have bit of a funny cold. Despite good physique last night, I think will be more humanoord though. No one thing it goes badly enough so can write fairly legibly. Secondly, thus far though we have paid for 1st class seats we having never bad them—the trains are so crowded. Our apparently people around the Parliamentary or also it is at a time when few are going to& from. I had good chat with [deleted] today. According to his version of Finland we can't claim most of credit & I shall want to talk to [deleted] about he
this Dr. I was in top form from French who pointed 1st page of notes in book taken by looking over shoulders learned how system worked. He also claimed credit for discovery (accredited by Pat Barkey & deduction by him) of reciprocating motion of book. Says we made a bunch of something & when I mentioned book sheet in paper he flat no. Also talked about our respective org & I admitted pleased to see we were greatly overstaffed for what we do. I am impressed with volume work done by these people per capita, under heavy physical handicap. I wonder if they aren't really much better workers than we are despite our modern mechanization, fine offices, etc. In a technical sense I think we are way ahead of them but in a practical sense, judged by accomplishments, these ancillaries (most of them real good but in my opinion) have been largely surpassed vis-a-vis detail attention to minute, digging out even if unintelligible. I applied high class thinking arguments it seems to the task their key personnel are of much greater capabilities than our. I think the place abounds with able, personnel of highest type licensed men who are used to getting much done in a quiet way without fuss & feathers. A very great deal of handwriting is no virtue in done even at the top. Their papers look dirty & messy, their card indexes are terrible to look at & yet they have the data & know how to use them. For as we would not put up with the printed slip produced by Types, & ragged paper, it bothers primate Barkey many.
Réf ID: #0517

With it OK. They posted slips on back of memorandum paper. They pass important info on dirty little slips of paper & during the day don't seem to get lost somehow. The rooms they work in are dirty & messy & cluttered up their toilets are few & terrible! But they get things done & you should see the exps they drink tea from—well, dishwashing facilities are nil, with a wonder how they can maintain themselves around. They must have their tea of course—10 30 & 4 30—but better than the coffee habit.

We are nearing the wood & will cease Saturday May 29th. Up at 7 45 am. Went straight to breakfast. From last night a bit late. I went to Park Lane where room had been reserved for me—a lovely double.
If it was a fact criticism said he had not noticed this, Ali said nothing had he but I agreed vehemently with me. I had been invited to Beau-maron, about which later. By the way the few street ladies were in the chest; fairly good looking but I didn't get close enough to verify. Back to hotel where took nice bath and went to bed about 11. It was an odd thing I learned later that Tel-Aviv were both working at the Embassy until 11 but it never occurred to me to phone them or walk over even to see if any messages or mail. A curious psychological blank spot—wonder what it's significance is. I had very good sleep.

Saturday, May 29th: Up at 7:45 to get an early start as had plans at Selfridge's tomorrow at 9. Train is leaving 7:20 now. A Sig C affair to which I'd been invited by T.R. All day tour of Sig C local work and places for summation. Sig C officers in post near film. Had interesting tour through Signal center & Photo establishment etc. but not through any Sig intell crypt. Signed as guest of T.R. Rumbrook with about 30 others, at Mansfield Hotel where Mr. Lee (C is GOS) has his private. We had a very good luncheon at good as any could get in peace time. Wash at Mayflower. Spoke with mail including marked (have mentioned these one or more times) as called serments, if you ask for marked the gals blush as that is what they use here for maudlin cloth), rice, salad & sparkling goblets. We had cocktails first then grape juice (not grapefruit juice) good soup; curry & beef & rice. Excellent. The potato soup, real white or almost
white flour rolls, scones & delicious sweet pickles & a very fine open-face pie consisting of pump

mum base with cherries topped by layer of strawberry jam. After short interval during which I tucked by cab to Embassy to see what doing & see Jodge. All for few minutes, took cab to next place on tour & continued with party until 5.15 then took cab to Embassy to read messages that had come in & been sent. Filet pemmican uncooked. Time passed very fast—it was 6.30 before knew it—had no time to go to hotel to wash up before going to Ann Sig C dinner, to which had also been invited. Chummy was all better this morning so felt I could enjoy food. There were over 200 Sig C officers & Kran. Diners CGEto ETO-leave, together with Dir.
went after very brief speeches. Devor made curious slip when he introduced
Sir H. Dever as Great Colonial Dever. Of the entertainment the best by
far was a Sgt. Travas who was on
singing staff NBC or CBS r. who has
a marvelous baritone voice. much
prestige appeal. Affair was over by
10 15 and I walked back to hotel to
see if Tel 1
t in his room. Wash up & talked
with him until 11 15. He & I very much
dissatisfied with ways from Art to me which
makes it seem that all the ways we had
been sending back made no impression,
were so much water so far as concerns an
understanding of what is going on here.
After that went out for few minutes short
walk in the blackout, walking up a drain
in front of hotel. Recalable. In the deep
Bull's Head Quarm (Chow)
Syracuse State
Shadows of entrances to plopo would dark
figures (occasionally) prostitutes on the
pavement would peep to me as I passed
by. In bed by 12 30 and good sleep.
Sunday May 30th. - Up at 8 30, breakfast
after bath = kipper & eggs good & it was
good. Pack up my belongings as de-
vided to keep up my expenses now the
not occupy rest of day or next 3 days.
Got prepared to go back to Tiffany
town. Jesse and I went to Embassy
where found second more message, one
informing me about leaving in future
fashion it really laughable. Can't un-
derstand why should ask for such de-
tailed info re intercept set up - They had
leadership in 1 field by agreement to
be used to excuse it all. Well, if they
are qualified to exercise it why don't
they ask the questions? Spent practic
ally all depart Sunday up to 5 pm

giving over messages, preparing replies

To enquire had come in lunch at

Offices were at 1.30 with Ted + At who

had just returned from overnight stay

in the Demilitaris. At 5 hour to St

Panamas Station to get train for Beaus

masar, large unit TN War Dept

called W O Y G pronounced "Wyg"

War Office I group Ted + Scott, whom I

mentioned before in heat of their activity

(among others) and it was at my request

that he arranged for itself coming along

with us. Company arranged + reserved

for us in first style with proper quarters

at ATS then as RTO representative A

3 hour journey which passed quickly

I began immediately playing jeeves

with questions + writing notes in my

book. We talked about bad news &

all about my great ability at that

sort of thing. I thought I would have

been a bedrooms. Got lot of good

info through on his side, where it

fits in general scheme, his official

relations with RAF or other groups.

After we had exhausted him I started

in on this story, rattling up to point

about middle of p.m. when we reached

Longborough, where Mr. [Redacted] E

Ellingham met us with big official

car & good looking driver to take us to

our Hotel - the Kings Head, where we

had rooms reserved [I]enjoy go to

runner found ought of company. +

wondered a bit but, merely assured

things as advertised with behind

as for house + pass under bed, tooth

brush I could see two rude occupant

but as regarding the group below

mentioned Ellingham for courtesy

in providing us with a sleeping con-


...person who, I hoped, was good looking. Much laughter at this I failed to report findings to management to forget about the matter until return after midnight, when doorman asked that I'd been given wrong key to that my belonging had been moved much laughter against. After quick drink we journeyed to an ancient inn on Beaminster (about 3/4 miles from Sturbridge) called the Bull's Head.

A very interesting place filled of people in the pub - nice surroundings had good dinner - nice table, white linen etc. House to suit taste -..

Last tour around - from 9 to 11.

After eating put up too long to explain less must on a few words about the central house - was found one central home of William P. Herrick, father of the poet. Robert Herrick, it
Monday, May 31st — Had good sleep
till about 1 when truck going by woke me & I stayed
until 8. Breakfast after bath. Had again
a nice supper! We then journaled to
station again & went into some things
more thoroughly. Al had undertaken
to give cocktail party on his wedding
anniversary & on account special cir-
cumstances be left ahead of us, at
11:30 I had promised him to come in
to town to attend but finding how
connections sufficient decided to go
direct to B/P w/ Al with Lyalt. I
hope Al will forgive me, but I am
so pressed for time & felt I just
had to get back to B/P today.
We had lunch (Taylor's, Lyalt,
Gelling with it). Wrote Chin depot &
got Bulls Head大学. Then re-
turned to station to pick up truck
then a very nice ride to Vegrove (Taylor &
we went back to town by train (from Roughmouth).
Announced B/P found plenty to do,
calls to make, talks with Delfrey, Mark,
Kay, Gulliver, message to announce the
grace. Came back. Worked late till 9.
6. Then with Lyalt in car to Lubin &
Sandia. Had my room plaintiff. Hope
the large double bed is a bit more com-
fotable than small one last bed.
Finger room, too. I bought double
scotch for Lyalt & self & we talked
the dinner twice. Left, played a
bit of "bowl" with him until 9 p.m.
Have been writing this since
9, 15 & it is now 10. 30. So many
things to do & have not yet written
the letters I should & I know E &
mother will be grateful but what shall
heordes can I do? Shall have to wait.
Tuesday, June 1. - Worked until 10 30 and then went below to have dinner with Col. Lynch. We talked till 11 15. Then to bed and had an excellent sleep. In the morning up at 7 15, breakfast at 8 15, then with Lynch in special car to P&P, arriving 9 15. Started in work immediately on wages to wash. Having come in to have classroom with him, got him to agree to give 0 15 on #61253. Washed wire, wrote on return. Mr. Vitter asked to see me in the afternoon. I went in at 10 but didn't get to have till 11 a. m. Mr. Tilton and I discussed wages to wash, he approved my draft. Later Mr.
From my headquarters at Attock, Sir, I have the honor to inform you that I have received a despatch from the Governor-General of India, in which he expresses his entire confidence in my efficiency and discretion, and authorizes me to proceed at once to the relief of Delhi, should the necessity for such action arise.

I have already taken measures to make all necessary preparations for this purpose, and I am confident that I shall be able to effect a successful advance upon Delhi, with the aid of the troops at my disposal.

I shall be guided by the advice of the best military authorities, and shall not undertake any operation without the most careful consideration and consultation.

I trust that this information will be held in confidence, and that no unnecessary delay will be occasioned by the transmission of this despatch.

I remain, Sir, your obedient servant,

[Signature]

[Name]

[Rank]

Vice-Admiral, British Navy.
day yesterday and today Auntie
and I was glad to have my
sweater on. But it was cold and
yesterday from Prof. Soace but to
a day got out of my own — how 10.30
and must be bed. I will try to make
earlier than tomorrow so as to get
two good stints. Have to do — all
out of my PX cigarettes this evening
I had to buy but quite ex-
penose. 2/4 for packet 1/20, which
is about 45¢! Used junk cigar at
that. Compared to ours.

Thursday, June 3 — Set my clock for
6:30 but was sleepy and didn’t get up
until 8:15, after my shaving water was
brought. A good sleep from 10 45 to
5 and then dozing until 9:15. It is
still sunny, cold, and overcast. No
special news in papers this morning
but all papers giving headlines to

— Remained pretty nearly all

— Forgot to mention that one of nice
things at the Tavern is that the food
that is meant to be hot is invariably hot & the plates are always
heated. Good food all round —
must have sanitary or precautions
of British catering. — Hiltman.

away today after Sunday Smith who
I must see at once today. A
disabling answer received from
Arlington to query I made re sec-
urity of stay. Looks like we’d
stay work has been going on pow-
ether. — Raised pretty nearly all

— Forgot to mention that one of nice
things at the Tavern is that the food
that is meant to be hot is invariably hot & the plates are always
heated. Good food all round —
must have sanitary or precautions
of British catering. — Hiltman.

away today after Sunday Smith who
I must see at once today. A
disabling answer received from
Arlington to query I made re sec-
urity of stay. Looks like we’d
stay work has been going on pow-
ether. — Raised pretty nearly all
REF ID: 18020

Tell have missed luncheon.

Story about passenger plane shutdown yesterday. Long notice at 10:30 p.m. in another bus. Tellman there - no message. Phone Embassy and get Taylor on phone to call Col. Syman to tell him we would not be able to see him until next Monday or Tuesday. Tellman's secretary brought back letter Ed posted yesterday to go in 10 p.m. coach to Maidment. She telling me that people there hadn't talked with letters so they'd not been canceled. Received one from Elizabeth Martin today, one that didn't reach. She ecstatic about the news which came on 21st. Not saying making re the number which I expect was 2.84, with exactly 28. Spent some time with Mr. Thompson's phone worrying and by JMA. Afternoon with Freeborn and IBM. Then settled in exchange.

Mrs. Rodgerman phoned to ask when I would be coming to see her. Others have told me how amusing she was to see me here at 5.30 and brought couple round to her. Clarkie & self be the oldest living JC&CS members going back to 1916. He is quite a talker. Got him going on Red Hunting. Says Falkland story a month or two ago he called up Freeland, also Hoarly in Bedale. Story = Fish for dinner again but very good. Felt very sleepy after it came up. Lay down. Fall asleep for almost 2 hours. How 10:30 p.m. — cen all out of matches, can't find it. Have but 3 British cigarettes, no pipes. Asks Taylor to bring me my cigar box tomorrow. Hope he does.

Welcome J. WO. in Bob phoned me today, to want to make date to see me. Set next Tuesday.
Friday, June 4th. Up at 8:30 after good sleep. Toasted eggs on toast for breakfast in addition to the usual porridge, i.e., oatmeal. This is day that A+T are to come up for final conference - the rain is gone, I think, but it is rather cool. The sunshine will warm it up today. Stop.

The post office in the village center is not open yet. At one corner is a man's comfort station.

In the large town there are very well kept places, with an attendant - for different from the usual European type.

In one, and these places are free and well patronized by the populace, high cup of coffee is 10 cents. Bus coming at 7 pm. Had a very interesting day. Expected to find A+T Telkwa when I arrived at 9:45 but they were not around. Work came later that they'd be unable to make 8:15 train and would be on 10:45, which got.

In at 11:50. Have to cancel research section under Wegner. Interesting talk on Surgeons and their functions. Saw looking younger than Cambridge - math every day. Finished with them at 12:45. Learned A+T had arrived so.

Jewes in Dr. Hay's office until Littman Decided to answer AE with this.

For bottom for him - one at a time, after one sort of thought - Oh, yes, another one for you. It went off very nicely. AE was tickled. They brought two bottles of port, one for me as present to Littman, which was nice. Other present to me. They had some clothes for Etow in for drink. June 5 being Etow's observation day over the world. Stuck at Grady today, too, as Etowish than once lunch. Khan, Johnson has a field day at farewell so he is off to U. S. on freight ship - left lunch, which was
•


We walked in the park near, after which we went to a restaurant to eat dinner.

The food was very good. We talked about how much we enjoyed ourselves.

I have never been to Rome before, but I had heard that it was very beautiful.

We decided to walk around the city for a while.

The weather was perfect for a walk.

We found a great place to have a drink.

I was so happy to be in Rome.
with the rather common Bulky type of an Etales) and a sweet smile, pleasant personality. I imagine her to be about 25 but may be mistaken, (A)rmstrong is intended as memory guide for our Mrs. Adams at 11) - nice demeanor, after which we sat in the lounge and talked until my bus came at 10:30. - Home at 11, still not dark. Great wind. I was leaving the same in morning. Pack up my things. In bed by 1:15, but somewhat wakeful. - Sleep by 1:00.

Sunday, Saturday, 6:15 - Up early (7:30) finished packing breakfast, bus at 8:35 - now at 8. Winding up affairs. Flew from U.S. yesterday.
day which I've not seen you
true general content of which
phoned Ted by El. Elizabeth
Boys would write any more on
make any comment for
I can't get dates for research
started on E.-Had talk
with Delrey on this point it
can be see while in -
A. in - Following being written on
ensue to Stock-on Trent, Tuesday morn-
my J.-Had a quick cup with Delrey and
E. works for A. 1. We asked me to draw up
freight on it, which I finished through in a
few minutes before lunch, at which Ted
So they present - Immediately after it
we showed up to see - Byron's Pool - a
small pool in the village of Stock-on-Trent
for Cambridge, despite ominous -
weather and dark clouds - It had been
namely pretty hard all morning and
it was still not finished. The car is a quiet
old one but was among the most expensive
models in its day. I was a bit appren-
tive at Vincent's handling of it as the
road was very wet and the car did not
start too well and Vincent kept changing
driving at high speed sometimes as much as
60 and for considerable stretches 50 -
the roads are seldom straight, often very
narrow and you can't see more than
100 yards ahead. However, he didn't get
us there safely, passing through some of the
loveliest of English countryside. Come
bridge is 50 miles from B. and we were
only 1/2 hours en route. One of the places
we show up to see - Byron's Pool - a
small pool in the village of Stock-on-Trent
for Cambridge, despite ominous -
weather and dark clouds - It had been
namely pretty hard all morning and

The Great Plague in the 1660s was one of the worst outbreaks of bubonic plague in European history. The disease, caused by the bacterium Yersinia pestis, was transmitted to humans from infected livestock, birds, or rodents. The plague reached England in 1665 and spread rapidly through the population, causing mass death and social disruption.

In London, the plague affected not only the poor and the sick but also the wealthy and the powerful. The city was divided into quarantine and non-quarantine areas, and specified rules were enforced to prevent the spread of the disease. Vaccination was not yet a possibility, and treatments were limited to remedies such as bleeding and the use of herbs and potions.

The Great Plague had a profound impact on the city. It led to a decline in population, which lasted for several decades, and contributed to the economic 和 social changes that were occurring in Europe during the 17th century.
Boating on the river is now legal, and life on both sides of the river is very pleasant, with the few remaining students and the growing number of tourists. The river is quite wide, and the bridge connecting the two sides is quite an engineering marvel. The city has a rich history, and the castle on the hill is a testament to its past. The university, founded in the 12th century, is one of the oldest in Europe. It has a long tradition of excellence in education and research. The current chancellor, Dr. Jane Smith, has been in office for five years and has overseen many changes and improvements to the institution. She is a respected figure in the academic community and has been instrumental in increasing the university's international standing.
incident in the "Masters" (President) of
Queens College. This office grew by
-notation to the heads of the various
Colleges. - Saw also, Clark College, and
"Saw the Water Supply" provided by the chap who originated the
"Hobson's Choice" catastrophe.
- Stopped for a few minutes in King's College
Chapel, where afternoon prayers were in
progress. Choirboys singing nice. The
old stained glass windows have been
removed for safety at Cambridge's request
near the steeple and in well with the
- bomber area. Saw lots of guns and...
in that old, tall high body with a view looking down into the churchyard with
ancient tombs, etc. There was a "man" to take care of me. He took out my things
and then out carefully: my chemise, trousse, etc. My father laid out, and in the morning
I was be would have bathed and dressed me, if I hadn't been done.

- A "modern" bedroom (about 1810 or
thenabouts) with a separate room for the
- Despite the age of the building
- around 1500 - it is clean and com-
- We went to see Venice's "officier" or private chambers, which is
- A most delightful place
- even without the furniture in it. A
- large study, a small bedroom, a
- tiny kitchen, a lovely view into the
- "yard" or "court." - Rain a few min-
- utes, crossed up a bit, and then we
- I went to the dressing room of the
- Not the master's table or High Table,
- Not the head (Sir Well Sprag) before
- going in to hall, where there were all at
- and other old professors and lectur-
- ers in the gymns - plus three French
- generals and we are marched in. The
- report of whiskey - then fell into dining
- hall where the boys were all sitting
- patiently at their chairs at the long,
- numerous tables, separately dressed
- each with a glass of wine. Grace was
- sent by senior lecturer - in Latin -
- the power, as has been said, the room
- the founding in 1430. - We sat down to
- a huge supper with a perfect
- sauce, green peas, boiled browned
- potatoes, and great big fruit dishes.
- Berries, whipped cream, and plenty of
- sugar. On my right was Prof. Mac-
Curiously, interested in medicine at John Hopkins but now professor of psychiatry there. We had an interesting talk about psychoanalysis. He knew a white father I knew as my gift was Prof. Thompson, also famous in physics and was EMC in biology. He was last week. Had a very interesting deal with time as he is in physics. Knows the complexities really well. Thompson is the son of the J.J. Thompson, one of the greatest physicists of all time. After that, we went for coffee, etc., in a cafe called the "Combination Room," where people "converse" and I was placed on the master’s right, as guest of honor there.

In the other room, I sat on his right as place of honor was given to one of the generals on his right, the other on his left. Coffee, port (vintage), Veuve Clicquot, and people at CCF were charming.

Now because the evening started, I put our handkerchief on table. I had very interesting chat with the leader about his daughter (43 years old) and my thoughts about 13 coming over to England after the war for postgrad work. The idea that if London School of Economics stays at Coward, OK, but if not, better for her to attend Oxford. After that, we all adjourned to the master’s private quarters where we met Lady Span and two others, one of whom I had chat with her husband (Army) who is prisoner in Hong Kong. Had whisky and coke there & chatted till 10. Host gave talk on "The Suez Canal," which is CCF. I whole East Anglia. A very affable and interesting man, with whom I discussed war situation. Back to our rear with V’s. Voisard recited some lines and recited for about an hour.
I am afraid that I cannot go. I have to stay at work. Please call me later. Thank you.
up all the way to the top of the 13th floor. Went to "views" - took about 30
minutes. Then to Park Lane where Al had reserved rooms for us. To see
us together again in a nice double room on 7th floor. Want to have
lunch, meeting Al at 11:30. Had couple cocktails followed by enormous dinner:

ham, chicken, pork, beef, pork, beef, beef, beef, beef, beef, beef, beef,

spinach, baked macaroni, asparagus, soup, salad, bread, rolls, pudding,

rare potatoes, peas, creamed spinach, chicken, beef, fish, chicken.

Tuesday, May 24th

Good morning, sir. Al's provision is many dreams. Showed mine; it included:

breakfast (good toast, fish, bacon).

Routed to Finsbury to send telegram of getting transport warrant for his trip, got to Finsbury station in good time to get a seat; and here we are. The train moves now for 2½ hours til noon. 12:45. All seats are taken. In a bit after 1 pm. [Written on the 25th: We were very lucky to have seats on the train as it was very crowded]
We should have got seats near the front of the train, having 1st class tickets, but the 1st class compartments were up front, but they were all taken by the time we reached the Fratton Station. People were standing in the aisles up there so we went to the rear of the train. The difficulty here is that the trains are no longer nowadays that when the cars are filled up with passengers who are to get off at that station, must be in that position of the train which will be alongside the platform. We were supposed to be up front, therefore as the cars for Stoke were there, so as the train came near to Stoke, we began working up toward the front of the train - no easy task with people standing in the aisles, luggage on the floor, etc. & the train rocking as it is now! At that, when we reached Stoke we had to jump down to the ground - about 4 feet as the car we had reached by first floor was still out at the nearest edge of the station platform. We were met at the station by an RAF Officer. I saw an appearance, with a car. Which took us to Chaddle, about 6 miles off, through somewhat rolling country. I think the train is doing about 40 mph now. At Chaddle, we turned left onto a little country lane and proceeded to the home of one of the local squires who had given up his place to the government for a Y station. He himself is now a Group Captain in the RAF (Allan). We were met at the door by the C.O. - Wing Commander W.S. Swanton. A tall & happy man of most efficient disposition - I had to give up at this point as train.
was looking too much, so this is being written Wednesday night. We had lunch with Swanhollow—"just a bite" it was supposed to be, but it turned out to be quite a repast, with port at the end. Then a tour through his establishment, which he has found extremely interesting. Mr. J. D. Cooper, C.M.G., made a special trip from B.C. for us with us—an act of great courtesy in view of this very busy life. At 4:30 we were served tea, ham sandwiches, bread and jam, jelly roll. At 7:30 we were served a fine dinner, preceded by "gin and French", followed by coffee and port. It was a very lovely evening and the spot was ideal—

calm, quiet, the fragrance of roses in the air and the wonderful color of purple rhododendron which abounds in the vicinity. At 10 we took our departure, in the official car which Swanhollow placed at our disposal with a driver to go 30 miles to Stafford where our hotel accommodations had been reserved for us. The driver went about 55-60 all the time over the narrow, winding roads and the ride was a thrill in that respect. Cooper came along when we arrived at the hotel he insisted on "buying us" Scotch & soda—two pounds it would not let us pay anything or return the courtesy. We had a mid-
Monday, June 1st.

We had a very pleasant train journey last night, we having left wool to be called at 9.30, with morning tea, which duly came at 7.30, by a maid who brought some and drew aside the blackout curtains.

Wednesday, June 9th.

A good sleep but with funny dreams—anyway I couldn’t recall. The idea of morning tea is a very pleasant one! I had to cook Jed to partake. He said that Reddix rather have had the extra yolk-to-please it to be cooked with a brown-saltman or a large glass of orange juice instead. But I maintain that hot tea is much better than either or both he named.

Breakfast, at which I missed a regale because the waiter brought me bacon & fried potatoes & I didn’t know there were peppers, darn!—The train just crossed the street from the hotel & we mounted at 9:39, fortunately getting past the train just finished along 70 miles an hour & I don’t feel how or why those light cars stay on the tracks. I bought a copy of Punch, read that through, then borrowed my neighbors June & read that through. By that time we were stuck in London. Got out right away, then directly to hotel. Lunch at Red Cross—no mail. No long urge from Cumberman, at least answering—a long-delay reply that should have come several days ago. — Want our
my papers, as Al had already
wired we were both coming
back at once, leaving here
Friday night! It felt to
do. — First thing was to get
in touch with Helsman who
was in town to commence
contents. Tuesday & I had a
 dealt with. Time getting him —
He had been at the embassy!
 — Dinner at the West, with
Eric, who leaves tomorrow
night. A very nice dinner
with good friends! — Went over
with Eric to his place to
collar some luggage he was
turning over to Ted. — Ted
was out to cocktails with
some friends. Forgot to
pay their dinner on Al, Ted & me. To cocktails

at the East India Club again
as a farewell. Arrived again — found Sid & Lil still
from May 4 to date — Which
is not bad at all. — From
then came over to my hotel
poor Ted came in — had a
Bath, washed about 10 p.m.
packed & left there. — Ready to
bed & next to last night in
London. — Can due home on
Sunday if all goes well.
Then worked up a bit at hotel and walked to bus for dinner. Had a date with Eunice there after which we went to his room. He being ready to leave tomorrow on his journey to U.S. He had 2 full bottles of Bourbon (figs.ograms @ 6/-) one nearly full of Canadian Club and a bottle of gin which he was taking to Ted. He carried this over to our room and after chat of some 45 min he was about to take his leave when Ted came in. We had surprise for him as his friends had arrived but had forgot his dinner so leaving was post it had not arrived here yet maybe at bottom of ocean by now. We had a drink or two left from this and then I had a bath and then Ted and I had a couple more drinks.
REF ID:A60517

I left without consulting anyone into a
U.S. club.- At 11:30 we

left, with Jack and to pay our
respects to him at the club. I

met Jack, and talked there. We

then had a pleasant chat with C. and

then had lunch there, I learned.

I then went to officers' mess for lunch,

and Ted went to Paris and to fetch

the bourbon. I bought the brandy

for all. We had a pleasant

time, and stayed until 2:30 or

3 p.m. I am and I went shopping

in Grand Street to buy some

tickets for family.- Capt. Boyd

having provided me with the

necessary coupons out of his

own pocket. I hope it will be

all right. We will like what I bring them.

I went to Embassy and to the

reception office, I having
Saturday, June 12th - Up at 4:45 a.m. I weekended by porter bringing morning tea - a very fine custom which I think would be wise to adopt. Shared it breakfast quickly. It is quite light now & we are passing through some of loveliest country in Scotland. I looked train at 80 miles/hour & we were a few minutes late. How getting in till came for time being to return on place or at Preston. - 8 a.m. Can we hotel at Park Inn at 182 feet for AFC. We got in to Bell Waldorf (I think it's spelled) at 5:40 a.m. (The train goes on to Glasgow)
and a beautiful morning. The sun was just coming up and the sky is almost cloudless. The train was very comfortable, and the compartments for single occupants are much like our most modern ones at home, with bed running transversely, warm trunk, but no booklet for reading, plenty of air. - At Bell Waldorf were picked up by AFC and after about 10 miles and I came to Park. Few minutes after I left I was to report at 8:00 a.m. in some form, more than I was going out. Breakfast at 8:30 and had excellent but
small powdered egg, toast jam, tea. Now taking it easy in hotel lobby and actually feel first winks of sleep in comfortable chair. 1:45 p.m. Had a shower at this hotel at 11:15 and the funny part of it was that there was no cold water - nearly got pneumonia!
At 11:30 the bar opened and I bought all two double soups...t...told be bought one so we each had three and left five at lunch, which was good. Sat out on the upper deck around nine watching my planes take off and Canada was interesting sight. He was in a warm but there is a cool breeze. We are now waiting to get aboard. I have passed through customs, etc. I had a momentary anxiety when they asked for my exit permit about which I felt not the greatest when nothing was said about such a thing when I signed out at the AID's office. All my notes were signed out and they did not raise a fuss about it. We were given to understand that we landed in England for an hour or so to signal but...just known for certain. United was the musical funnies! The place is quite crowded now with incoming and outgoing people—a busy airport. In the morning wrote a letter to N. today, with address I learned just yesterday. Also two post cards. The lady of my seat was quite kind to the children. After I went aboard at 2:00 and put our mittens on. They were back to get off and wash. At 2:30 we were told to get aboard, and all passengers were there, with all other passengers. There were 24 seats but only about 22 passages. It is a Douglas C-47, just like the one we came over on. Warming up covers from 2:15 to 2:45. We're off, and now over the water, set about 2000 al.
7:15 p.m. — We have found our way to the room where we found our room table — 1:30 a.m. — We were driven by a staff car to the officers' quarters. The officers were awakened and we were served breakfast. We were then driven by staff car to the airport. We flew back to London by staff car. We arrived at 11:15 a.m. We are now aboard the plane again, waiting for signal to start. The plane was expected to take off at 11:15 a.m. 

The local time at Heathrow is two hours behind London time so we have just
REF ID: A60517

Through the time figures we coming from Paris to Iceland. It is local time 9:15 here or 11:15 London time or 5:15 p.m. New York time. So 5:15 to 5:15 a.m. would make flying time 11 hours and 15 minutes. We'd see how close we come to it. Every body is now about plus a bit more mail occupying last six seats. - Announcement made that there would be no stopping at all to New York. 11:37 start taking toward runway. 11:44 started down - runway. 11:45 were up off the ground. - Climbing fast. - 10:15 a.m. (Local time) its quiet light now. We have been flying 10½ hours so far. I slept at least 6 hours of that time. I woke several times and looked out. It was never completely dark, and I could hardly tell whether the rosy color in the sky to the right rear was the setting of the sun or just the reflection of the moon. It was most confusing. The greenhouses about 1/3 of the way up from the horizon. We passed over very large ice fields and icebergs, over barren rocky country which showed us sign of life. I learned our coordinates -- must have been Newfoundland. I woke several times with this stifling heat, very hard to control at 2010. It was alternately hot and cold, but mostly the former. It is now 10:30 by my watch, hence it must be 10:20 a.m. New York time and if we were to be over we should be in New York in about 2 hours. - Hotter than hell. Land is inaccessible only a vast pool of water in which we cannot see any slight ripple. It's very calm down below. The plane is very steady. As a matter of fact...
it all quite deceptive. The noise of the prop is so like the noise one hears aboard a big ship, and the absence of scenery making fast travel (as on a train) makes it seem that we are just crawling along at a snail's pace, not 2 to miles an hour. 10:45 a.m. We have just been handed the usual customs forms to fill out. Have been told we may land at Cape Jolie or New York. At last, something is allowed. 11:30 a.m. Scott Jolie: The ice field we passed was not at our first approach to land in vicinity of Nova Scotia. We then crossed Gulf of St. Lawrence, in 1 1/4 hrs. we land at Cape Jolie, have breakfast, then on to N.Y. where we should land at about 11:30 - 12:00 N.Y. time. Depending on how long we stay in N.Y. we should get to Washington in early P.M. We're flying over clouds now, above the white clouds which are very thick but occasionally can see through them, at the forms of trees below, rivers & fields, rivers & a little here and there. - The 12:10 p.m. (S.F.) time now and I'm pretty hungry. The plane made hot chocolate an hour or so ago, which has to be thrown out as the milk was sour. I tasted very funny, quite disagreeable in fact. 12:45 p.m. We are about to land at Cape Jolie. It is very thick out & can't see anything. Going down now. Seat belt fastened. 1:08 p.m. We're on the run way now & taxiing toward to hangar. It was a very hazardous landing, as the ceiling was practically zero. We couldn't see much land until right down atop of it. It's raining hard & the weather still foul! We may have to hang up here some hours. 11:10 p.m. out the door & we were at a full stop non total time in
the car from Seattle to Pacific Jakes was 3 hours and 25 minutes.- Bus takes to passenger terminal. Customs now took up my passport-say it can be returned to me Washington on application, State Dept. A fine breakfast, two fried eggs, bacon, tomato juice, coffee, toast.- Had all flights cancelled- would have to stay overnight. Possibility of getting out on W.S. Biddle, Commercial point got a car & went there over bumpy roads. Plane to have left at 3:15 AM was cancelled & just as we got there got a cancellation on 7:15 AM one.- Then back to terminal, where I shaved & felt better. All + I then phoned about a three hour flight to hear voice of Elizabeth Bank & + John still asleep. Told her would phone from New York tomorrow. We went next door to hotel De Lank for premeints & for room.

4:30 PM Start making for a brand new temporary building very much furnished. Had a very fine dinner with both coffee which we were told to report to terminal at 8 PM as there was a ship unavailable! - Had a fine dinner tonight. Juice, vegetables, three steak, fresh - fruit, potatoes, peas, corn, canned - peaches, coffee. Then repacked my gear & went to terminal building. Sure enough - a plane getting ready. Took a long time to board up a cargo plane, converted from regular Coast passenger plane. We don't have regular seats - but what they call "bucket seats" along the walls. Not too uncomfortable. 4:50 PM Local EST. The warming up began; 4:55 took down to runway; 4:15 began the run, 4:43 up. Off the ground! At breakfast this morning the Captain of our ship told
that we flew pretty steady to have made a good landing as the information had been from the control tower was that the ceiling was 1,000 feet whereas in fact it turned out to be about 200-300. We had a difficult time as we were flying about now-pity high. I can tell you it is pretty high because below us at 300 feet are the pure white clouds so thick you can't see a thing through trace. It was dark and raining on the ground but up here the pure white clouds is very brilliant. Just unable to see through the clouds. Quite comfortable flying as yet. The copilot (Thurston) who flew the Hotel Denmark at Portland was assistant manager of the Ambassador in Washington also managed to keep in touch. We are scheduled to stop in New York and it takes about 3 hours to make the run. 5:45 p.m. we are now just out of the cloud.
REF ID: A60517

We should make the run to Washington in 1 1/4 - 1 1/2 hours. All told us to tell E when I called her to tell
Winnie to have Martinis ready +
that he was hungry; said I did.

It's dusk now + friends hot outdoors
when we too off. Not bad inside the
place but I imagine it will be tough
when we land in Washington- me with
my winter suit on + heavy overcoat.

all my belongings are here- including
my stick.- I was made a member
of the short preachers fraternity this
afternoon at Praga 19 1/2 from two
young lawyers. 19:53 -

We are
approaching Washington now
and should be at the airport
in 5 minutes. Coming downstairs
now at 19:59 -
REF ID: A60517

C.W. Drayton
Anthony Eden, Feb 11, 79
Henry Newbold, 1909
A. Marshall Foot
John E. Colcuorth, Apr 1959
Ammons
J. McG. Jackel 67
Butler Hallahan, 51
Edward S. Weaver, Judge
A.D. Laughon, Ph.D.
Henry W. Russell, Ph.D.
J. A. Weig, Army, NY
Robert A. Williamson, USA

Young is quite
approaching Washington,
got the express
in 5 minutes. Coming down now at 9:39.
REF ID: A60517

W. P. Heuer

Feb 8, 1859

E. C. H. Aber

C. A. L. L. Y. M. A. N.

A. O. Longson, Ph.


J. B. W. Perry

A. C. N. H. Y. A. W. Y.

Young ladies approaching Washington and should be at the

in 5 minutes. - Coming in now at 19.59.
CONTRIBUTIONS IN THE FIELDS OF

COMMUNICATIONS SECURITY AND COMMUNICATIONS INTELLIGENCE

1. As Principal Cryptanalyst (1939-1940), Head Cryptanalyst (1941), then Director of Communications Research (1942 to date) I have had technical and staff supervision over a large staff (in 1945 amounting to almost 10,000 people) of cryptographic and cryptanalytic personnel working on many complicated problems in communications security and communications intelligence before and during World War II. My specific contributions in these two fields are briefly summarized below.

2. My contributions in the Communications Security field during the years 1939-1945 include practically all the systems and devices employed during World War II for cryptographic purposes by the Army and the majority of the systems and devices employed for the same purpose by the Navy and the Department of State. A detailed statement is attached covering the following:

   a. Converter M-134 and M-134 A, covered by patent application (Serial No. 682,096) filed by the Chief Signal Officer in my name as inventor on 25 July 1933. This machine was the predecessor of the Converter M-134 C (Sigaba) and represented the first invention of electrical control, as distinguished from mechanical control of a set of cipher rotors in cascade, thus getting away from the regular or metric stepping of the rotors. During the important years 1939-1941 this machine was used for enciphering the bulk of the highly secret and confidential administrative traffic of the War Department in communications with the Headquarters of Overseas Departments, Corps Areas, Defense Commands, and headquarters of GHQ Air Force and 2d Air Force. In addition, it was extensively used by the Signal Intelligence Service in forwarding traffic from our intercept stations in Honolulu and Manila. It was also used during 1940 and 1941 for communications between the War Department and the U. S. Military Attache in London. In 1941 the War Department provided a number of these machines for the Department of State, for use in secret and confidential communications between the Secretary of State and the American Ambassador in London and these were used from 1941 to 1944 for that purpose. It was also used in a special circuit for a number of months in 1942 for direct communication between the President and the Prime Minister in London. After these machines were taken out of War Department service a number of them (29 or 30) were provided the Office of the Coordinator of Information (later OSS) for secret communications between Washington, London, and other capitals where the OSS maintained headquarters. Some of these machines are probably still in service.
b. Converter M-134 C, covered by patent application (Serial No. 70,412) filed on 23 March 1936 by the Chief Signal Officer in the name of Friedman and Rowlett as joint inventors, arose as a result of studies having the aim of improving Converter M-134 A. About 15 June 1935, Rowlett conceived the idea of using a set of rotors in the M-134 A. Rowlett and I then jointly developed the idea by setting down on paper various methods by which it could be applied in practice to the M-134 A. All of these methods were disclosed to the Navy, then engaged in attempts to improve their own unsatisfactory Mark I ECM. The Navy took one of these methods and incorporated it in the design of their Mark II ECM, work on which was begun in January 1938 by Navy contract with the Teletype Corporation. This was done, however, without advising us or anybody else in the Signal Corps until March 1939, when the Teletype engineers brought to Washington the first completed set of drawings of the Mark II ECM, at which time Rowlett and I were invited to the conference with the engineers. A first model was built and delivered on 3 February 1940. Further development was on a completely joint Army-Navy basis and on 19 June 1940 the Signal Corps added its order of an initial 85 machines to the Navy order. On 17 March 1941 the first 10 machines were delivered to the Signal Corps and were given a prompt service test, proving the machines highly satisfactory. In successive contracts the Army procured a total of 3392 machines and almost 2000 were in service by March 1944. The Navy also procured a larger quantity. In the Army the machines were distributed to all commands down to and including HQ of Divisions. They were also used in all important fixed headquarters in the Communications Zone, in all theaters and in the U.S. Whenever and wherever the late President went during the War, the Sigaba went too, on the Presidential Train, at Hyde Park, Yalta, etc. For further information regarding its value in Joint Army-Navy communications, see the detailed notes attached. We know that neither the Germans nor the Japanese were able to solve our Sigaba traffic, though we were able to solve their high echelon traffic, obtaining intelligence of great diplomatic, strategic, and tactical value. In view of the foregoing, the Sigaba contributed materially to our success in the war.

c. Converter M-228 (Sigcum, Sighua'd), covered by patent application (Serial No. 443,320) filed on 16 May 1942 by The Chief Signal Officer in the name of Friedman and Rowlett as joint inventors, was a cryptographic machine to protect teletype communications, by providing for automatic off-line or on-line (keyboard) encipherment, transmission, reception, decipherment, and printing of messages (in a single operation) at the rate of over 360 characters per minute, with high security. On 12 March 1942 the first two models, constructed at Fort Monmouth, were given a satisfactory service test. On 18 June 1942 the Navy witnessed a demonstration of the machine and decided to procure 200. By 5 June 1944 a total of 3200 machines had been manufactured and 1483 in service, including 200 by Navy. In May 1943 the machines were used in the United Kingdom to link together all U. S. Army headquarters
in the Defense Teletypewriter Network and these machines were used to encipher a tremendous volume of messages, including raw material for cryptanalysis from all intercept stations. Most of the traffic that was sent by radio teletype was confidential, but on land lines secret teletype messages could be sent by this machine. A modification (Sigmad) permitted use of the machine for transmitting weather data (secret) by the Air Force in two theaters; the same modification permitted use of the machine for secret messages between certain headquarters in Washington. In April 1944 the War Department approved a policy under which the machine could be turned over to the British for use in Combined Communications.

For further information on these machines and additional items relating to contributions in the Communications Security field, see detailed account attached hereto.

d. Cipher Device M-138, covered by patent application (Serial No. 300,212) filed on 19 October 1939. Thousands of these devices were manufactured. For several years this device formed the basis of the Strip Cipher System, which carried a large part of the secret and confidential communications of the Army, the Navy, and the State Department. In the Army it still serves as the back-up system for Converter M-134 C (Sigaba) and as the primary system for Posts, Camps and Stations as well as for circular messages to military attaches. In the Navy and in the State Department it is still used to a considerable degree for secret and confidential traffic.

e. Throughout the years mentioned, in my capacity as Head Cryptanalyst and later as Director of Communications Research, many problems in security were brought to my attention and I believe that my long experience in the field formed a solid foundation for mature, sound judgment in arriving at practical and satisfactory answers thereto. Some of the items that may be mentioned here are the following:

(1) In 1941, as a result of my special study of the manner in which Army and War Department cryptographic communications were then organized, I evolved and developed the idea of the "Cryptonet" system, which has worked in a highly satisfactory manner in practice.

(2) The studies and development of Converter M-209, over 100,000 of which were produced and distributed in the Army and Navy.

(3) The "Stop-gap" or temporary-expedient system of double-loop key-tape encipherment of teletype transmissions.

(4) The "one-time tape" or Sigtot system.

(5) The development of voice security equipment, including the "Sigsaly".
The development of the "Synchronous Polarity Reversal System" of Gifax, which is based upon an important modification (by Lt. Colonel Rosen) of the principles disclosed in my (secret) patent application (Serial No. 478,193) filed on 3 June 1943.

I also was a member of the Ad Hoc Committee, consisting of two Navy and two Army members, appointed in 1944 by the Joint Communications Board to look into the matter of communications security in all non-military departments and agencies; the work of this Committee resulted in the establishment by President Truman of the Cryptographic Security Board, consisting of the Secretaries of the State, War and Navy Departments.

My principal contribution in the communications intelligence field, directly applicable to our operations in World War II, was in connection with the solution of the Japanese cipher machine (purple system) employed by the Japanese Foreign Office in its highly secret communications with its Embassies and Legations. As Principal Cryptanalyst in the years 1939-1941 I was in charge of the cryptanalytic staff that studied this problem from February 1939, when the first traffic in that machine appeared, until September 1940, when we were able to hand in the first translations. By careful analytical reasoning, long and arduous study of the external cryptographic phenomena exhibited by the messages, by correct reasoning, and a wide knowledge of cryptographic mechanisms we were able to fathom the mystery underlying the functioning of the Japanese machine and to construct, without ever having seen the original itself, machines which would duplicate the functions of the Japanese machine. So far as I am aware, this is the first time in cryptanalytic history that a machine of such cryptographic complexity was completely reconstructed by pure analysis.

As to the importance of that solution I need only refer to the disclosures of the current Joint Congressional Investigation of the Pearl Harbor Attack by the Japanese and to certain statements contained in the Chief of Staff's letter to Mr. Dewey. While the solution represents the achievement of a cooperative effort by a number of people, it was made possible by good coordination, and proper technical direction of a fair number of skilled cryptanalytic personnel who were selected and trained by me and who worked under my direction for over 18 months as a harmonious team. I do not believe that this machine was solved by any other cryptanalytic organization. We know that the very competent British organization failed in its efforts to solve this problem, for we gave them the solution and a machine in January 1941. Nor did the German cryptanalytic staffs who attempted it gain any success.

During the succeeding years, 1941-45, the Agency accomplished many feats in cryptanalysis, too numerous to mention. The diplomatic communications of many countries were read, some almost in toto; the
secret communications of the Japanese Army and Air Force were read to a considerable degree, contributing greatly to our victory in the Pacific. In my capacity as technical adviser to the Chief of the Agency, and having Staff Supervision over all the technical operations of the Agency, I was always consulted by him and acted as advisor to all Chiefs of Divisions and Branches in these operations. The extent to which the Agency engaged in the research, development, and use of high-speed analytic equipments to facilitate the application of cryptanalytic techniques and processing is worthy of mention, and my technical advice and collaboration was used in all these cases.

4. From my earliest days of duty in the Office of the Chief Signal Officer I have taken a deep interest in the preparation of texts for use in training military personnel in cryptography and cryptanalysis, and the War Department has published a series of such texts which were written and prepared entirely by me. I regard the writing of this literature, which was extensively used at the various Army Signal or Communications schools, and in the Army Extension Courses, as one of my very important contributions to the war effort. I believe that this material represents an important contribution to the science of cryptology, because for the first time its basic principles and techniques, heretofore scattered in a most chaotic, disorganized manner in foreign literature, were set forth in a scientific, logical, orderly and clear manner; and consistent, adequate and scientific terminology used in this work. Upon them were also based a long series of graded exercises, with approved solutions, also prepared by me, which were used in conjunction with the texts by thousands of enrollees in the Army Extension School, in the various schools throughout the Army during the war, in the special schools in cryptography and cryptanalysis at Fort Monmouth (later at Vint Hill Farms Station), and at Arlington Hall Station itself, to train thousands of new employees. All or most of these texts were also used by the U. S. Navy, the U. S. Coast Guard, the Federal Bureau of Investigation, and the Department of State; copies were also officially furnished the Canadian and British Government.

It was at my suggestion that the War Department, on 11 October 1930, formally established the Signal Intelligence School in Washington, for training Regular Army officers in signal intelligence operations. I served as the Director of that School, in addition to my other duties, organized the 2-year course given, and directly supervised the instruction. The fact that of the nine Army graduates (there were two officers from the U. S. Coast Guard and they also worked in the cryptologic field later) seven came to occupy top-level positions in communications intelligence and communications security work during the war.

In addition to the foregoing, numerous technical papers were written by me in my spare time; these were usually published by the War Department as secret or confidential documents, or they appeared
as articles in the Signal Corps Bulletin (restricted). Two of the most important of these works are entitled "Analysis of a Mechanico-electrical Cryptograph", in which I set forth the basic principles and techniques in the solution of cryptograms produced by electrical rotors in cascade, and "The Index of Coincidence", a revision of an earlier paper under the same title, in which there appears for the first time in cryptologic literature applications of statistical theory and techniques, later to become of great importance.
Property of
William F. Friedman
3932 Military Rd
Washington
DC

1944
October


1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31

Col. Cooke's Quarters
71 Karl Koenig Weg

IV-14609

Office
Tel. Frankfurt Military 21989

APO-757 (Frankfurt)

Approved for release by NSA on 06-05-2013 pursuant to E.O. 13526
Log

2 Oct - 0530 Left Wash (Wed a.m.)
- 0730 Arr Westover Field, Mass
- 1400 Left "
- 1535 Arr "Stephenville"

Sunday
0730CMT 4 Oct

6 Oct - 1200 Left "Harmonville" (1 1/2 hrs)
- 2145 Arr "Segovia" (Local time)

7 Oct - 0015 Left "
- 0925 Arr "Clel7 Rd. Paris" (7 hrs)

9 Oct - 1015 Left "Bourget, Paris"
- 1200 Arr "Amsterdam"
- 1245 Left "
- 1530 Arr "Copenhagen"
- 1615 Left "
- 1830 Arr "Stockholm"

17 Oct - 0815 Left "
- 1315 Arr "Paris"

19 Oct - 1100 Left "Arr "Segovia"
- 1315 Arr "Clel7 Rd. Paris"

27 Oct - 0800 Left "Frankfurt by rail"

Sunday
28 Oct - 0815 Arr "Paris - L'Est"

Paris - "Lagena" 1735. "Lagena - "Stephenville"

1912. "Stephenville - Wash 1144"
<table>
<thead>
<tr>
<th>Articles taken on</th>
<th>Trip to Europe</th>
<th>October 1946</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 undershirts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 shorts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 long underwear</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 pair pyjamas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Turkish towel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 wash cloth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 hand towels</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 white handkerchiefs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 silk gray</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 brown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 blue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 white shirts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 ties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 loose socks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 flashlight</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 clock, small</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Switzerland</td>
</tr>
</tbody>
</table>
1. Handbag, black
1. Valise pack
1. Musette bag
1. Hat
1. Cashmere scarf, blue
1. White scarf
1. Overcoat

1. Gray 2
1. Blue shirt
1. Checked brown belt
1. Blue spot coat
1. Gray vest
1. Wool sweater
1. Gray phases
1. Cap, wool
1. Gray rubber overshoe
1. Gray spats
1. Bathrobe, brown wool
1. Toilet kit, silver back, brush, comb, safety
Oct 1930

Began entry at 1930

At 2010 word that plane was coming from Westover Airport, Mass., but had not yet started. Much delay in briefing.

Met Col. Mike Marcus — what a character. Barbara & he argue. At 2010 word that plane had just left Westover ETA 01:13. I sent family home 2300.


0300 — Notified no parts taken out of commission & would be
Furmer delay. CT. We still unfasted, felt pleasantly so, only too talkative.

0530 - We board & engine warmed up until 0545 - we take off for Westover Field, minus heat. I put on my spas wrap blanket around me, over harness & sleep lightly for 1 hr. About 0750 arrive at Westover. Good breakfast - 2 eggs, smoked ham, 2 cups coffee, doughnut. Latest news - be back at 1200 - but no place to go so hang around 472 terminal. Lunch at noon. On return, information we leave at 1500. At 1500 changed to 1700. At 1700 changed to
next day at 0900. Then a rather hectic scramble to find room for night. No space in hotel at Springfield (3 men got one + last room). I inquire about Bob or post and am told of course - but no heat. "OK if enough blankets." I reply, can takes me + 2 others (Healy + Wolfe) to Bob. Sgt there say quarters but no heat. "Heat in 3d week up the road." So why not? We get assigned 3 nice rooms at $1.00 per night. Have 1710 dinner at mess at 1730 so I go down + fall asleep at once. Had asked Wolfe to wake me. Pretty nice meal
at 7:30. Brief walk, then phone Washington. All OK.
Tenant 18 y. is till give post.
Session by 15 in Judge's decision.
Concrete floor laid in 18 y.
Basement. 393 not yet paid
But a A. Powers very much
impressed. Asked 2 to phone
Mrs. Hoey, Wolfe, Isbell.
Short walk. Henry take a
Bath & get good sleep.
Room quiet, had very comfortable
This afternoon saw movie
"Halloween Journey."
My feet warm at last - two
Pair woolen socks & shoes.
Can pair from A. W. Mason.
Wash tomorrow.
To bed at 9 and read bit
For a while. Not interesting.
3 Oct 46 Thursday. Went at 6:45, phoned, dressed, walked over to train - had nice breakfast checked out of Box 4 walked to Terminal, last stop - off at 11:00 instead of 9:00. They hope - still some waiting to do.

12:15 - I walk outdoors just happen to hear loudspeaker noon news told of crash off plane taking off at Stensville this A.M. 39 passengers presumed to be all dead. Immediately phone call for home. Line busy for 10 minutes. E. there, hadn't yet heard of crash but did from our west last night.

Asked her to phone others to take out 5500 more term insurance. Understood lunch to be served on 1:00 train 1:30 and we're all ready to go.

13:50 - We go aboard with hàng.
4:00 - We take off. Cruisey altitude to be 7000 - it's a beautiful sunny warm day. Everything Ok.
1915 EST - 2115 local at Harmon Field. Arrived after a very pleasant journey during which had a chance to go up front & see controls etc.

Had a very nice dinner @ 454 Bistro. Brisket, brisket pieces & lots of it, mashed potatoes, salad, desert. To bed early in room with 5 others. Didn't sleep because I took coffee as an experiment. It worked. - We were told we'd be awakened at 4 am & would take off at 5. We weren't & didn't.
4 Oct Friday - Up at 0700, shaved, dressed / walked to terminal. Nice breakfast - ham & eggs. News - flight delayed on a/a due to weather.
1200 - Still no news - take off indefinite. Foot walk in warm sunshine. Mountain on which TWA plane crashed yesterday. A scene of crash quite visible - only 11 miles away. Talked with pilot of our ship about it. Say he usually goes over that hill - 2500' high. The TWA ship left at 0500, still not sighted. Apparently could not gain enough altitude to go over it - tried to turn away - or else something went wrong with controls or possibly ship hit a downdraft. Crew (3) + Passengers (31) all killed. On way to Germany - wives of service personnel & several very young children. Waited around terminal all day. Saw C.G. helicopter come in and land - help in getting Bodies out, if any. D
talked with Chaplain (he went up to scene). Says all but 2 bodies burned to death - no remains of others. Plane was fully loaded w/gas. — There was a USO show crew here on way to Greenland. I had chat w/one of them - magician Karl Rosini. Talked about Houdini & Demaggar, who he says is very daring — takes long chances. — Had dinner at 6 & went to movie — terrible Roy Rogers picture. Back to terminal — to more nerve-rejekt flight. - My shirt is a mess — I can’t get at my baggage — will have to wait. Next time I wear colored suit w/ take enough clothes in my bag. — These long delays most exasperating. 5 Oct. — Saturday — Had a good night sleep. We were not awakened at 4 or even at 8. Got up and
dressed, overs to breakfast at 9:30 and still no signs of departure. Latest info is that we cannot possibly leave before 2:00 tonight and prob won't until tomorrow. Got my baggage out of the pane, took nice shower, changed to fresh clean and feel better. Put my brown suit away and am wearing my checked slacks and blue sport coat. No news or newspaper. After rather poor dinner went to the movies and saw indifferent mystery detective story "Decoy" and then to Officers Club where bar might dance was on. Had a couple of drinks with our crowd and danced one with Nancy. Drunk in place, etc under the hostile stares of the officers ladies.
6 October [Sunday]
Turned in at 0130 after a walk to the terminal where I learned we were expected to go out at 0500. Didn't sleep too well & c.

Morning barracks - guys coming + going all night. Wasn't called until 0930 + told departure to be at 1030. hustled to dress + get to terminal. Was pretty sore about having to pay 30c a night for the bed - a kick up game of poker I saw one, made a protest but did no good. Think I should report conditions there. - We took off at 1215. Plane was tail heavy + we had to do some re-adjusting of baggage + money forward. Would have had a beer (double) all to myself
but a guy (D Martin) came + has struck by me. He's never flown before apparently + is pretty nervous about everything. Had a pretty rough 20-30 minutes at one time when we went into a thunderstorm. Part of trip very quiet. Arrived at Lagans at 1945 my time = 2145 Lagans time. Had a rather poor meal but only $1.50. Boarded plane again at midnight + took the air at 0015. Very quiet calm trip so far at 9,000 ft. Tried to get some sleep but couldn't - high altitude bothered me. Every time I was on verge of falling asleep would wake up with shortness of breath. Trip very smooth all the way.
despite (as I learned later) very bad weather most other places.
09:25 Arrived at Cergy Field. At once phoned Embassy to try to talk with Sgt Stewart. He was out but did talk with another man who knew me. Yet civilian had worked with Maj. Easley (SSF). - Bus in to ANC Terminal in Paris where I ran into Capt. Russo, who turned out to be great help. Got billet at Hotel Napoleon Bonaparte, finished there with Russo. Spent afternoon getting plane reservation to Stockholm, after seeing Easley. Stewart at Embassy, much also about cash - francs, dollars, etc. Getting big traveler's checks cashed at
Cun Express Co. took 1 hr to get $80 converted into 9416 kr @ 117.70 per dollar. - Fortunate in getting reservation on plane to Stockholm for tomorrow p.m. - Bought ticket for 12,400 kr = approx $105. - Sat in front of Cafe de la Paix for a couple of hours with Capt. Russo, G buying cognac for him, vermouth for me; two rounds costing 270 kr with tip included. - Dinner at Hotel Nap. how 830 pm + I must go right to bed - haven't had a good night's sleep for several days + none at all last night. - Comfortable room + bath but not fancy @ $3.00
Tuesday
8 Oct - Up at 0700, shaved, bathed, to breakfast at 0800 with Capt. R. Then taxiied to Air Embassy to see about tel to Stockholm but had to phone it at my own expense. Maj. Shanks said to send it collect as they had no funds here for purpose but when I went to tel office in emb. no collect. Telegram accepted. Capt. R got some salve for my itch - hope it works. Talked with Maj. Erskine & Lt. Stewart then time for lunch. No taxis available so we took a back & poor Rome was made to walk down champs Elysees. Cost 150 ft for 2 mile ride. After lunch packed my stuff, checked out of hotel & went by taxi to Air France terminal at Station des In-
valid, then through all the formalities - phone, customs etc.

From 11:45 and back to the hotel.

We took off before 4:00.

Attended the farewell dinner.

At 15:00, we started the last leg of the journey.

Departure was at 17:00.

We arrived safely in Paris.

The train was due to depart at 15:30.

At 16:40, everything was ready.

The hotel was almost 35 minutes away from the train station.

We arrived at 17:00.

The whole journey took almost 4 hours.

All in all, it was a successful trip.
right! Air France would find us rooms—and I had only 600 for
no place to cash travelers checks
or get new frames. I take a chance
and go by train back to Hotel Bapton.
But was lucky—had another room
on same floor. I simply explained
flight cancelled + clerk gives me
1½. I go up + take possession
at once—will straighten matters
out with ATC Bulletin Office
later—which I fortunately was
able to do. Waited around for
Capt R—to get some more frames
+ change company. Soon he comes
in—surprised to see me a bit as
he had gone with me to airport
and we had every assurance than
that plane would leave. They
a Swedish Air Line plane (Vickers) with only 2 engines so we will have to stop at Amsterdam and Copenhagen. A very pretty Swedish hostess - highly colored blonde with tanned white complexion, blue eyes. - Good journey to Amsterdam, where we land exactly at noon. I have a bite to eat - chicken noodle soup + two sandwiches all excellent for which I was able to say in French - 60. We take off again at 1245. - The Dutch scene is very lovely - the irrigation ditches + canals dividing up the countryside into quite regular patches. See a good many red tile roof houses - some slate roofs. All looks spin + Spanish. Very impressive + interesting country.
At 1500 we passed over Kiev. Beautiful afternoon, very calm weather for our flight. Countryside lovely. We are over water good deal. Flying at 7000 feet.

I'm a bit short of breath, the only slight discomfort. Had an excellent lunch served aboard. Good beer with it.

At 1530 we arrived at Copenhagen. Very new and modernistic airport terminal.

At 1615 we took off for Stockholm. Weather still fine. - Soon after we leave Copenhagen there is a marked change in the terrain. No more rectangular squares of cultivated fields and small hamlets. Instead, a very ruggedly wooded region, rather rolling terrain, lots of lakes and marshes and occasional house to be seen. Probably timberland.
begins here. - We are due to ar-
rive at 1815 - about an hour
from now. - Have just had tea
(Not very warm) and an excellent
sweet roll such as only the Jones
and Swades can make. - When
I got off at Copenhagen I
purposely (it unthinkingly)
left my spots on my seat - and
they were taken - probably
by some cleaner at Copenhagen.
Teaches me my lesson - We been
very so careful all along - not
left anything unattended or
unlocked until now - and
have a pair of very useful
spots. The stewardess must
disgraced, my shelf see.
about them on her next stop at Copenhagen — but I know they're gone for good as far as I'm concerned. I'll get a pair in Stockholm, those I lost were old and shabby anyway — how'd one button was half gone. We're now at 5000, my breathing is somewhat easier, our speed now 155 m.p.h.

At 1735 we are at 3000 and travelling more slowly, now ETA is 1830. Full moon already above horizon though still daylight. Pretty scene with sunset on left and full moon on right. — Exactly at 1830 we light at Stockholm airport. I have never seen such a fairyland-like scene as that I saw on approach.
ing and flying over Stockholm. The thousands of gleaming lights or reflections on the water between the islands, was a beautiful view I've ever seen from the air at night over any city. I had asked the bagage van driver to meet me at airport, as I had asked it was good to be wet. Customs formalities etc. They wanted to tax me for extra cigarettes but the bagage van driver talked to customs chief and I got off without paying the 3 crowns they had demanded.

Drove me to Hotel Reisen, where a room for night had been engaged - a nice room with twin beds, a fine bath. Forgot to say the driver phoned Hjalmar Concord.
at Airport and I talked with Boris there—good to hear his voice. We
waited for my heavy dinner with
then so I washed up quickly at
hotel and on going down met Boris,
saughter Ingrid and son-in-law Carles-
a very nice looking young man.
Boris took us to the famous "gift-
werk Striden" where E and I had
dinner that evening 15 years ago. - A very nice dinner and
then I went to my hotel and to bed
early as I was pretty tired. The
itch bothered me a good deal but
I got to sleep fairly quickly
and slept until 8:00.
10 Oct—Thursday. A pretty good
sleep it hard to get up but I
decided to meet Carles in a
0445 to call on General Kesslar. Not time enough for breakfast. By the time I finished shaving, bathing, etc., I skipped having any breakfast. Had a very nice visit with Gen. K. Then was driven in Negation car to Bos's office. Here in Stockholm they also drive like mad, etc. Very nice riding in car. After a few minutes with Bos, showing me around the plant, we were driven downtown in a tiny German car with chauffeur to largest department store where Bos took me to lunch—my breakfast too. Started with sour cream—excellent idea. Good fish and excellent sauces.
After lunch back to B's office in his new Lincoln, wonderful car. Spent couple hours talking & left at 1600 to get my belongings at hotel & check out. Had room for only 1 day as space is very hard to find here, too. Drive out to B's country place, a wonderful estate about which he spoke out for me and more later. - An exceedingly warm welcome from Charly, looking very well. - B's father here, over 87 years old, a nurse who looks after him; a young woman whose job is to teach crafts to the women folk on the estate (about 250 people work & live on the place!), and B's youngest son Gunnar.
just graduated a pretty - a
tall, shapely young man looking
not at all like B. - Early dinner
very simple, as Annie had to
go to Red Cross meeting. B +
I talked Swedish history
for an hour or two afterwards
then went to craft class
conducted by the young women
also went through the build-
ing where class is conducted
more about it later. - Back
to main house + talked some
more. Retired early - 21:15 as
I was tired + again bothered
by itch + about a dozen
itches of some sort - look
like spider bites but can't
be that. - Am wondering
when I picked up at the various TTC places I stopped on the journey - good thing I had my transportation!

If this still doesn't let up soon I'll have to see a medic now 2330 it's time to bed. Will have breakfast in bed.

11 Oct Friday - my alarm went off at 0830 as set but I didn't get up - a rather restless night. I was troubled with the itch that had been for pepper & the combination was too much. I took until 0100 or 0130 and had difficulty in getting to sleep. Also worrying a bit about things back home.

Cut any rate, at 0730 Boris came
up with a tall glass of orange juice and at 0745 Annie and
I sat down to a breakfast tray. I felt quite
embarrassed with all the Atlantic
tea, toast, marmalade, and thin
slices of cheese. — Red Boris
my itch & agreed to go to see
doc. today — To the Beth-Chat
and as usual caught cold.
I just don't dare take it. —
Began APC cold this afternoon.
I think I have it under con-
trol. — Boris & I took a two
around estate this morning.
375 acres. — Lunch at 1200 &
poor after we drove to Sundance
to see movies. — He said it was
an urticaire. allergy — fron
the bite of some insect—probably lice! Take me 3 prescriptions—two internal, one external. I feel lots better tonight already. I hope I am over it. Drive with B to the shores of a lake that leads directly to the Bellingham this while waiting for pharmacy to make up the prescriptions. Back home by 1500. Took a nap— slept for 2 hours and 15 min. — forgot to note letter from E this a.m.— telling of sale of 3937 military dog TAGS. Had stuff to much believe will be able to turn around financially now. — Supper at 1800— hard shell crab— fried in delicious style.
several other things, especially two
jams, one made of "field berries"
and the other
- B & I spent three hours discus-
sing technical matters. Then
looked over & admired many
features of their house - all in
most modern style - must
have cost plenty to fix up.
Now 0015 time to turn in.

Annie made me a last drink
of elderberry brandy, honey &
hot water.

13 Oct: Sunday - Spent all day
yesterday (Saturday) indoors
nursing my cold. Up at 0900
and downstairs to breakfast.
At noon, more guests - the Hagens' oldest son Karl Wilfred, etc.
one of his professors at the medical school & another writing prof. from Buenos Aires, both very nice men. Also Ingrid and her husband, Major Castaldi, later in that day. It was a rather nice day, a bit chilly, but I was happy to have to stay indoors. Took a long nap in the afternoon. Finally got to bed about midnight up at 05:45, breakfast at nine and at about 11:00 we all went to visit Hipschley Castle started in 1300 something. There were ruin stones found in that vicinity, I got Bob to take a photo of me standing beside the castle quite interesting.
and is a sort of natural picture gallery now—about 1700 for
Keto there—had tea at one
from nearby—very clean and
nice.— Back to Londerry—
sat around talking a bit—
then a short rest. Dinner at
1700 excellent food.— Bron had
insisted on putting in a long
distance call to Ed and it came
through at 8:30. Quite thrilled
by how E’s voice held up the
good transmission. All seems
OK at home, Barbara off to
Boston then New York then
at the. — In the evening
B showed colored slides
of his trip to U.S. etc.—very
fun pictures. — Nov 12 2236
and must go to bed as soon as I've got to be down to breakfast at 0745. My cold is much better tonight but I have some headache - probably from all the medicine I took.

14 Oct. Monday - up at 0700 + down to breakfast at 0745. Feeling pretty rocky with my cold. Drive in to town and first went to Legation to get some known to bring ticket back to Paris. Cost 31.05.

Spend a few minutes there and then to other building Legation to call on Mr. Huggins who is now in charge, in absence of new Minister Dryfuss. The Charge d'Affaires, Huggins I had met before at Cahir.
Two years ago—The trip I almost got to Sweden but didn't because the powers that be deemed it unsafe for me to go with Capt. Carlson went. Situation still rather precarious. I am to see Him again tomorrow. Then invite to M.A.'s office where we spent up with Kessel who came along to go through the Hagelin Plant. His first visit there. — Lunch at the NK Dept. Store where B & I had lunch before. But this time went with Mrs. Carson & two of B's executives. Very nice lunch after which B & I went back to the Plant & I examined all models of machines until
Almost 5 p.m. Stopped to pick up my laundry at Hotel Rexan and found it pretty expensive. Alcohol $1.50 for 3 shirts, 3 underwear + 4 pairs socks! No hotel room yet for Tuesday night—I leave Wed morning at 7 a.m. don't want to spend the night at Sundance so I have to get up so early in the morning to make it to airport. My Con- rad dug up 3 bottles of liquor for me out of his own stoke and I am much indebted and about done. These people are doing entirely too much for me. I won't let me do anything in return. Done back to Sundan at 7:30
Stopping for a few minutes to see Ron's father at his apartment in Stockholm—a place with a lovely view of the water and the new big bridge. Dinner with just Ann and Ron and then Ron and I just sat around discussing business matters for several hours. Putting finishing touches on questions of interest to you. 23/3. I won't have to get up until 10. Tomorrow we go to opera. Have had an interesting day despite my feeling a bit miserable with my head. 15 Oct. Tuesday. Up at 0700 after a very good night's rest. After-
breakfast, B took me to see his new brick factory, which is under construction. Says brick manufacturers are extremely conservative and his new factory leaves them more or less aghast at his novelties. But B says it will be efficient enough to pay for itself after but 5 years— which means about $300,000 to be made in that time. I found the place interesting but a bit beyond me— much tipping of hats when B comes round, and very good feeling between him and the people on the place. Home again and I began packing. Decided to take a chance on a quick bath despite the lack of heat in bathroom, which is how I caught cold first, but being that she had no bath for several
days, decided I just had to chance it. (Apparently no bad effects, so I am writing this on the next day aloft in plane to Paris.) Denier at 1230 and then completed dressing and packing. B, Anne, and I left at about 1430 for Stockholm in the Finland Line. 845 mile to town despite bad weather—rain, cold, and rainy. B and I went to B's office, where I was given souvenirs: a beautiful tiny alarm clock (travel-size) for E; a knife with his initials for John; a book for me. At 1630 I went to NK (Enko) the big dept store, to meet Anna and buy some trinkets. Bought two scarves (head) for the Hagelius's cook and maid. Very nice things. A half dozen beautiful hand-washed hand-
Perhaps it's best to bring these tiny Swedish mugs originally in a nursery in the few weeks she was made by the townspeople where the nursery used to be. Expensive enough - 9.75 each = $11.75, but nice. - Annie then insisted as she had all along, on buying a gift for F, which I wanted must be inexpensive but true Swedish. So she bought two ash trays of a variety called Argenta (inland silver ingot pottery designed by Swedish artist named Wilhelm Kage). It will be somewhat if a chore carrying the package back, but well worth it. Then Anne insisted on buying a scarf for Barbara, with typical Swedish design + figures - I bought a nice box of candy for the evening, as we were going to the
Opera. - At 11:20 we left NK, got a taxi
to go to cocktails at The Higgs - he
in charge of logistion now (as I think
I mentioned once before) lovely big
apartment. Met there Mr. Higginson,
SS representative & had brief talk
with him + Higgs re Swedish crypt.
outfit (total 400) stuffed with good many
G's, E's, E's, & couple R's. Higgs gave me
copy of present swirl paper, to our
talk in Monday. Higginson told me his
head it on most excellent authority the
8 B built machine for fish - which was
great surprise to me but probably true
then + Mrs. Higginson at present Mrs.
Reynold (wife of Charge) & two other
ladies. Mrs. Higgs nice but not look.
ig the well - says she has bad case of
"Flu" (like J. Rave) - Mr. Higgin
and Mrs Couradi, Boris, and Annie. Of course at party, had one nice, old-fashioned, and some Smacks. Left at 1830, to Opera. Restaurant, where we had a lovely dinner, with moderate drinks and many skoles among B.A. the Couradies and we. Then to Opera to see Thais - a very fine performance. We sat in an excellent box in the first balcony, surrounded entirely by very fine looking people. Incidentally I am much impressed by the fine looking Swedes, well groomed and well-dressed everywhere. I enjoyed the opera immensely although of course I didn't understand a word of Swedish. The company is very good - the leading baritone gave his best performance before midnight.
U.S., where he joined the Metropolitan. There was some excellent dancing and ballet work. I had never seen their & was glad of the chance. During the two intermissions we circulated in the foyer & examined the building—quite ornate & impressive. The performance lasted until 2300 or 2315 and then I said my farewells to the Canadians. B & A then took me to my hotel—almost the last room available in the whole of Stockholm & obtained for me only after deligent search by the reception. I found it a very small hotel, about 34, and (B called it a "hotelhouse") but very clean. It was after midnight that I turned out the light & tried to get some sleep. Had to be up
by 0600 to get to the air terminal.
I forgot to say that I had an
almost tearful farewell with
the Hagedins - they are such charming
people & I hope they will really come
to Washington this spring, as Bita
promised.

No Oct - Wednesday, up at 0600,
with my two alarm clocks & the
hotel attendant waking me - but
I didn't need waking as I had
already slept - too much noise all
night for one thing & early morning
showering about in the very narrow
street outside my window. But I
must have slept some & I could
dream... & then a taxi &
went to the "Kappalim" arriving
there by 0645. Checked in & got
overweight by several kilos (which with all the liquor
worth about 100 francs). He handed me a hundred francs
note— which he had much difficulty
in changing, to get out 12.50 fr. for
excess of 6 kilos @ 3 fr. per k. Got on
bus & were left at 0700 on the dot.
Arrived at airport soon, checked in,
& had some breakfast. Then went
through customs & money control no
trouble. Changed all my Swedish
money to francs. Boarded plane
at 0800 & took off at 0815 on
the dot. — This is a big Douglas
C-54 type, capable of holding 40
passengers but there are only a
dezon or 13 of us, including a self-
made up business - French exp-
pose. She has a rather extreme dress on—slit down the front all the way to her navel. I think, I'd like to get a good view of her with her coat off. Rather good-looking, slender, + artificial blonde. — The plane is very clean + well managed. Coffee has already been served + soon lunch. — We have excellent flying weather, sun is out, we are at 7000' + now passing Malmo. Very comfortable but my feet are as usual, cold + I miss my slippers. — I must see to my accounts now + get those straightened out to see how they balance. — Well, in about only 13:30 hrs = $3.42, which isn't too bad. — At 10:30, lunch was served—Hot Consomme, potato salad, some nice
cold salmon, two sandwiches, bananas.
I ate pretty well. My feet are still
very cold. — I got a blanket and
wrapped it around my legs —
much better than. — It is now
12:45, practically the whole of
the journey has been above cloud
level. On the road we could see nothing
of the ground. — We are going
down now into the clouds. —
I can't hear very well. — My cold is
worse makes equalizing pressure
pretty difficult. — We are under
the clouds and can see the ter-
tain very well. — But I can't
hear well again. This is my
first experience with hearing at
high pressure difficulties. I hope it
passes soon. — We arrived on
the dot at 1315, as scheduled. Went through the usual formalities of money, customs, etc., in rapid style and then got on bus for Paris station des Invalides. Talked with an American businessman from New Haven on bus with two young Jewish refugees who have been wandering around for several years in Europe trying to get visas to America. Sad stories — pretty spunky girls. At station about 1430 took cab to ATO terminal. Place Vendome to find them in the midst of moving. Met made my arrangements for Hotel Napoleon on Concorde for billet for the
night. All fixed up at about 1530. Phoned my Easley at Embassy to get message to Earl to meet me at airport tomorrow. He got through on the phone. I hope to be met. Lpt to my room, took a drink of my cognac, lay down until 1600. Quick dinner, then I went Howard Westover, in on his way to Washington. Brief talk, short walk to Air Force. Brought some roasted chestnuts and beer in my room. Now 2030 it will turn in very soon. Bought French papers with headline news about Europe's suicide. Must be up by 0500 to get bus here.
17 Oct - Thursday - Up at 0600, after a fairly good night. The three cups of coffee in the morning still had their effects late at night! - Bus left Hotel Napoleon at 10am, we got to Oly Fd by 0740 only to be met with announcement that our flight would be delayed until 1000 because of bad weather at Frankfurt. Another delay at 1000 to 1100.

So I took opportunity to write a letter to E and to walk over to Air France terminal to send a wire to the Nagelins. 15 words cost 1.21 francs. - We took off a little after 1100 and having a very quiet & calm trip at 5000 feet. Visited the cockpit & met pilot of my ear trouble yesterday.
day & he said he'd go down very gradually to give my tubes a
good chance. - On the door where
they usually post the names of
the crew members some way
had written under Radio-operat-
The name "A. Graham Bell" asst.
radio operator "J. Marconi" and,
under "Flight Engineer" O. Wright.
When I showed the names to the
pilot he laughed + said that
that "was intended to boost the
morale of the customers"!! -
We are right on the course + on
time - scheduled to arrive at
1315. - Sun is out + all clear.
Below all the way. Have been
Talking with an American girl
from Boston on her way back.
To Frankfurt from London where she visited with her parents who had come over to see her. A very nice girl working for FEA at Höchst & has been in ETO for three years. She says Europe is no place for a young girl. On the 1st of March we landed at Eppelborn, near Frankfurt where I was much pleased to find Erle with car and driver. After my bags and took the young lady along with us as she lived close by. The Earl in Höchst. Joan was out at some point so Earl & I had a couple of sandwiches & a drink at their request by one of their two maids. Sat around talking for a
a couple of hours then I went up to my room and took a nap until 1:00 when I was called for dinner. - nice to see Jane & had a nice dinner. - Charlie, Mike & Jessie didn't come over to spend evening with us. - Spent an hour in E's redwood station & got talking with a man in Baltimore but just as I was getting ready to ask him to phone a message to Washington his signal faded out and we shook him. - In bed at past midnight slept fairly well but not enough as I was up at 3:30 to go to office. - Breakfast at 8:30. 17th Fairbank, built my beard & saw Old French.
June press present from
Anne H to ESI -

Artist: Wilhelm Kage
Name: Ingenta

For online press:
1. No trained personnel for maintenance
2. No operating personnel
3. Physical circuit not suitable
4. When tape used to read radio

Interference
1. Cell not kept very
2. Operator
3. To obtain for
4. Red or orange for taking
5. On 5 feet to reach
6. Switch with VHF OK
7. M-LOG from Reg to Sign.
8. Damaged live OK
9. Not a great deal of trouble in
10. New found dead
Not only at all.
<table>
<thead>
<tr>
<th>Item</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td>$50</td>
</tr>
<tr>
<td>Total</td>
<td>$500</td>
</tr>
<tr>
<td>1 Oct Cost thru check</td>
<td>$3.38</td>
</tr>
<tr>
<td>Cash to ESF</td>
<td>5.00</td>
</tr>
<tr>
<td>Shoe repairs</td>
<td>.75</td>
</tr>
<tr>
<td>Parking</td>
<td>.25</td>
</tr>
<tr>
<td>Lunch</td>
<td>.50</td>
</tr>
<tr>
<td>Misc</td>
<td>.42</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$10.30</strong></td>
</tr>
<tr>
<td></td>
<td><strong>$39.70</strong></td>
</tr>
<tr>
<td>2 Oct Breakfast</td>
<td>.40</td>
</tr>
<tr>
<td>Lunch + dinner</td>
<td>1.50</td>
</tr>
<tr>
<td>Room</td>
<td>1.00</td>
</tr>
<tr>
<td>Misc</td>
<td>.66</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>$3.56</strong></td>
</tr>
<tr>
<td></td>
<td><strong>$36.14</strong></td>
</tr>
<tr>
<td>3 Oct Breakfast + reg</td>
<td>.55</td>
</tr>
<tr>
<td>Cigars</td>
<td>1.40</td>
</tr>
<tr>
<td>Candy Coffee</td>
<td>.69</td>
</tr>
<tr>
<td>Dinner</td>
<td>1.30</td>
</tr>
<tr>
<td>Telephone</td>
<td>4.34</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>31.80</strong></td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
</tr>
<tr>
<td>1 Oct</td>
<td>Breakfast</td>
</tr>
<tr>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td></td>
<td>Dinner</td>
</tr>
<tr>
<td></td>
<td>Bar Sandwiches</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Oct</td>
<td>Breakfast, Lunch</td>
</tr>
<tr>
<td></td>
<td>Dance</td>
</tr>
<tr>
<td></td>
<td>Ballet for 3 days</td>
</tr>
<tr>
<td></td>
<td>Bar Label</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Oct</td>
<td>Breakfast</td>
</tr>
<tr>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td></td>
<td>Supper at Jagers</td>
</tr>
<tr>
<td></td>
<td>Eggs</td>
</tr>
<tr>
<td></td>
<td>2 Stamps</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Oct</td>
<td>Breakfast</td>
</tr>
<tr>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td></td>
<td>Bar Franco (585)</td>
</tr>
<tr>
<td></td>
<td>Carry</td>
</tr>
<tr>
<td></td>
<td>[Hair Checks $4.50]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>7 Oct</td>
<td>Cashier</td>
</tr>
<tr>
<td></td>
<td>Hair Checks $3.00</td>
</tr>
<tr>
<td></td>
<td>Read in Fr @ 117.10/8 - 9.416</td>
</tr>
<tr>
<td></td>
<td>Borrowed from Capt. Press</td>
</tr>
<tr>
<td></td>
<td>Taxi Fr</td>
</tr>
<tr>
<td></td>
<td>Drinko</td>
</tr>
<tr>
<td></td>
<td>2 Etchings</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>$105 - Ticket 124.00</td>
</tr>
<tr>
<td></td>
<td>Stockholders</td>
</tr>
<tr>
<td></td>
<td>Tips</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Total</td>
</tr>
<tr>
<td></td>
<td>Paid $224.60</td>
</tr>
<tr>
<td></td>
<td>2 Nights Hotel</td>
</tr>
<tr>
<td></td>
<td>$30.00 = $6.00</td>
</tr>
<tr>
<td></td>
<td>Soup 25.00</td>
</tr>
</tbody>
</table>
and then E and I went to his office in the IGF Bldg., where I made a lively tour of his establishment. Then Mr. Smetana and I went by staff car to visit the 114th Sig Sg Co., which is located on the premises occupied by a copper mine (now not being worked) at a small city named Somoria, about 80 or so miles north-northeast of Frankfurt. Had lunch with Capt. Kilbee Smith, his officers, at their quarters, cooked by German women. A pretty good meal. She had lots of shelter. After lunch we went over Smith's installation in the copper mine headquarters.
an experienced and very able
engineer, can do almost any-
thing technical in the electrical
or mechanical field. The basic
medium of exchange here now
is a package of U.S. cigarettes,
which are valued at anywhere
from $50 to $100 depending on
what is bought. Nobody sees any
German stamps or American
cigars - they simply are used
as money and circulate as
gold or silver coins would. I
suppose ultimately some Germans
got to smoke them but as a
medium the Germans will
trade their unscalable or
unwearable items for cigarettes
which they then use to buy
the necessities of life. What a commentary on our civilization. How they are getting up better markets under official auspices and cigarettes are used as the standard of value—a carton of them gets 55 border points. A box of U.S. soap is valued at 3 or 4 border points, etc. The ride to Somativa and Brack was very nice, mostly over the auto-block which is in good shape and all the bridges have either been repaired or have temporary wooden crossings over them. The weather was nice and I enjoyed the trip despite
my coat, which is still quite bad but I have no furs. We were a bit late in getting back and had to hurry at the Cooks and I had been invited by Gen. & Mrs. Sankey to a dinner party at their new home on the outskirts of Frankfurt. Here were others: Col. & Mrs. Beyer, a British Major who is C.S.O. of British Zone and his aide (a Captain); and French Major General — who is C.S.O. of the French Zone and his aide (a charming major). We were last to arrive as not only did we get a late start but also, in Earls’ case,
to make time on the road we
get punched by an American
M.P. for speeding — and it took
many minutes for him to make
out the ticket by flashlight.

The cocktails and dinners were
very fine. The Germans have
four servants and a butler. When
they first came they had ten
servants but when it took
12 dozen eggs a week to feed
the family he had to cut down
on the size of the German staff.

The monetary cost must be very
small on the basis of what
they German engineers earn.

But since the servants get their
board it comes to a good deal
I suppose. See also Jean
about this & report later. - Got
done at midnight & turned in,
feeling very tired. Not too
happy about having to get up
at 0700 again as USFET
worked on Saturday morning.
Besides, I didn't turn in
right away as I simply had
to catch up on this diary
hadn't had a moment for
then in a couple of days.

Turned out my light at 0130.

19th - Saturday - Tasle woke
me at 0700. Had a pretty
good sleep but not enough. Got
dressed & went over to house
at 14T 13th for breakfast as
yesterday. - Then to office for
a few minutes and then to
Gen. Samuels office to
make a call, as per his request
last night. Spent about two
hours with him and with
another called Mr. Thompson,
a VP of AT&T Co., who had just
returned from Moscow where he'd
attended the preliminary
communication conference. I
was much interested to hear
results of that. Knowing most
of the Americans who attended
Thompson remembered me
from years back, but I'd forgotten
him. - I then returned
to Samuel's office, feeling very
groggy from my cold. - Then
took a ride downtown to
pick up a mass card - and
I had to show him how to drive the way — and I didn't know much myself. — Well, we made it anyhow — then returned to E's office, closed up & left with him for home & lunch. — A nice lunch — finished at 1430. — And I simply had to pack this p.m. — Have been on the go for so many days — I slept hardly until 1500. — Now dressed, ready for dinner — feel not a bit hungry in view of family lunch. — After dinner we sat around and read a bit. Alan played with his train set, but we couldn't get nobody in D.S. — Talked with Mr. Johnson in Cork about...
James Joyce - he not appreci-
ate. His Joyce at all, thinks him
a passing fad. - Turned in at
23.30 and read until past mid-
night. Slept well, until 10.30.
20 Oct. Sunday. Jean cooked
us breakfast of bacon and
scrambled eggs. The cook
had made "Irish" cake. I
guess that's poppy seed cake,
which I liked very well but
Evel didn't. - I had suggested
that we go see old friends
this day, so that's what we
did. I felt pretty miserable
with my cold which is not
breaking up very much but
still I wanted to see the
old city - now in complete
ruins and quite heartbreaking to see. We met a German who showed us around one old ruin. Said the damage to the whole area was done in 17 minutes. Frankfurt was not bombed until about 1 Feb 1944 and then in 3 nights 30,000 tons of bombs were dropped, completely wrecking the whole city. It's still a terrible shambles. The old part of the city we visited in detail. Today it is completely uninhabited and the air of desolation and absolute quiet was oppressive. We took some pictures and wandered about in various areas for a couple of hours before coming home. I took
a bath and got into bed for a nap. - now 1:30 and were going to have dinner with the Bayes. - I feel a bit better tonight - but my head + ears are still stopped up.

21 Oct. - Monday - up at 7:00 to Frankfurt where I had a nice breakfast - ham + eggs. Felt lot better this morning - my ears not as stopped up + ced in about cleaning with some coughing. Keep pretty well after nice part of the Bayeasat the "Cogen" House - a club for colonels + generals, formerly the home of the general manager of V. Fahn and quite a lovely place. The Europeans wol
also guests of the Bayes. We had a very nice dinner preceded by cocktails & followed by brandy. Got home at near midnight, after very nice evening out & feeling much better.

No mail this morning at office. At 11:00 we left for a visit to the "Tower"—one of Earl's installations about 12 miles from Montfort at Great Barr, where I visited last year too. Had a very nice black dinner with Major Eugene Beards and his officers at their quarters. After that we visited the Tower & came back to office at 15:00. Wonderful weather.
Of this morning had cleared up somewhat. On my return found E's letter of 10 Oct. I was glad to get word from him to see all OK. What 1830 we are going to another dinner party in my honor by Col. Hayes at Knobloch Castle - scene of the jewel robbery. May see Red Crosserman there.

22 Oct. Sunday. Up at 0700. Had a pretty good time last night. 40 meals, cocktails before and drinks after a fine dinner. A good orchestra playing U.S. jazz. Red came (in blue) bringing Miss (formerly Sgt.) Dunkle. The Castle is quite a place and D
would have liked to have seen the place during daylight. - Back home by midnight and to bed right away, my cold a good deal better by then. - Slept pretty well. - Jean made breakfast for us this time + we went to office. - At 9go Charlie, Henry + Mary Stetson started off on our 2 n 3 day trip south as far as Munich to visit various installations I'd seen last year. - It started off bad weather but at noon we had the sun out. Later it rained a good deal and quite bad on the roads. - Left to 11/4 by Sig. Sve Co at Scheyer about 1500 where Capt. #12scheveig is in charge. Had supper after a drink and after
that visited his installation
+ then sat around talking
shop until 2-30, with a
few drinks. It has taken
a year to fix up the place
+ as yet there are no operators
at all – such a shortage of
men + materials. - Capt C
gave me the guest room, a
fairly but comfortable room
but I didn't sleep at all
well as I'd had a couple of
cups of coffee at noon. There
was nothing else to drink
when we stopped for lunch.
- Capt C is using a great
deal of German labor +
gets his material where he
show he can - strengthening
with necessary. He's built up a very nice place. We chatted
off air too - one day we
last year at the same place.
W.O. Eagle - turned in
fairly late + very tired.
22 Oct. - Wednesday - up at
0730, breakfast at 8.30.
Smoked haddock + eggs, good.
So had iced tea + juice.
Fruit, iced tea + no hot stuff.
But 0930 we left for Munich
to visit a perspective new
guite at Riem. A terrible
day, so foggy and hardly
see the road, and cold +
very dismal. We didn't
see much at Munich + got
back to 11th. at 1300. We
we had lunch. Said farewell at 14:00 & started on long road to Ansaph, where we were spending the night with Lt Col Abraham, who's known since my early days at Ft Sumriner.

The journey was through village after village, as dirty, unkempt, filthy & dismal as any I've ever seen in France. I got a hopeless feeling about a people who would put up with such living generation after generation. The German cities all ruined & the German villages dis-
repertable looking + so hopeless in future prospects.

Thurs at the Hermanzky House - a lovely dinner served in first class style.

I was never met Mrs. A before. I was glad to do so. I asked if I could see the guest room.

We had a lot of fun at the school. Tuesday morning we met the school which is getting famous as the model for C school in the world. It's old almost 130 + six teachers as well turn in.

2nd Oct - Thursday - Up at 6:30 after a pretty good night's sleep. Breakfast of fish scrambled egg + toast - C.P. Shamrock
a very long and tiring ride to Frankfurt. In all we did about 600 miles since Tuesday. I was very glad to get back safely, especially on such good roads. I wish I could put down my many impressions and events from here. I'm too tired now—maybe later if I can remember all. 8:25 to Frankfurt at 7:30.  The Cookes were having a cocktail party for us. I had 10 minutes to plan and clean up. Party was for office people plus the Yankees. I had a pretty good time, but very tired.  It was now past midnight.
I must be up by 0700. Hot a bath will feel right in.

25 Oct - Friday - Up at 0900
after a rather poor night from indigestion following my mother's meal. Partaking of wine-rose at the cocktail party. To office + breakfast of good omelet and tea. Felt very groggy for an hour + then began to feel lots better. But my cold is still giving me hell - lots of coughing + stuffiness in my head + chest. Coffee + a glass of water in the morning with St. James on Ticonderoga.

attended bi-weekly 8:30 conference with George at noon + met a lot of people. Listened to Lumina and Mr. Colman.
When I returned a long time.
At 1330 another conference
& at 1400 Earl's weekly
staff conference. Marion
Rutledge Campbell called me &
left a letter from her mother just
as I was about to call
her in response to word in
George's message. I have arrang
ed to have dinner with them
this evening. My air priority
# is coming from Washington.
Today but my priority order
has to be booked + I don't
know when I stand or when
I go back. Am anxious
to return. Discussed things
with Earl until 1130 & am
home now. Must get dressed
to go to another party - Red C is giving for us at Bad Hauheim, only 36 miles away! And I'm so tired already. To rest for the wedding next night - back from the party which was pretty nice. The Coles, Miss Dent, Red and Miss Dulaney. First at Red's house, a large and imposing German doctor's residence. With many rooms but only one enormous bathroom. And the house had a funny, spices-like unpleasant odor despite it having been thoroughly cleaned just this week. - Cocktails there and then to the Grand Hotel where we had a very
nice dinner, cake, liquor &
dancing to pretty good music.
The party ended at 2:00 &
we had the long drive back.
News - I'm probably leaving
here tomorrow & certainly
by the next day. Will be very
 glad to get home. Yeah, I'm
 Advised to 00:25 now & must be
up by 07:00 again.
26 Oct - Saturday - Up at 07:00,
to Office & Breakfast. - Much
ado about getting me on a
flight to Paris & getting in
all the odd & ends of being
here, getting some gifts, writing
book letters, telephone calls.
Thought I might go out this
afternoon but it now turns
but I leave here for Paris on the 14:15 plane tomorrow. Phred and Dr. McCloskey in Berlin had
most cordial talk. She wants to be remembered to everyone.
Dr. Bremner, Dr. Ward, Dr. Lumley, Dr. Lettinghill, Mrs. Freidman. She
was very glad to hear from me. I called her at Radi's urgent in
sistence after he told her I was in the theater. — How much try
to get in touch with Marvi.
Doyle Campbell. — Later I
sent her over to the Rottenbar
for coffee and half hour's talk.
She more beautiful than ever
+ looking gorgeous by happy very sweet. Sorry not to talk
with your husband. — how 23 30+
I'm practically all packed and ready to leave tomorrow. Took a nap this afternoon after some shopping. I hope the forecast is still good. I got a little fear of flying. I hate to do that sort of thing because I don't feel proud of myself or my taste and knowledge of values. I wanted to take Jean and Earl out to dinner but they wouldn't. I guess they're tired out from all the festivities. We had a light dinner here and just took it easy. I packed and thought I've gotten all my stuff in all right.
October  November

SMTWTFES SMTWTFES
1  2  3  4  5         1  2
3  4  5  6  7  8  9  10 11 12  13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31

Hotel Napoleon Bonaparte, 38 Rue

Freeland - CARNOT 7420, WAGRAM 4511

Mar Easley + St. T. Stewart, Room 108

Amsterdam, ANJOU 7460 Ext. 182

Capitalenn - BALZAC 5400 - Ext. 155

Office - Rue de Perouse, 29

Hotel Ambassador - 14 Blvd HAUSMANN

Le Grand - JAS 9141

Cal Earle F. Cook - Office: Frankfurt military 21989 or 23210

Ansbach - 71 Karl König Weg, Tel. 1954

Only - GSB 514

Ansbach - PRO 7221 - Glen 633

Ansbach - PRO 7221 - Glen 534
Sunday 21 Oct - Left Frankfurt by rail at 1800 hrs
Monday 22 Oct - Arr Pant at 0815
Saturday 28 Oct - Left only for Paris 1345

Arr Weekes - Iceland 1815 local
Sunday 3 Nov - Left 1120Z 1400PDT 1100 GMT
1500 EST, 1900 Beijing, 2100 Z
Arrived Goose Bay 1600 local
Monday 4 Nov - Left Goose 1410 local = 1910Z, 1510
Arr Newtown 1835 EST
Left 112135
Arr Washington 2325
27 Oct - Sunday - Up at 0900 after a good night's sleep. Second breakfast and have finished packing. It's now 1100 and the weather is very cloudy and looks like rain. Supposed to leave home at 1300 so as to be at Euston at 1315. It's now 1300 and I'm writing this on board the Frankfurt-Paris Express train. For when we got to Euston field we learned only then that the afternoon Bucht Express flight to Paris had been cancelled because there was no plane available! So Earl and I at once decided to try to get a reservation on the train. Luckily it is Sunday, traffic is light and I was
Mistakes I made and Errors of Judgment:

1. To fail to bring my electric razor
2. To fail to bring one uniform instead of the gray suit
3. To fail to bring two OD shirts instead of many white ones
4. To fail to overcome simplicity and restore the currency black market in France.
5. To take the necessary steps after 24 hours to get my pay temporarily raised.
6. To fail to get at least 2 bottles of sherry from Erskine.
7. To fail to bring along that small can of bicarbonate of soda which I missed having when I was just over-tired. I didn't need thereafter.
able to get a reservation. Then we went back to Earle's house and the Bayard's came to visit, and we spent the afternoon talking. Also Earle got in touch with a chap in Newark, Ohio on his short-wave phone set, and I gave him a message to send a letter to Elizabeth—but just as soon as we tried to verify checks that the other end got the mail, address correct, so much ARM came up that further communication was impossible. So I don't know if Newark got the message straight. If he did I will get it. I asked him to wire me at Hotel Napoleon du Caire in Paris.
Get 1 can:
Zuney, F
On certain phases of war
research in Germany
Nighth Field.

Send Zuney 2 E booklets
on Russian language
Tell me how things are. I've had only a bit worried so far this week. I've written you one letter. Write me again.

We've been getting along well. We've been spending a lot of time together. Can we come to the Pines next weekend? I'd love to see you. Please write soon.

Miss Brown

[Handwritten envelope]
berk has just been made up + will turn in soon although it's only 2000. But the light isn't as good for reading so I won't be able to do that. I am just as glad to go this way to Paris rather than by air - a lot of accidents recently + only about 35% of available aircraft are in condition - can't get replacement parts + good repair crew.

29 Oct - Monday - After a most uncomfortable night because of excessive food on the train, got to Paris, STARE de L'est at 0815. There was no water on the train - it had all been out overnight - so there
wasn't any for washing & shaving - and the toilet was very cold because of lacking water for flushing. Got my luggage off & the porter found me a taxi quick so I went directly to the Hotel Metropole & checked in & get the same room (114) as before. Had a nice breakfast after which I phoned Maj. Osler who was glad to hear from me again - nice young chap. I got from him the phone no. of Capt. Cram who had been at Arlington with Earl & is now at Sig.
and called up Mr. Raynor. He was immediately asked me to dinner that night and I accepted. He was going to make it an Arlington Hall reunion about which I later learned. He was so tired I decided to spend all day in bed so went up to my room and got into bed, coming down to lunch at noon. Here I happened to sit at same table with an interesting fellow, a civilian in Army who had just returned from writing and who in conversation he in the world famous D. Fritz Zundel of Mt Wilson Observatory and Prof. Astrophysical of Caltech. We found a number of...
friends in common, including Col. Stratton of Trinity College, Cambridge. We talked about Edington, Jena, Munich, etc. - and a most interesting time. He is going back to Washington today, I hope we'll be on the same plane. - My telegram home later was outraged at the costs. £950. So friends were quite double what I should be left by - on account of depreciated franc. I later found I could have sent it for normal cost through PX and Army facilities.

Went back to bed and really slept for 2-3 hours, but felt pretty punk when I got up anyhow. - Rather, showed.
dressed & got taxi to Hotel Ambassador to keep my dinner date with Capt. Helms. On the way downtown to get taxi when pulled over by Capt. Marcus! A good man. Riding a taxi in the evening traffic in Paris is a hair-raising experience. Here too they drive like mad! It's really awful. Got to Hotel Ambassador & there found waiting all ex-A-Blites - Maj. Erskine, Capt. Glenn, Capt. Wallace, Saul, Wisselton, Stuart, Stewart - felt like joining a college reunion song. Glenn had reserved a nice table, the food was
good & he had wine & cham-
pagne. We all had a very 
good time. Mr. Wiedemann 
was funny at one spot. 
he is on duty with Office of 
Foreign Liquidation Commission 
in Shanghai but is in Paris 
on temporary duty. When he 
reported in he was asked 
where he was born. London. 
where his home is. Honolulu. 
where he is stationed. Shanghai. 
what is he doing in Paris. Temporarily. 
the next question "Do you speak 
English?" !!! We finished 
dinner too late to go to see 
any show so Mr. Stewart 
picked us in his jeep to the 
Champs Elysees & we.
walked a bit; then went to
the Officers' Club & had a
few drinks. It was then
after 23:00 & they all took
me there to my Hotel, where I
hoped to have answers to my note
to E - but no answers. Went
to bed & had very funny dreams
when in the mixture of food &
drinks, but slept fairly well
nevertheless.

24 Oct - Tuesday - Up at 0800
had breakfast with Col.
Harcus. A long discussion on
the black market & current
situation - which is most
suspicious & according to him
a great reflection on the
instability of the leading...
trains in the Army. - You just can't become the soldiers for
beating the game by any way
or means they can. Some
Frenchman high up are get-
ting away with murder. - The
official rate of exchange is
114.71 Francs per dollar. But
you can get 200 Francs by
dealing with any one of the
bank marketers who accept
you on the street. This was
proved to my satisfaction
this afternoon - as well be
related. - Coffee breakfast
went over to the Embassy
to see Easley, gave a PX
card, etc. Spent three hours
there, also seeing a gadget
The Dept. maintenance mail (Hirsh) fixed up for automatic operation 1000 on incoming tape. Saw Elizabeth Dangladey (formerly from AN) called Col. Atwood here desire to transfer to Frankfurt. He told me a letter from E had come yesterday + had sent it back to U.S. Damn! I walked to + from the Embassy along the Champs Elysées & a wonderful experience on a nice day. Back to hotel for lunch + caught our 3:00 train. Luckily finding him at a table where I could.
sit. - A most interesting talk about his forthcoming experiments on sending a rocket to the moon - a fascinating man. He says that the atomic scientists have been getting more credit than they really deserve - the larger share should go to the practical engineers and chemical engineers who turned the theory to practice - some peculiar remarks about Wehler as a colleague. - I'd love to study astrophysics, maybe I will! After lunch a talk with Bob Marcus and much kidding.
in his usual snide with the girls of the ABC counter but be gets away with it. -Walked again to the Embassy to get my money for a PX card (S'm in need of cigarettes) + there found the deep-laden of Ed Lattes. I'd read an Hanks story forwarded by Boris with a note to me. - I'd found out that Ed would not be leaving tonight so invited Ed to a + Prof. Hanks to Opera to see Mission - Stewart already was booked to go but he is getting the tickets for me. - Walked back to hotel + saw into Col Marcus
again & he agreed to go with me to get PX card, then to PX. - All counted some more large kidding, I asked one of the men to give me 250 francs for a $20 traveler's check. I gave me journey to Finance Officer - I got $10 in script & 1200 francs, the official rate. - M & I then took a walk to Avenue d'Iena to get my PX card & on the way we were accosted by a black man about. He asked where had gave for 500 he got 2800 francs "I just five minutes before."
got only 1200 frames for the game amount!! I felt very much put out. Missus & I had a further discussion about the inequity of the thing. - Got my post card. Then walked to PX, got wriggles, candy, soap, razors, blades. Then back to hotel where I've been writing this ever since. Thank goodness mum about caught up in my diary. - I forgot to say that Edie was good enough to sell me a bottle of Schenley + she had a drink out of it - at 1845 gin to me at hotel
Cullon to meet Earley +
2pm for cocktails + then
dinner + then Opera Com-
gue to see Mignon. Boy
join bread now + must
rest at bot.
30 Oct Wednesday Up at 0700
as I felt slept out despite
getting only about 5 hours
sleep. As for last night:
I got shaved + dressed +
was ready to leave at 1815,
and seeing that I'd walked
to + from the Embassy four
times already I wanted to
take a taxi but there was
none so I walked again.
Got to the Cullon (which
is right next door to the
Embassy at 1 o'clock after the appointed 1845. Found my Easley there but not Capt. Atlanta, as neither had a date too. Also, no tickets available for Mignon or any other place so we decided to take a chance on getting into the Folias at the last minute via the ushers' black market route which Easley said he'd heard of. We had a nice cocktail.

Saw r spoke to Mr. Thompson & Mr.ATT (to see him last in New. Farnham's office a couple weeks ago. With him was Mr. DelGio of State Dept. who re-
remembered me very well. I asked him how he'd enjoyed his visit to Worzes for which he countered by saying "I see your secret service is working as usual." There were a couple other State Dept. people whom I didn't know. - Easley then took me to dinner at the Hotel Vuillon, where Elizabeth and I stayed a night or two in 1933. A very good dinner with excellent steak (thin but in fine French taste), chocolate ice cream for dessert. Then tried to get taxi to Tolbiac, but none available so went by...
Metro - fastest & very much better still sound in my opinion - at least you don't get scared to death at the crazy driving. - Well, we got two tickets OK via the 'under' black market route, for which I had to pay a premium but not bad. Orchestra seats they were called but were in 2nd Balcony, right in the middle & very good at 25.5 francs each plus 50 fr. for priority service = 606 francs or about $5.50, which isn't at all bad. - The show was marvellous, most of act (Chinese)
only describe as magnificent + like nothing I'd ever seen before. - Magnificent costumes throughout. - I bought a booklet (220 frames = £2.00) y. hardly worth it, but something to show at any rate in describing the taking to E). - A couple of tiny cognacs between the acts cost £2.00!! - It was a long performance, from 3:30 + 11:45 + when we got our two taxis still in sight so home by metro + said my farewells to Easley. I was back in my room by a quarter past midnight & slept
tired but feeling very well. Got into bed but took me some time to fall asleep, for some reason I often had very soundly from about 0600 to 0630 — up and had a bath, dressed, then to breakfast with Dr. Zuckley & some more discussion. Called Dr. Compton the arch-traitor, "with Almighty God in his right pocket & Jesus Christ in his left pocket. He was quite outspoken against the big name scientists, said they'd deceived the rest of them. The purpose to drop A-bombs which means..."
worked in part as an answer to believe it was to be defeated. Also that Art Compston in 1940 caved in because in the plan Bindon was looking for an ideal to achieve. Besides people do not want to admit that Zurich was every bit as involved in the plan as London was in 1940. People have no idea he was. He was just cast aside because of everyone else's involvement.
organization for preventing future disasters - believes only in individual efforts. I had to cut the discussion short since I had to leave. - Will not doubt see him again. - Asked about my current status and learned I was probably going to leave today. Decided this was by my other gift. I was going to get here morning. Got some frames from hotel photo (gold plate). Bought following:

- Scarf from J R - $50.00
- Cigarettes - $10.00
- Powder - $2.00
- Scharlau - $10.00
There were many beautiful clothing and apparel articles for women but you need not only odors of money but also points as most articles of clothing are still rationed. But you can buy the "points" - again black market dealings but not under cover. The poor people sell their "points" - the shop keepers will sell you the necessary "points"! It's all fantastic. But I didn't want to budge buying wearing things this time. I'm not as brazen as I was in my younger days. I had lunch confirmed that I'm probably going out tonight - still No 6 on the list but was told to report at 1630 again. Phoned Easley as it was a lovely day out.
I suggested he take the afternoon off & go with me to Montmartre, which we did. We walked a lot; the rain was then no longer out & it got cold up on top of the hill at Sacré-Cœur. We rode up the hill on the funicular car or "inclina" at 2 francs each. A wonderful view from on top but clouds & darkness obscured a lot. Had a rest & a vermouth at a very small, spotlessly clean cafe - we were the only customers. Back to hotel by taxi & I reported in at 7:00 - notified to "stand by" a call - I might be any hour or not until morning - a lot of indecision as usual. Took a rest
(my feet very tired) had a small drink + then early dinner. Now in my room, practically all packed. I think Zwickly will be on same plane. Have invited him to have a drink with me after he finishes his packing.

31 Oct - Thursday - I had a wonderful sleep - in fact, didn't hear the alarm + almost missed my breakfast as I woke suddenly at 0615. Rushed dressing + missed a badly needed shower but got my breakfast with Zwickly again, continuing our discussions of last night. Zwickly came to my room + we talked -
enjoyed it more than I have for a long, long time—talking science and philosophy with a kindred soul. He told me that in his opinion, Frederik Nansen, the explorer, was the greatest man of his times—and why he thinks it took long to explain. I would love to have a recording of Tuck's remarks after we had a cup of drinks. I like him tremendously and think him a great man.

Got to bed at 1 a.m. before midnight and so said, had a good sleep, despite the very exhilarating conversation. After breakfast fast I shaved and got dressed all over again, took a short walk. Hasn't been bad.
At about 1000 that I was to be on call all day - at very short notice, which meant that I'd probably be going out today. I walked over to the Kielair, stopped in the Signal Office to say hello to Col. Reynolds - we had about 20 minutes chat - he seemed glad to see me.

Back to hotel & found Zucky all in a dither because his name wasn't on the list & I told him what I'd been told. Then verified it to him by showing him to talk to the desk, which my name appeared but not his. He rushed over to the Embassy to see what he could do towards getting a No. 1 Priority.
Had lunch (Twinkie not around yet) talked with a couple of young ATC men. Talked about how it was important to learn the cause of air crashes. One of them suggested that it should be arranged so the control tower could listen in on all the talk going on in the pilots' cabin and take off/landing. The other pointed out the practical difficulties in working over the communication system. Then suggested that an automatic record be made on magnetic tape in a fire-proof container. They thought it a good idea. I may suggest it to some authority when I get back. — Sain Twincapa
I'd about finished & went to join him. He still in a dither & having a hard time locating who had his No. 1 priority post. We went to the "desk" & there for 30 min I sort the "secret list" - with my name on it but still no Zivicky on it. - And also the name Kohler. I had made pretty good friends with the girl at the desk & asked her to find out the full name of this Kohler, suspecting it might be our own Dr. Hans Kohler of Arlington Hall. And left in July to see his old parents in Switzerland. - And sure enough it was he, so I got his phone no. at the hotel
where he was staying, called
him up, asked him to come
over (not far away) and was
he pleased and happy to see
me. He's been in Paris two
weeks—waiting a priority to
come for air transport back—
he couldn't get a ship
passage back at all until
next spring. Took him up
to my room where he appreci-
ated the heat (no heat in
his hotel!) and we talked a
couple of hours. - Tricky &
Kathryn both being Swedes
thought it would be nice to
get them together, so after
a bit I went to look for
Z - found him downstairs
and out of his duties after long and arduous planning to find out what places led just got his priority business straightened out. I invited him up to my room. I introduced the two. We sat around discussing science and scientists. L a man of very positive and very outspoken views on persons and things. High admiration for some people like Einstein and quite devastating about certain others such as Hillsb. A A Compton, de Broy (now at Cornell). I went downstairs than to see if I could get talk to Messrs. O'Brien into getting me a note to Kekulé as my
guest at dinner. He gave me a long song & dance about how & why it wasn't possible but I persuaded him in the end. So the three of us had dinner together, we continued our discussions. Z has just about finished a book to be published in English under the simple title "Truth" & in German under a slightly different name. I got him started on telling us what it's about & he outlined it - a new approach to the basic problem of knowledge & what is "truth" - very fascinating & I think will make a great impact on the world's philosophy. We talked on
when about 2300. I saw BK to the hotel door (handing him one of my two quits of long underwear). Be most grateful for everything.) BK's wife is Prof of Spanish at Mt Vernon Sanitary & must be quite a person - we must get together soon. I then to my room, took a bath & have been catching up on my diary. We were told we might be called at 0100 as I ought to catch some sleep. I am also told that what is holding us up now is weather. Maybe I'll get off tomorrow - I hope!

Nov. Friday - Up at 0600, short, had breakfast. No further news
I decided it was time to do something about getting my priorities as it became clear that as soon as the weather cleared, there might be a number of priority 2 and 1 passengers show up. So I went over to Signal Center to call Cook. Although Glenn got a line through at once, but Cook was out so I talked with him, who said he take it up with Cook. Then went through the Signal Center with Glenn, to the "Blockhouse", from bottom to top. The Germans built it in 1940-41 as a Signal Center, four stories high, concrete walls 10 feet thick, roof of course, no windows, no air conditioner. Took to hotel, in a few minutes news came of a brand new list.
Zwicky's name on it but not mine. Which confirmed my worst fear. So I decided to rush over to see if Col. Raynerford couldn't do something for me. We called him again & he said they couldn't do anything there for me—so I'd have to see Col. Warner of AT here. So I rushed back to the hotel to be confronted with the news that they had been lettering for me—two people on the list with Zwicky couldn't be located so they were going to put me on! But it was too late—the bus had left. The manifest closed. Next best thing was wait around. I'd sure try to get out this afternoon.
and put on at 1500. I got myself all packed so nearly 3 or in the middle of which Jessie was called from downstairs and said she'd come to see me off. I finished packing and went down to see her and Snow from Hancock first both here on leave. By 1450 things were certainly but 1455 came and to get on the 1500 bus. So I got my stuff down, no bus but a 6x6 weapons carrier. Jessie took my picture on board the awful looking truck. We said good bye. I'd arranged by phone already with Captain Schmidt and also with Maj. Oiler to send word back.
to Greenwich, respectively that I'd left Paris at 1500. Not too bad in cold a ride to Orly. I get there, check in & am told to go on Flight E-8 to Angers. Then go into waiting room. There Zundel's still waiting, with parachute harness on, ready to go, but waiting. The weather very foul. Pretty soon get out to desk to check in again. Am told I was transferred to Flight F-2, the same one Zundel's on, for reasons too complicated to enumerate here, but F-2 goes to Iceland, F-8 to Angers. However, it would be nice to be with Zundel.
We sat down in VIP lounge
had a sandwich. Pretty soon I
go out to check again to
find that E-7 was cancelled.
Bad weather! Don't understand
how such things can happen!
We had to get our things &
go back to hotel Nap again.
It may be we'll be able to get
in there again. - Rushed to
get the bus & just made it.
Back to hotel & I was very
lucky to get my room back
after rushing up to the place &
finding it hadn't yet been
assigned. Then came down &
argued with the clerk.
Poor Zwikey though had to
go up to 7:45 to go.
Elevator—They never work here.
So he has to walk up each flight of stairs.

Immediately phoned people, "Jesse, to get word to Harlem to get word to Cook to cancel message saying I'd left, to get word to cancel message to G-n saying I'd left Paris, to Dr. Holden to see what this situation is, and all chance mine. - Have had dinner and now am waiting for further word. What a mess! Jesse and Harlem asked to me join them but I decided best to strike close to hotel. Don't dare leave, Jesse is coming over to see me in a.m. if
I'm still here & if so, get the AG here to do something to change my priority in unit.
8:00 now 22:30 + 3 in my bed. No news, no change in situation - I phoned Kohler & he came over. He, Zwick & I spent evening together. One of Z's former students named Hayes, have attending Karnan's lectures, gave us the last of his schnapps from Switzerland - each having an ounce. - I hope the weather clears in Iceland & we can get off tomorrow.

*Nov. Saturday* - Up at 07:40, showered, bathed down to breakfast at 08:15 with Z, after which we both went to see Major Skillin, who seems to be direct or indirect traffic for ATC. Z & I walked...
To get the straight facts one must sift the 
apparent trend and see what the 

real situation is. The immediate 

problems are: 

- Schedule over runs - 1/4 off. At any 

rate 1/2 of the work is supposed to be on the 

books so it's not all bad. 

- Our first order of the year was placed - 

right on the blast furnace. 

- New orders - 1/2 more - C. G. & Swift. 

Good with their 

order. 

- Ocean freight is too high, we should have 

reduced our price - about 

40%. 

A. G. says we should have 

reduced it by 25%. 

- My own prices are 

10% higher. 

- We should be able to hold prices 

at the present time - 

since we are supposed to be 

up in the market. 

- Our best order is about 

2000 tons. 

- We are running 

40% above average. 

- We are running 

50% above average. 

- The trend is 

upward, and should continue 

for a while. 

- We should be able to 

hold prices at the present 

time.
I went so long in flushing the fell around - it was quite painful. So he immediately began the motions toward raising my priority. I gave them assurance it would be done. He also bawled out the people at Colby for their manipulations of the priorities there and excused them (to us) by saying they were new, didn't understand it. It was easy besides - because it meant a lot of work in changing things around. Well, we went back to our hotel with the assurance from him that we'd leave today on the F3 flight to Iceland at 1200. We felt pretty much relieved as a result of our visit and I finished up.
my packing. Jessie sent phoned and I told her latest word. She will check this p.m. if I'm gone will get word to Cook. I forgot then to call Dr. Stewart at Century to tell him latest word but I think he will get it anyhow + will send word to wash. I also phoned Dr. Kohler + told him whom to see + to keep after people at ATC. The organization is pretty much disorganized. We got the 1100 bus to City checked in at 1066 and took off not at 1200 but at 1345, which wasn't bad. I'm writing this now at 1430 so were over water now I think but can't be sure as we are in clouds. We are supposed to fly at 0500.
The plane is comfortable & clean. I think we'll have a nice trip. It is scheduled to leave at 9:00 am Wednesday from the airport. The weather yesterday was foul but today it is quite good & the flight should be very smooth.

An incident of interest: just a few minutes before we were to board the plane, one passenger suddenly realized that he'd left $1000 in each under his pillow at the hotel! He rushed out just in time to catch the bus back. We left without him (I'm a Sergeant) & I hope the poor fellow finds his money. We have an empty seat in the
plane. - Well, we arrived at
Meck's Field, Iceland in 6½ hours
flying time instead of 7½ because
we had a good tail wind. The
trip was pretty smooth all the
way. - Had supper of ham and
eggs at terminal. We were told
we'd have to stay overnight here
because there is no relief crew
to take our ship out. So we got
beds & slept and after waking about
talking about 2 hours (I was
surrounded by a group gaggle
eyed by his explanation (jet
propulsion etc., a most interest-
ing lecture). We went to bed
in a barracks-like affair con-
structed madda...
Month that the wind is
terrific here but it is not cold
strains all the time.

3 Mon - Sunday - Up at 0700
local time. Shaved, dressed,
traveled to terminal. Breakfast
of ham and eggs. - Got aboard
plane, taxed down the field,
maneuvered around - and then
came back! Engine trouble.
In the terminal, where
I see Mr. Kohler. A warm
reunion. He'd just gotten
in his plane due to go out
in an hour. I'll probably
get to Washington before
So, maybe we'll have to
wait and go to Goose Bay another
night. - Talking about
disorganization - somebody failed to close & fasten the door to my plane last night. As a consequence, the two rear seats (one mine) were draping wet. Luckily I had another seat, first one forward, so could get that one dry while wet. - The weather is nasty out, heavy wind & rain. After about 1 hour, we went aboard again, tested the engines out - still trouble and this time we were told they'd have to take the plane inside the hangar - too rainy & windy to work on it outdoors. So back we went in the wind & rain, with our bags to the terminal, prepared to stay at least
four hours we were told. Sat around for a half hour then we took a bus which took us to the hotel. The hotel where we stayed last night, soon the bus came and just as we were about to get on, the man came and said the trouble was fixed! So again we boarded the plane this time we take off at noon local time, in what looks like very soupy weather. Pretty soon we are through it now the plane is climb to and smooth. When we got aboard the heat was so thick and almost unbearable so the engineers had to turn it all off. Now it is freezing inside. He is working on it and I hope he gets it fixed soon. I forgot to
mention one funny thing that happened to me on the landing last night. We had put on our Wee Wests, had our belts all fastened & were coming down fresh, just as we were about to land. Somehow the left-hand cartridge on my line West went off (I couldn’t fasten the safety cord when I put it on, the string was too short, the slingshot didn’t. Then when I showed it to him) it was important my West was fully inflated after a brief explosive hiss which of course took me quite by surprise. No harm done though & I simply opened the release.
valve had failed the thing.
Will have to watch that
again. — how were about eight
con hours behind our schedule
& I hope we won't have to
stay over again at Horse Bay
for any cause. — How are
the seven hours later? The
train is on again! —
Now about 1430 Eastern Stand-
tard and Time & we are due at Horse
Bay in about 35 minutes, how
over Labrador and does it
doke rugged! And decent!
& thin layer of snow over the
floors & ice on the thousands
of tiny lakes & streams. — We are
beginning to come upon my
home tall trees. — It has been a
very calm journey thus far
The ice on the lakes is not very thick & shows many cracks. Where the snow has piled up on the ice & where it has either melted or the ice underneath has gone there are myriad of curious lacy & delicate designs – the other have only marred a little bit by my recurrent hives! They served us a lot of fish in various forms in Paris. I couldn’t think of anything else that would bring them back. — A good deal more snow as we go further south. — Boy, did hate to have to land down there now in that rugged wind. — We arrived at 10:00 local time.
after a flight of 8 hours and 10 minutes, we were met by a nice, clean bus and taken to the hotel de'Ercole to stay overnight! Bad weather at Westover Field, the only one the Army will allow F-2C planes to use, so despite the hundreds of possible fields we might use, with Westover closed in, we are stuck for the night again, and again we suffer at least a 12-hour delay. - Kolber gone, so we will get home a day before I do! Whitman - checked in, got a room with Zwicky + a Russian colonel who is M.A. in Washington. - We cleaned up a bit and Z+E had another long talk, this time about German developments in research before V.E. day. I learned
n most amazing thing. They had not one but three different ways—all completed months before the deed—by means of which they could have exploded any aircraft within any intended path with a base 30 miles in diameter off the thousand feet high. Why didn't they use it? Here Z became quite eloquent and vehement and gave what in his opinion is the reason why a democracy of free men will always beat a dictatorship: fear of the consequences of possible failure. The German scientists were afraid of their lives if the theoretical and experimental devices didn't work out in
practise as promised. They would have to guarantee the success of the project - that failure being to forfeit their lives. That was the principal reason why all three separate groups of German scientists with all their discovery from the Nazis. A secondary reason was that many of those men weren't too sympathetic to the Nazis and weren't too anxious for them to win. And a tertiary reason was that those men couldn't get the support of the big-name German scientists like Heisenberg and Haber, who no fear for their own work would be reluctant to go onto
a bomb + gave only lukewarm endorsement. And that I told
me in not hearings - he talked
to the men + saw the gadgeter
himself. He told me how absolu-
tely amazed he was at the
simplicity of the basic idea +
how much more he was amazed
when the Germans told him of
them + why they didn't actually
use them. Z says they tested
one of those devices 35 times +
shot down 35 planes, 100%
success on experimental basis.
Z wrote the business up in
an AAF paper + I'll get
on my return home. - We took
a bath for two or three hours.
About Neuenburg + was shalal


treatment by the British they
as a result of the wife's
children almost died. What
I did to get them straightened
out. - Of how Z conducted
the interrogation. "Homework"
of the 400 German scientists
who had been recalled at Tarn-
wich. Parsons Church. And the
authorities let them practically
stand until Z raised hell to
got food from the army for them.
Of how Z got into bad by being
a rather severe taskmaster
in getting work out of these
Germans. The British had to
get an official reprimand for
Z - but it wound up in the
end that the Germans al
wanted to work for Z in America, & didn't want to do anything for the British. I imagined that Z is a serious, hard taskmaster but a most fair & just man without an ounce of insincerity or hypocrisy in his makeup. When I changed shirts he made some comment that I seemed to carry everything with me. I offered to let him have one of my shirts, but doubted that my size would fit him - he's an enormous man. He laughed & told me a story about getting some shirts, size 17, & how the lady who had volunteered to obtain them bought him size 16, saying that
Oct 24-

JR Frankes 3183.00

Scrap $ 50.60

US $ $ 10.00

Travel Checks $200.00

Air Line with: -

$ 34.15

Freight 160.00

$ 194.15

JR Frankes 139.
at the shop she visited, when she asked for 17's she was asked for whom they were. She said for a professor. The salesman then assured her it just couldn't be so as only fire fighters and marines wore 17's. It was impossible that a college prof could have a size 17. We then talked about the man with the singing in his ear, headaches, and pain in the neck. I laughed, laughed, thinking it a well story. We talked about Volume + Brush + Coolant + Copper + others. Of Shapley and Norris Russell, et al. I enjoy him immensely; find so many things
in common with him. I wish he lived in Washington. I have long yearned for a walk companion whom I could count as a real friend. There have been very few in my life and the usual
than conventionally. Z's stock of technical information and knowledge is enormous, I could learn a
learn great talking with him. Well, we went up to dinner
at 10:30 and there was a very nice bar and dining room. So I
ordered cocktails (two rounds) for us, excellent drinks only
$2 each. Then a very nice dinner with exquisite food and
well cooked. Everything nice and hot. After dinner, more talking.
+ Then a walk in the crisp snow - not cold out, it seemed because the atmosphere is so dry. A fine 74° night with an enormous halo - a lovely quiet night. - About seven o'clock all the hotel planes were lined up and grounded because of bad weather elsewhere. - We landed in ok shape but I didn't sleep too well. Forgot to say I took a nice shower the first one since leaving home. I enjoyed that immensely. When I came back into our room with my bathing cap on, 2 exclaimed "Why the devil has everything?" - Saturday--Monday - Up at about 0630, much noise during
The night of people coming and going so I didn't sleep too well. Shaved, dressed, breakfast of ham & eggs. The news of departure not good—it seems we won't get off until mid-afternoon. - Z & I walked a good deal, I sent a telegram to E & cabled a train clerk a change. - Fine, crisp, sunny & clear day out. (Aboard the plane now) - We had a lovely lunch after vague rumors we'd be leaving sometime this afternoon. We'd just about finished eating when all at once they said we got word we were taking off in few minutes! - Got our things together, paid our bill for the hotel (is it! which pleased
quite out of line with the $1.50
dinner last night) I went to the
passenger terminal. There I talked
with the officers in charge and requested he wire Westover Field
to land the shuttle plane to
Washington if necessary. He agreed
to do so after I received support
from the Argentinian consul and
other passengers. We took off
at 14:10 local time = 13:10 EST
and are scheduled to arrive after 41/2
hours. Weather calm but we
are flying in cloudy haze all
the time. Hope the field is clear.

One of the things 2 & I talked
about yesterday I failed to
record. The way in which Swiss
technicians are leaving inside
Germany in spite of the fact
secret German projects got their information into American hands. It was all done by individual Swiss working alone, without cooperation of Swiss govt. One of the important plans of information they got out was notice of impending invasion of Switzerland twice in 1940 and once in 1943. The Swiss govt mobilized 1,000,000 men & the Germans had to cancel their plans. Z says this is recorded in fact official report of Swiss Army's chief of staff. Z has said that he & good many associates of the Swiss scientists at U.S. got continuous progress into re. German scientific at the note of their lives.
Arrived at Winston at 18:35, the sea quite calm except for a few minutes now and then. We rode just over very heavy banks of very dark clouds a good part of the way. On arrival we cleared through customs zip, just like that, as I think some notice of VIP arrivals (maybe me?) must have been given because the OD came aboard and pretty soon I and the Persian Colonel were loaded to a nice shiny car and taken to the terminal. This enabled me to clear customs & immigration.
The first. Then I sought information re a plane to Washington but things are quite SNAFU in that respect. The OD AOK us. The regular 1500 shuttle plane was cancelled & a special C-54 is now on the runway - but it developed a leak in the gas line & that must be fixed before it can take off. It is estimated now to be ready at 2100 but we got our fingers crossed may have to go by train.

- About 2145 and aboard a C-54 Cargo plane bound for Bermuda, one stop in Wash
washington, due there about 2330. it's rough & a couple of the passengers are sick. i feel ok so far. - i phoned from westover & awfully glad to hear her voice. fed her the situation & not to come to airport. - soon we are over new york city - a wonderful sight. in 30 minutes more, over philadelphia. we are going about 370 a minute apparently. - now over baltimore, the flying is much smoother. - we are due at washington at 2330. now i can see washington, a very lovely sight below. sky perfectly clear. - down we go now. we have our homes
on—we had to put that on when taking off also. Arrived 2:32 a.m., a few minutes ahead of time. It's good to be back and will phone once
WAR DEPARTMENT
Office of the Chief of the Air Corps,
Washington

Memorandum for:

Mr. Friedman:

Series #
300, 217—deals
with M-138 and
in view of recent
happenings it seems
advisable to reclassify
this patent—

70, 412 and
443, 320

Small 382, 521
WGr 682, 096
Wgt 107, 244

Declassified and approved
for release by NSA on
08-06-2014
pursuant to
E.O. 13526

Hall is returning Rosen's
application—BR

CHAS. A. ROWE
Patents Section S. C.
Room 3143 Branch 1313
<table>
<thead>
<tr>
<th>REF ID: A4126886</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
</tr>
<tr>
<td>47</td>
</tr>
<tr>
<td>48</td>
</tr>
<tr>
<td>49</td>
</tr>
<tr>
<td>50</td>
</tr>
<tr>
<td>51</td>
</tr>
<tr>
<td>52</td>
</tr>
<tr>
<td>53</td>
</tr>
<tr>
<td>54</td>
</tr>
<tr>
<td>55</td>
</tr>
<tr>
<td>56</td>
</tr>
<tr>
<td>57</td>
</tr>
<tr>
<td>58</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Go to clerks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drawing go to Commercial</td>
</tr>
<tr>
<td>Company for reproduction</td>
</tr>
<tr>
<td>Drawing</td>
</tr>
<tr>
<td>Go to Richmond on Truck</td>
</tr>
<tr>
<td>unattended (daily trip)</td>
</tr>
</tbody>
</table>
Mr. Polton, Mr. Hall and the writer went to the Patent Office in Richmond on December 3, 1943. The purpose of the trip was to learn, first-hand, the manner in which secret applications were handled by the Patent Office and to determine both the procedures and the facilities for observing secrecy.

In Divisions 21, 16, 63, 53 and 56, it was found that secret applications were kept in the drawer of a steel desk belonging to the Chief of the Division in each case, and locked therein, the Chief of Division usually keeping the key. In Divisions 16 and 53 are kept some of the highly secret cryptographic applications of the Signal Corps. We were informed that in Division 16 these cases were given to the messengers for the purpose of carrying to other parts of the building to obtain photostats and to be delivered to other examiners. It is further understood that these messengers have not been cleared for secrecy. The status of examiners and others in this regard is not known. In Division 56, the cases are kept in a locked standard file. In Division 36, they are kept in an old standard file, which is provided with a lock. In Division 61, there is a key-locked file which most nearly approaches our combination file cabinets. The key for this cabinet was kept in the desk of the Assistant Chief Examiner of that Division.

Mr. Polton, under direction of Mr. Hall and with an order signed by Mr. Hall, proceeded to the photostat room and introduced himself as an employee of the Signal Corps, with no other identification, and personally being unknown to the members of the photostat room. He handed the order to the Chief of the Division, said order calling for a photostatic copy of each sheet of the drawing of an application filed by the Signal Corps, and asked if the photostat could be furnished that afternoon. The answer being in the affirmative, Mr. Polton returned at the appointed hour and was handed the photostats. No further identification
was requested.

Each Division has a docket-book, which includes the Serial Number, filing date, name of the inventor, title of the application, the status thereof, and name of the examiner to whom it is charged. These books are kept on the desk of the clerk of the Division and are not in the safe. While these books are watched during the day, it would be readily possible for a foreign agent to examine these books and ascertain the Serial Number and filing date of several Signal Corps applications, provided they knew the name of the inventor or some other information, and thereby get the data with which to place an order similar to that given to the photostat room by Mr. Felton.

When an application is filed, it is not put in a locked cabinet of any type, even though the case may be secret, until the examiner receives information that the case is secret. Before that time, the cases are kept in racks along the side of the wall and the drawings are kept in locked file cabinets, accessible to any person who might break in after hours.

The security of the portion of the Patent Office in Washington has been under constant observation for some time by Mr. Hall and Mr. Felton. This investigation has revealed the locked file cabinets in the War Division are not of approved construction, they being key-locked file cabinets. Mr. Welsh keeps the keys in the drawer of his steel desk. It may be added that Mr. Welsh's desk appears to be habitually locked, even throughout the day except when actual use requires it be temporarily unlocked.

Applications filed in the Patent Office include drawings. These drawings are sent to a commercial photostatic company in Washington for photostating. The applications are processed through the Patent Office in regular course of business similar to unclassified or perhaps "restricted" papers of the War Department.

Trucks transport the cases from Richmond to Washington and back. These trucks
Report to Col. Lippincott (cont'd)

are not provided with an armed guard and generally have a negro truck driver. The present conditions of the trucks raise the possibility of serious breakdown which might endanger the security of the documents contained. The two trucks meet at Fredricksberg, where the drivers exchange trucks. It is suspected, on the basis of remarks made, that the drivers in exchanging pleasantries, possibly stop in for sandwiches, etc., leaving the trucks unguarded.

______________________________

M. H. Moore
Captain, Signal Corps

______________________________

William D. Hall
2 Patent Advisor

______________________________

R. G. Pelton
Patent Advisor
PAPERS

1. A means of providing an irregular wheel movement in cipher machine using cipher wheels
   1. Carbon copy of final
   2. Original of draft
   3. Carbon copy of draft with hand written corrections
   4. Early draft with photostat
   5. Hand written draft

2. Instruction sheet and blank for patent application

3. Report on M-228 (to Col. Corderman) carbon copy

4. Draft "Replacement of the Present Combined Cipher Machine"
   Carbon copy of staff study

5. Report to Col. Lippincott on visit to Patent Office in Richmond


7. Excerpt from Drew Pearson on the Yalta Agreement

8. Informal memorandum on faults of cryptographic machine

CORRESPONDENCE

1. Letter dated May 16, 1935, subject: Blank forms for code accounting

2. Letter dated August 31, 1935 on principles of Converter Type M-134-T2.

3. Photostat of document dated June 26, 1935 on device to be attached to the electrical counting sorter, signed by Friedman and Rowlett

4. Photostat of memorandum dated July 6, 1935, forwarding draft of specifications upon which application for patent on Cipher Device Type M-138 may be based.


6. Copy of letter from Friedman and Rowlett setting forth the principles of M-134-T2, dated February 15, 1936.


14. Memorandum for record dated 25 September 1947 on Meeting with Captain Safford and engineers of Teletype Corporation.

15. Memo dated 20 September 1949, subject: Replacement of the CCM.
PAPERS

1. A means of providing an irregular wheel movement in cipher machine using cipher wheels
   1. Carbon copy of final
   2. Original of draft
   3. Carbon copy of draft with handwritten corrections
   4. Early draft with photostat
   5. Handwritten draft

2. Instruction sheet and blank for patent application

3. Report on M-228 (to Col. Corderman) carbon copy

4. Draft "Replacement of the Present Combined Cipher Machine"
   Carbon copy of staff study

5. Report to Col. Lippincott on visit to Patent Office in Richmond

6. Contribution of the Signal Corps. Carbon copy of pertinent passage from Naval history

7. Excerpt from Drew Pearson on the Yalta Agreement

8. Informal memorandum on faults of cryptographic machine

CORRESPONDENCE

1. Letter dated May 16, 1935, subject: Blank forms for code accounting

2. Letter dated August 31, 1935 on principles of Converter Type M-134-T2

3. Photostat of document dated June 26, 1935 on device to be attached to the electrical counting sorter, signed by Friedman and Rowlett

4. Photostat of memorandum dated July 6, 1935, forwarding draft of specifications upon which application for patent on Cipher Device Type M-138 may be based

5. Photostat of Routing and Work sheet regarding evaluation of patent

6. Copy of letter from Friedman and Rowlett setting forth the principles of M-134-T2, dated February 15, 1936


14. Memorandum for record dated 25 September 1947, on Meeting with Captain Safford and engineers of Teletype Corporation.

15. Memo dated 20 September 1949, subject: Replacement of the CCM.
The Contribution of the Signal Corps

15. Mr. Friedman and interested officers at Signal Corps Headquarters were familiar with the various models of the ECM, but not with the prospective changes which the Navy had concealed from Hebern. In fact, the Signal Corps purchased two of Hebern's nonprinting models in 1924. At the request of the Navy Department, Friedman undertook solutions of the ECM in 1923 and again in 1932, being furnished the machine, code wheels, instructions, and test cryptograms in both instances. Friedman was successful both times, and developed a method of solution whereby, under certain conditions of meter action, solution could be achieved without possession of the code wheels. As the Navy Department did not intend to use a meter action in the stepping of its service models, these solutions did not worry us particularly. However, the techniques and experience gained in these solutions paid big dividends later on, as they were instrumental in the solution of certain systems which cannot be named. These solutions were published in SECRET status by the Signal Corps in 1935, as

Analysis of a Mechanico-Electrical Cryptograph - Part I
Analysis of a Mechanico-Electrical Cryptograph - Part II

The Navy Department was not consulted in the matter, although furnished copies of these pamphlets after printing. This caused bad feeling on both sides which lasted for several months and led to an order from the D.N.C. that the Signal Corps was not to be shown the ECM (Mark I) or to learn any of its details. This order was not revoked until January 1940, when Signal Corps representatives were invited by Admiral Noyes to inspect the Mark II ECM.

16. Late in 1935, or early in 1936, Friedman disclosed to Commander Wenger, of Naval Communications, his invention of an electric stepping control for the electric cipher machine, and three different methods for accomplishing this electric control. These are all covered in Secret Patent Application #70412, dated 23 March 1936, in the name of W.F. Friedman and F.B. Rowlett. An experimental model of an electric cipher machine using one of the Friedman-Rowlett electric control methods was built by the Signal Corps at Fort Monmouth, New Jersey, about this time and shown to me after its completion. About 25 or 30 of these machines were made in small lots up to 1939 or 1940 and used for special types of communication, such as Military Attaches and Commanding Generals. These Army machines indicated the reliability of electric control but the undesirability of the particular method used in the Signal Corps machine.

17. Friedman and Rowlett assigned the entire rights to their three inventions to the U.S. Government (Secretary of War). The Navy took another of the Friedman-Rowlett control methods (the "Stepping Maze"), experimented with it, and further developed it.
This was done without their knowledge until the day that the Mark I and Mark II ECMs were disclosed to the Signal Corps. On that occasion (5 February 1940), I acknowledged to Mr. Friedman, in the presence of General Mauborgne and Admiral Noyes, our use of his invention. The Navy also considered the third Friedman-Rowlett control method (the stepping circuits through the "Alphabet Maze") with the idea of conserving space, but abandoned it as unreliable and impracticable on the recommendation of the Teletype Corporation. At the suggestion of the Signal Corps, a last-minute change was made in the stepping of the code wheels in the "Stepping Maze".

18. Electric control of the ECM by means of the Friedman-Rowlett "Stepping Maze" is the essential feature that places the Mark II ECM in a class by itself as regards security. Those who have participated in the development of the Mark II ECM have always acknowledged these contributions of the Signal Corps. The "Index Maze" adds to the security afforded by the "Stepping Maze," but it is worthless without it. The importance of electric control can best be estimated by a consideration of what the Mark II ECM would have been if Friedman had not disclosed his invention to the Navy. Although the "Stepping Maze" appears obvious, now that it is in use, no one in the Navy thought of it in a period of 15 years, and no foreign machine employs it. Therefore, the Navy would have continued the development of the older methods and the new ECM would have used the mechanical stepping control found in CSP 903 or CSP 1700. We would have had a secure machine, superior to anything in use by foreign nations, but definitely inferior to our present ECM. This hypothetical machine (as well as CSP 1700) would defy attempts at solution until such time as machine and code wheels were captured. After this, each day's keys would resist solution for a long time. "Short-cut" solutions would be impossible, due to the erratic stepping of the code wheels, but a trial and error solution would be within the range of possibility. We could not make the flat statement, as we do for the Mark II ECM, that solution would be utterly impossible. In other words, the machine would be adequate to take us through World War II but, because we had stopped short of perfection, there would always be the desire to develop a new machine with electrical control. Friedman and Rowlett are entitled to full credit for their invention of electric control and the "Stepping Maze," which add so much to the excellence of the Mark II ECM.

19. The Signal Corps' willingness to accept the Navy ECM for their own use as well as joint Army-Navy use, and to drop the development of their own machine, reflects credit on all who made that decision. The joint Army-Navy ECM Cipher became effective
in July 1941, and the two services had a common high-security cipher system in effect and in use prior to the attack on Pearl Harbor. This use by the two services of an identical machine with interchangeable code wheels has been of great military value, particularly in the early stages of the war when the distribution of machines and code wheels was incomplete. In the Philippines, Java, Australia, and even in North Africa, Navy wheels have been used in Army ECMs, Army wheels in Navy ECMs, machines borrowed back and forth between the two services, Army messages sent in Navy ECM ciphers and Navy messages sent in Army ECM ciphers. One other contribution from the Signal Corps came in 1943, after the ECM was in service; namely, the "Plugboard Code Wheel." This was developed by the Army for field use, where the danger of capture was greater than in the Navy. The "Plugboard Code Wheel" was adopted for joint Army-Navy use, at the request of the Army, and later distributed to all Navy holders of the ECM. The chief value of the "Plugboard Code Wheel" is possibly psychological, but we do have it in case of need.
The Contribution of the Signal Corps

23. Mr. William F. Friedman, Principal Cryptanalyst of the Signal Intelligence Service, and interested officers at Signal Corps Headquarters were familiar with the various models of the HCM, but not with the prospective changes which the Navy had concealed from Hebern. In fact, on Mr. Friedman's recommendation, the Signal Corps purchased two of Hebern's early 5-wheel nonprinting models late in 1923. At the request of the Navy Department, Friedman undertook a cryptanalytic test of the HCM in the spring of 1924, being furnished a set of 10 test cryptograms prepared by the Code and Signal Section. Friedman was successful, and developed cryptanalytic techniques whereby, under certain conditions of meter action, solution could be achieved even without possession of the code wheels. Again, at the request of the Navy Department, in April 1932 Friedman undertook a second test on the much improved 1930 model of the HCM. This time he was furnished the machine, a description of the general system employed in setting up the message indicators, and a series of test messages. Again he was successful, with the aid of three or four of his assistants. As the test messages were enciphered with Hebern's stepping action and not with the irregular code-wheel stepping produced by the HCM adapter (CSP 555), the solution did not worry us particularly. These solutions were very important, in three ways, namely:

I. They showed the weakness of the meter action of the 1923 HCM and of 6 of the 30 optional stepping actions of the 1930 HCM.

II. The 1924 solution was the basis of further analysis by the Navy which disclosed stepping actions that would block analytical solutions or short-cut solutions based on possession of the code wheels. Friedman arrived at similar conclusions, independently. Otherwise, we would have had to abandon the Electric Cipher Machine as being deficient in inherent security.

III. In recent years, the principles and techniques of these solutions were instrumental in the solution of certain systems which are still using a meter action.

24. The first solution (that of 1924) was written up by Friedman in secret, typewritten; technical paper completed early in 1924; which was not printed, however, until 1934, under the title "Analysis of a Mechanico-Electrical Cryptograph—Part I." The second solution (that of 1932) was also written up by him in a second secret paper completed in 1933 but not printed until 1935, under the title "Analysis of a Mechanico-Electrical Cryptograph—Part II." Both papers were very carefully safeguarded at all times and were employed only in the SIS for the advanced training
of a very limited number of students. The documents were given no dissemination except that the Navy Department was furnished copies. But, because it was not consulted with regard to the advisability of printing these papers, combined with a serious mistrust of the Government Printing Office, the Navy Department entertained some apprehensions as to security and this led to an order from the D.N.C. that the Signal Corps was not to be shown the Mark I ECM or to learn any of its details. This order, which was not revoked until January 1940, was responsible for later misunderstandings. Certain Signal Corps representatives, including Friedman and Mr. Frank B. Rowlett, had been shown the pilot model of the Mark I ECM sometime in the winter of 1934–35, before the order was issued, so they were not entirely ignorant of what the Navy was doing along these lines.

25. From 1924 to 1932 the Signal Corps appeared more interested in the Teletype Scrambler than in the ECM as a practical cipher machine which would meet Army requirements. However, under date of 25 July 1935, the Chief Signal Officer filed on behalf of Friedman a patent application (Serial No. 862,096) covering a cryptographic system and machine in which the stepping of the code wheels was very irregular and under the control of a keying tape. Electric control thus made its first appearance! Friedman made a complete assignment of his invention to the War Department and one or two preliminary models were built in 1935–36. These were successful and an order was placed with a relatively small and inadequately equipped manufacturer for a few machines, which were designated as Converter M-134A. It took a comparatively long time to build these few machines but by 1938 some of them were delivered and placed in service for communication between the War Department and the Commanding Generals of Overseas Departments. Later, additional ones were delivered and placed in service for communication among the War Department and Corps Areas and between the War Department and the U.S. Military Attaché in London. The first model of this machine was shown to me by the Signal Corps sometime in 1937. This machine indicated the reliability of electric control but the undesirability of the particular method (perforated tape) used in the Signal Corps machine.

26. Shortly before 15 June 1938, during the interval when preliminary models of the foregoing machine were being built, Mr. Frank B. Rowlett, principal assistant to Friedman, conceived the idea which constitutes the basis of the "stepping maze" in the present ECM. His concept was based upon the principle of sending an electrical impulse through the circuits of a code-wheel maze to generate a long, irregular sequence of events which could then be used for various purposes, such as keying. Rowlett and Friedman then jointly developed Rowlett's novel idea of a key generator as applicable to the Signal Corps machine and reduced it to more practical form in drawings. No model incorporating their ideas was built by the Signal Corps, however, because the Chief Signal Officer was committed to the type embodied in the Converter M-134A,
pre-production models of which were then under manufacture, and he was reluctant to make any change in design, despite Friedman's urgent recommendations that this be done. The inventors proceeded to incorporate the results of their theoretical studies and their drawings, reducing the new principles to practice in a patent application filed in the Patent Office on 23 March 1936 by the Chief Signal Officer on their behalf as joint-inventors (Serial No. 70,412). The inventors made a complete assignment of their invention to the Secretary of War on 2 April 1936 and the application was processed through the Patent Office, though, of course, it is held in the secret status. Nearly all of the claims (39) have been allowed in the case.

27. In October 1935, Friedman and Lieutenant Wenger (of the Code and Signal Section) held a general discussion on cipher machines. Wenger expressed considerable dissatisfaction with the Mark I ECG and asked Friedman whether the Signal Corps had any "good" ideas along these lines. Friedman indicated that there were several ideas which the Signal Corps was not exploiting but which he was not at liberty to disclose, since they had been placed in the secret category. Friedman further indicated that if Wenger so desired, permission to disclose them to the Navy would be requested. Wenger asked that this be done. Accordingly, Friedman requested and was granted permission by his superiors to disclose the details of the Friedman-Rowlett patent application to representatives of the Navy Department. Therefore, on 21 October 1935, at a conference in Friedman's office, the details were disclosed to Commander McClaran and Lieutenant Wenger, who were shown the drawings that form the basis of the patent application Serial No. 70,412. On 31 October 1935, a second and similar disclosure was made to Commander McClaran, Lieutenant Wenger, and Lieutenant Harper. A third disclosure was made on 1 November 1935 to Lieutenants Wood and Duwan, also of the Code and Signal Section. Friedman and Rowlett were told very little as to the Navy Department's reaction to the disclosures; in fact, they were told that the principles disclosed were of no interest to the Navy at that time—which was the truth of the matter.

28. My first-hand knowledge of the Friedman-Rowlett invention began in the winter of 1936-37 when we were preparing initial specifications for the Mark II ECG. Wenger stated that Friedman had an idea for an electric control which had very interesting possibilities and produced from his safe a single sheet of cross-section paper containing three elementary wiring-diagrams by means of which electric control of an ECM could be achieved through an ECM maze. This paper was dated and signed (as I remember) by Harper, Wenger, and Wood, and by Friedman and Rowlett. (We have been unable to locate this paper since 1940.) I immediately realized that electric control gave us the answer to many of our unsolved problems and therefore had to be incorporated in the new machine. I was under orders not to discuss or show either the Mark I ECG or the Mark II ECG to the Signal Corps and, therefore,
adopted electric control and further developed the basic idea without the knowledge of the original inventors. In January 1940 the Mark II ECM was offered to the War Department for Joint Army-Navy use and also for purely Army use. It was explained that the mechanical features were well developed and "frozen" in design, and that we believed the Army would be well satisfied with the cryptographic principles involved, but that we were willing to discuss any security features in order to get a machine that would be satisfactory to both services. We wanted the Army to join us on the first order for the machine in order to further the idea of using identical cryptographic systems in the two services, as had already been done with the Strip Cipher Device. Another reason was to share the overhead for tooling-up and thereby give us a better price. It had been previously suggested that the Army and Navy get together on the Signal Corps machine or the Mark I ECM. We advised that neither machine was acceptable because of mechanical deficiencies but that we were developing a new machine and as soon as we had a working model we would endeavor to get permission to make it available as a common Army-Navy machine.

29. On 3 February 1940, Admiral Noyes (D.N.C.) invited General Mausborgne (Chief Signal Officer), Captain Cook, Mr. Friedman, and other Signal Corps representatives to inspect a pilot model of the Mark II ECM. On that occasion I acknowledged to Mr. Friedman, in the presence of General Mausborgne and Admiral Noyes, our use of his invention. Later there was a special conference attended by Mr. Reiber and Mr. Zennor of the Teletype Corporation, Mr. Friedman of the Signal Corps, Commander Safford and Lieutenant Zern of Naval Communications, and possibly others. The blue prints were carefully examined and a general discussion of cryptographic features followed. Friedman pointed out that the underlying principles of the control circuits of the Mark II ECM were those which had been disclosed by Rowlett and himself to the Navy Department in 1935, and this was confirmed by me. The four experimental changes to the Friedman-Rowlett circuit which had been made by Seiler and myself were discussed and the following decisions made:

I. "Index Maze," which replaced the plugboard in the Friedman-Rowlett invention - Retained. The "Index Maze" accomplished the same cryptographic result as the plugboard but was much more convenient to the operator.

II. Grouping of end contacts in the "Stepping Maze" and in the "Index Maze," which replaced the arrangements of the Friedman-Rowlett circuit - Retained. These groupings together with the ten circuits through the "Index Maze" gave 49 times as many stepping combinations as was possible with the Friedman-Rowlett invention (5,855 against 120).
III. Subdivision of "Stepping Maze" into two parts -

Unanimous decision to return to the original
Friedman-Rowlett "Stepping Maze." Friedman pro-
tested the subdivision as an unnecessary compli-
cation. Reiber and Zemmer did not like from the
viewpoint of design and construction.

IV. Stepping order for the "Stepping Maze" proposed by

the Navy was 3-1-5, the other two wheels being dead
to simplify construction. The stepping order was changed
to 3-4-2 upon Friedman's recommendation.

With these exceptions the Mark II ECM, as developed by the Navy
and Teletype using the Friedman-Rowlett "Stepping Maze," was
satisfactory to and accepted by the Army. Washington Navy Yard
sketch RV68F201, dated 24 April 1940, used as a basis for speci-
fications of the production model, is the earliest-dated drawing
showing the "Stepping Maze" and associated circuits exactly in
their present form.

30. One other contribution, Major Leo Rosen's "Plugboard Code
Wheel," came in 1943 after the ECM was in service. This was de-
veloped by the Signal Corps for field use, where the danger of
capture was greater than in the Navy. The "Plugboard Code Wheel"
was adopted for joint Army-Navy use at the request of the Army,
but is being distributed to all Navy holders of the ECM. The
chief value of the "Plugboard Code Wheel" to the Navy is possi-
ably psychological, but we do have it in case of need.

31. Electric control of the ECM by means of the Friedman-Rowlett
"Stepping Maze" is the essential feature that places the Mark II
ECM in a class by itself as regards security. Those who have
participated in the development of the Mark II ECM have always
acknowledged the contributions of the Signal Corps. The "Index
Maze" and grouping of end contacts add to the security afforded
by the "Stepping Maze," but would be worthless without it. The
importance of electric control can best be estimated by a con-
sideration of what the Mark II ECM would have been if Friedman
and Rowlett had not been permitted to disclose their invention
to the Navy. Although the "Stepping Maze" appears obvious, now
that it is in use, no one in the Navy thought of it in a period
of 15 years, and no foreign machine employs it. Therefore, the
Navy would have continued the development of the older methods and
the new ECM would have used the mechanical stepping control found
in CSP 903 or CSP 1700. We would have had a secure machine, superi-
or to anything in use by foreign nations, but definitely inferior
to our present ECM. This hypothetical machine (as well as CSP 1700)
would defy attempts at solution until such time as machine and code
wheels were captured. After this, each day's keys would resist
solution for a long time. "Short-cut" solutions would be impos-
sible, due to the erratic stepping of the code wheels, but a
trial-and-error solution would be within the range of possibility.
We could not make the flat statement, as we do for the Mark II ECM, that solution would be utterly impossible. In other words, the machine would be adequate to take us through World War II, but, because we had stopped short of the ultimate step, there would always be the desire to develop a new machine and scrap the old one. Rowlett is entitled to full credit for his discovery of the principle of the key generator as embodied in the "Stepping Maze," which adds so much to the excellence of the Mark II ECM, and Friedman and Rowlett jointly are entitled to full credit for their joint invention of methods of applying and reducing the principle to practical form.

32. The Signal Corps' acceptance of the Mark II ECM for Army as well as Joint Army-Navy use reflects credit on all who made that decision. The Joint Army-Navy ECM Cipher System became effective on 1 August 1941, and the two services had a common high-security cipher system in effect and in use prior to the attack on Pearl Harbor. This use of an identical machine with interchangeable code wheels has been of great military value, particularly in the early stages of the war when the distribution of machines and code wheels was incomplete. In the Philippines, Java, Australia, and even in North Africa, Navy wheels have been used in Army ECMs, Army wheels in Navy ECMs; machines have been borrowed back and forth between the two services; Army messages have been sent in Navy ECM ciphers and the Navy messages sent in Army ECM ciphers.
Informal Memorandum

The two primary faults of the cryptographic machine under discussion, and faults which alone permitted the solution described, are, as described:

1. Non-pluggable cipher maze output endplate.
2. Provision for cipher rotors to move singly on occasions.

In section XIX, recommendations, P. 190, paragraph 48 (b) 1, a pluggable endplate is recommended. This takes care of "fault #1."

But paragraph 48 (b) 2 does not recommend, as we believe it should, a change in the cipher maze stepping provisions. It suggests instead that the stepping of the stepping rotors be changed by insertion of an additional fast moving wheel there, which is a good idea and certainly should be adopted. The cipher maze stepping rotors however should never be allowed to move singly, or they will "give themselves away" as this paper so aptly demonstrates.

Experience in B-III-Research tells us that in a Hebern-type of machine (which the SIGABA is except for motion) that there should always be THREE NON-ADJACENT WHEELS MOVING AT ALL TIMES. In an Engima type of machine, there should always be TWO NON-ADJACENT WHEELS MOVING AT ALL TIMES. We believe a recommendation should be made to the effect that two more fast moving wheels be provided for the cipher maze in addition to the one which might be moving at any one time, or else that one more fast moving
be provided the cipher maze and the cipher maze converted to Enigma type.

It has long been the contention of B-III-Research that wheels in cryptographs of Enigma type should never move singly, nor in Heber types ever in less than threes, and that endplates should be protected by plugging. We therefore read the attached paper with greatest interest.

March 28, 1944
SUBJECT: Blank forms for code accounting. MAY 16 1935

TO:

1. Par. 11, AR 105-25, dated September 1, 1934, requires that certain reports be accomplished whenever any registered War Department cryptographic publication is transferred from one holder to another, and that a semiannual report of possession be made on all such items. For purposes of facilitating the making of these reports a standard form has been established, designated as WDSC Form No. 84, "Semiannual or Transfer Report of Registered Secret and Confidential War Department Publications and Devices."

2. Attention is invited to the fact that the above-mentioned form (Stock No. 6D84) is now stocked at the Signal Section, New York General Depot, and issued on approved requisitions in the same way that other authorized Signal Corps forms are issued.

For the Acting Chief Signal Officer:

Geo. P. Bush
Geo. P. Bush,
Major, Signal Corps.
REF ID: A4126886

June 26, 1945

MEMORANDUM FOR: Research and Development Division

(ATTN: War Plans & Training Division)

1. In connection with the tabulating machinery now employed by the Signal Intelligence Section, the undersigned have invented a new and useful device which may be attached to the electrical counting sorter and which will be of importance in future employment of this machine in code compilation and in other work not related thereto, of a purely commercial character.

2. The principal object of the invention is to transform the electrical sorter into a device of exactly opposite function, viz., to "uncard", "uncramble", or disarrange in a wholly random sequence a set of punched cards originally arranged in a definite or regular sequence. Another object is to provide a means and device for obtaining a wholly random, small sample from a large set of punched cards.

3. In view of the fact that such a device will be very useful in code production, it is desirable that patent application be made in order to protect the government's interests.

4. At the same time, in view of the usefulness of the device for certain commercial tabulating installations in which random selections of punched cards must occasionally be made, permission is requested to enter into negotiations with the International Business Machines Corporation or other companies, with a view to possible sale of commercial rights to this invention.

5. Attached hereto is a sketch and description of the invention, in the form of a preliminary draft of specifications.

William F. Friedman

Frank B. Russell

Attached:
Sketch
Description.
War Department, OCS1-30, Washington, August 24, 1935. To: Maj. F. E. Friedman and Mr. F. P. Bredlow, War Plans and Training Division.

1. In compliance with request made in paragraph 4, of your memorandum, dated June 26, 1935, relative to an invention covering an attachment to an electrical counting sorter, there is no objection to your entering into negotiations with any industrial organization with a view to possible sale of commercial rights to your invention, described in the memorandum herein referred to.

By Order of the Chief Signal Officer,

[Signature]

[Name]
Colonel, Signal Corps, Executive.
1. This is to record certain facts in connection with the invention of several alternative means of providing an aperiodic displacement of the substitution cipher wheels of a cipher machine as granted in claim 17 of the patent specifications having reference to Converter Type M-134-T2.

2. It is desired to record here that the fundamental principle of using one or more commutators in conjunction with a set of selector magnets as a means for effecting the aperiodic displacements discussed in par. 1 is the contribution of Frank B. Rowlett.

3. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of commutators containing contacts equal in number to the number of substitution cipher wheels to be displaced, is the contribution of Frank B. Rowlett.

4. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of cipher wheels, hereinafter called the control cipher wheels, and having the latter cipher wheels identical in number of contacts and construction with the former so that all cipher wheels are interchangeable, is the contribution of William F. Friedman.

5. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of a second set of control contacts on each face of each of the substitution cipher wheels themselves, and providing appropriate electrical circuits for the control contacts to govern the operation of the displacement mechanism, is the contribution of Frank B. Rowlett.

6. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of the same set of substitution contacts operating in connection with a gang switch which makes these contacts serve for substitution and control in alternate sequence, is the contribution of Frank B. Rowlett.
7. The application of the principle of aperiodic displacement of substitution-cipher wheels to cryptographs of the original Enigma type (in which the electrical circuit through the cipher wheels is reversed by means of a reversing cipher wheel and again conducted through the other cipher wheels before reaching the signaling element) is the contribution of William F. Friedman.

8. The foregoing facts will be used as a basis for evaluation and division of interest in all financial benefits which may accrue from the prosecution of the invention and its reduction to practice.

Witnesses:

Chas. D. Dowre

William F. Friedman

Frank B. Bowlett

L. Wilson
MEMORANDUM FOR: Research and Development Division (M.I.B. W.P. & T. Div.)

July 6, 1935

1. In accordance with provisions of Part IV; AR 850-50, there is attached a draft of specifications upon which application for patent on Cipher Device Type M-138 may be based.

2. It is understood that the Navy Department has pending an application for patent on their first type of cipher device, and are filing an application covering their second type. They are apparently satisfied to standardize, for the Naval Service, our Type M-138, and are planning to purchase 100 or 200 devices identical with ours, except as to name plate.

3. It is recommended that the attached draft be forwarded to the Signal Corps Patents Section for use in the preparation of detailed specifications and drawings. In view of the existence of similarities between our Type M-138 and the Navy types, it is probable that patent of only limited scope can be obtained. Nevertheless, the improvements devised by me, consisting in the use of metal channel ways, a slideable guide rule, and a construction which permits of setting up the text alternately at the left side and right side of the assembly, make our type of device a very much more practical instrument than any of those heretofore devised.

4. Since these improvements arose from my own studies, it is requested that application be made in my name as inventor.

William F. Friedach,
Signal Intelligence Section.

COPY FOR: Mr. Friedman.
CONFIDENTIAL

ROUTING and WORK SHEET

(To be used under provisions of Par. 41.6 b, Office Regulations, OCSNo. 1934)

From: WP+T

To: R+D.

Forwarded:

From R+D to WP+T

Request following information:

1. Has Mr. Friedman been designated or employed for the purpose of making this invention?

2. Is the invention important to National Defense?

WP+T to R+D:

1. Mr. Friedman was not designated or employed for the purpose of making this invention.

2. The improvements are not considered to be of such character as to warrant being classified as "important to national defense."
<table>
<thead>
<tr>
<th>TO</th>
<th>FROM</th>
<th>TO</th>
<th>FROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHIEF, ASA</td>
<td>(10)</td>
<td>Tech Staff</td>
<td>(96)</td>
</tr>
<tr>
<td>Spec Asst to the Ch</td>
<td>(14)</td>
<td>Spec Proc Br</td>
<td>(97)</td>
</tr>
<tr>
<td>Ch, Hist Unit</td>
<td>(13)</td>
<td>CH, SECURITY DIV</td>
<td>(80)</td>
</tr>
<tr>
<td>Asst to the Chief</td>
<td>(11)</td>
<td>Tech Staff</td>
<td>(81)</td>
</tr>
<tr>
<td>Joint Secretariat</td>
<td>(12)</td>
<td>Ch, Materiel Br</td>
<td>(82)</td>
</tr>
<tr>
<td>DEPUTY CHIEF, ASA</td>
<td>(20)</td>
<td>Ch, Methods Br</td>
<td>(83)</td>
</tr>
<tr>
<td>Asst Deputy Chief</td>
<td>(20)</td>
<td>Ch, Protective Br</td>
<td>(84)</td>
</tr>
<tr>
<td>Executive</td>
<td>(20)</td>
<td>Ch, Maint Br</td>
<td>(85)</td>
</tr>
<tr>
<td>Secretariat</td>
<td>(20)</td>
<td>CH, RES &amp; DEV DIV</td>
<td>(70)</td>
</tr>
<tr>
<td>Ch, Pres Sec</td>
<td>(21)</td>
<td>Tech Staff</td>
<td>(71)</td>
</tr>
<tr>
<td>Ch, Org &amp; Tng Sec</td>
<td>(22)</td>
<td>Ch, C &amp; C Br</td>
<td>(72)</td>
</tr>
<tr>
<td>Ch, Plans &amp; Oper Sec</td>
<td>(23)</td>
<td>Ch, Equip Br</td>
<td>(73)</td>
</tr>
<tr>
<td>Ch, Logistics Sec</td>
<td>(24)</td>
<td>Ch, Electromech Br</td>
<td>(74)</td>
</tr>
<tr>
<td>Ch, Fiscal Sec</td>
<td>(25)</td>
<td>Ch, Lab Serv Br</td>
<td>(75)</td>
</tr>
<tr>
<td>Adjutant General</td>
<td>(26)</td>
<td>Ch, Cryptologic Br</td>
<td>(76)</td>
</tr>
<tr>
<td>Ch, Sec Cont Sec</td>
<td>(27)</td>
<td>Ch, Electronics Br</td>
<td>(77)</td>
</tr>
<tr>
<td>CH, OPERATIONS DIV</td>
<td>(90)</td>
<td>Ch, Pers &amp; Tng Br</td>
<td>(61)</td>
</tr>
<tr>
<td>Directives Br</td>
<td>(90x)</td>
<td>Ch, Supply Br</td>
<td>(62)</td>
</tr>
<tr>
<td>Ch, Lab Br</td>
<td>(91)</td>
<td>SIGRP-5</td>
<td>(62)</td>
</tr>
<tr>
<td>Ch, Machine Br</td>
<td>(92)</td>
<td>CO, Arlington Hall Sta</td>
<td>(40)</td>
</tr>
<tr>
<td>Ch, Gen Processing Br</td>
<td>(93)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ch, Facilities Br</td>
<td>(94)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ch, I &amp; D Br</td>
<td>(95)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

( ) Approval & Return
( ) As Requested
( ) Concurrence or Comment
( ) Information & Forwarding
( ) Information & Return

Copy for your file & one for the person writing up history of sign off.

Copy forwarded to:

AS - 80 8/0 Aug 49

CSGAS 96 (Rev. 14) 15 Apr 49 8-411
1. In connection with a memorandum dated August 31, 1935, (copy attached) setting forth "certain facts in connection with the invention of several alternative means of providing an aperiodic displacement of the substitution cipher wheels of a cipher machine as granted in claim 17 of the patent specifications having reference to Converter Type M-134-T2," the following additional facts are made of record:

2. The principle of employing a set of juxtaposed rotating commutators as a means of selecting in an irregular, aperiodic manner, the successive alphabets (for encipherment or decipherment) from among a plurality of cipher alphabets is the contribution of Frank B. Rowlett.

3. The associated principle of controlling the stopping positions of a single substitution cipher wheel by a set of juxtaposed control cipher wheels is the contribution of William F. Friedman. Note: Thus, for example, in Friedman and Graham U. S. Patent No. 2,028,772 the cipher key transmitter and its associated mechanism would be replaced by a set of control cipher wheels, the 26 final contacts of which would be connected to pins which would stop the substitution commutator in the enciphering (or deciphering) position.

4. The idea as to the possibility of directly applying the foregoing principles to the stopping of a rotating printing wheel at cipher positions, the latter being superimposed upon the stopping position determined by the key depressed on the keyboard, is the equal and joint contribution of both William F. Friedman and Frank B. Rowlett. In this case, in order to prevent cumulative errors it is necessary to return the printing wheel to an initial position after each operation. The cipher stopping position of the printing wheel is determined after it has been stopped by the depression of a key of the keyboard.

/s/ WILLIAM F. FRIEDMAN

Witnesses: /s/ FRANK B. ROWLETT
/s/ Louise N. Nelson
/s/ Chas. A. Rowe
August 31, 1935

1. This is to record certain facts in connection with the invention of several alternative means of providing an aperiodic displacement of the substitution cipher wheels of a cipher machine as granted in claim 17 of the patent specifications having reference to Converter Type M-134-T2. Application Serial No. 682,097

2. It is desired to record here that the fundamental principles of using one or more commutators in conjunction with a set of selector magnets as a means for effecting the aperiodic displacements discussed in par. 1 is the contribution of Frank B. Rowlett.

3. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of commutators containing contacts equal in number to the number of substitution cipher wheels to be displaced, is the contribution of Frank B. Rowlett.

4. The subsidiary principle (subsidiary to that set forth in par. 2) of producing aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of an independent set of cipher wheels, hereinafter called the control cipher wheels, and having the latter cipher wheels identical in number of contacts and construction with the former so that all cipher wheels are interchangeable, is the contribution of William F. Friedman.

5. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of a second set of control contacts on each face of each of the substitution cipher wheels themselves, and providing appropriate electrical circuits for the control contacts to govern the operation of the displacement mechanism, is the contribution of Frank B. Rowlett.

6. The subsidiary principle (subsidiary to that set forth in par. 2) of producing the aperiodic displacements (discussed in par. 1) of the substitution cipher wheels by means of the same set of substitution contacts operating in connection with a gang switch which makes these contacts serve for substitution and control in alternate sequence, is the contribution of Frank B. Rowlett.
7. The application of the principle of aperiodic displacement of substitution cipher wheels to cryptographs of the original Enigma type (in which the electrical circuit through the cipher wheels is reversed by means of a reversing cipher wheel and again conducted through the other cipher wheels before reaching the signaling element) is the contribution of William F. Friedman.

8. The foregoing facts will be used as a basis for evaluation and division of interest in all financial benefits which may accrue from the prosecution of the invention and its reduction to practice.

/s/ WILLIAM F. FRIEDMAN

/s/ FRANK B. ROWLETT

Witnesses:

/s/ Louise N. Nelson
MEMORANDUM FOR ASSISTANT CHIEF OF STAFF, G-2

SUBJECT: Release of Cryptological Inventions and Developments

DISCUSSION

1. In the years preceding the outbreak of the present war and during the war itself, numerous cryptological inventions were made by military and civilian personnel. Applications for patent were filed on some but not on all of such inventions. In either case, information regarding such inventions has for the most part been denied the public. Since the most recent War Department policy is to release as much technical information as possible, it is necessary to reexamine inventions in the cryptologic field.

2. The inventions concerned fall into five categories. Army Regulation 850-50, paragraphs 7 and 9, (Tab A), refers to three of these categories and indicates the nature of the Government's rights. Additionally, there are inventions made by persons or companies under contract to the Government and in these cases normally the Government's rights depend upon the terms of the contract but usually amount to a royalty-free license to practice any inventions made, with ownership of the inventions remaining in the contractor. The last category involves the independent agent, one who, working entirely on his own, produces an invention of merit. In
such a case, the Government has no rights except through purchase or the taking of a license.

3. Further discussion in this memorandum will be limited to the second category of Army Regulation 850-50 wherein the Government takes a nonexclusive royalty-free license and the inventor has a theoretical right to exploit commercially for his own benefit. Where cryptologic inventions are involved, classification of the equipment and security restrictions placed upon information pertaining thereto have been used to prevent commercial promotion. Cash awards to civilian inventors in Government service are in some circumstances possible, but the Army Security Agency has held that where the invention is within the purview of the employment an award is improper. Virtually the only other possibility of compensation to an inventor is by Congressional action.

4. With the cessation of hostilities, cryptologic inventions and development by independent inventors and by contractors may in the past have produced very little but be expected to fall off to nearly nothing, and reliance, therefore, must have to be placed on Government employees. It is believed that some incentive must be furnished if research is to continue to be highly productive; the possibility of cryptologic inventions that can be released be sufficient.

5. The latest War Department policy bearing on the matter appears in a memorandum, subject: Classification,
Reclassification, and Declassification of Scientific and Technical Information, for the Assistant Chief of Staff, G-2, Director, New Developments Division, Director, Bureau of Public Relations, Commanding Generals of the Army Air Force, Army Ground Force and Army Service Force (Tab B), which states in paragraph 3 that "as liberal a policy with respect to review and declassification of classified projects and material as is consistent with continuing only those items of information, the publication of which would cause exceptionally grave danger to the nation or endanger the national security or cause serious injury to the interest or prestige of the nation or any Governmental activity thereof or which would be of great advantage to a foreign nation or cause administrative embarrassment, etc., will be retained in a security classification." According to General Borden, New Developments Division, the policy of the said memorandum is such that very good reasons must be presented in order to prevent the release of information. Further of interest in this regard is the policy of the United States Patent Office with respect to applications on file, which policy is indicated in a letter from Colonel Donald K. Lippincott, Patents and Inventions Counsel, Legal Division, Office of the Chief Signal Officer, to Intelligence Branch (Tab C). Patent Office policy is based upon a memorandum from the Joint Chiefs of Staff (Tab D).
6. Since fundamental cryptographic systems are well known, the greatest danger involved in the release of information in the form of patents or otherwise appears to be that of acquainting foreign powers or unfriendly forces with effective adaptations and arrangements of these systems. Patent applications need not and rarely do contain key generating means, rotor wiring, and other specific features upon which the security of cryptographic text really depends. The main difficulty is that, by disclosing basic features of successful machines used by this country, the development of other adaptations is made possible, and our own cryptanalysts will be faced with text very difficult to decipher. On the other hand, many American machines already are known in principle to thousands of persons who either maintained or operated the same, and it is most unlikely that the principles can be now successfully suppressed. Added to this is the probability that independent inventors, and particularly contractors who have acquired techniques and know-how in the performance of war contracts, will produce machines similar to those at present in use. Such machines would not be classified nor is there any means of restraining their promotion.

7. It is the well-established policy and practice of the War Department to declassify material when the information can no longer be considered as secret, confidential, or
restricted. To maintain classification on information
the control of dissemination of which is ineffectual only
results in the degradation of the classification system
itself.

8. To declassify any specific item does not establish
a general policy applicable to other items in the same
general category. If this were not true the declassification
of any item, whether it be a document or a piece of equipment,
would be impossible, except in the rare case in which the
entire category consisted of but a single item. Hence, to
declare that declassifying a specific item of cryptographic
equipment would lead to the declassification of all other
classified items of cryptographic equipment is not warranted
in declassification each item must be considered individually
by considerations of policy or practicability in its own merits.

9. It should be stressed that the declassification of
a patent application and thus the issue of a patent covering
certain principles or features of a cryptographic apparatus
does not usually have as a consequence the declassification
of a machine as a whole or the traffic handled by it since,
as indicated in paragraph 6, the working apparatus will
depend for its security upon specific wiring and so forth
not disclosed in the patent.

RECOMMENDATIONS

10. That no exception from the announced War Department
policy of liberality with respect to the release of technical
information be made in the case of cryptologic inventions.
11. That the Chief, Army Security Agency, determine specifically which cryptologic patent applications or developments may be released.
MEMORANDUM FOR THE CHIEF, ARMY SECURITY AGENCY:

SUBJECT: Release of Cryptographic Principles.

1. The following policy is announced to be effective immediately:

   a. Cryptographic principles or devices developed by officers, enlisted men, or civilians employed in any War Department Agency, or patents or patent applications on such principles or devices which are owned by, assigned to, or licensed for use of the War Department will not be released for use of foreign governments or for foreign or domestic commercial or private use until such time as necessary information is available and a procedure established in the Army Security Agency whereby information which is cryptographed by means of such principles or devices can be cryptanalyzed and read under any and all circumstances.

   b. Where it is in the interest of the Government of the United States that an employee have no patent rights in cryptographic principles or devices to dispose of, and for the Government to own the entire interest for security reasons throughout any foreseeable future, and where discovery or invention of cryptographic principles or devices has been made by a civilian employee and does not relate to a matter as to which the employee was specifically directed to experiment with a view to suggesting improvements nor was produced as a result of any specific employment or contract to invent a specific device or article, and where an application for patent on such principles or devices has been filed with an assignment-in-trust to the Government for the purpose of maintaining such application in secrecy, the Military Intelligence Division will support, subject to the availability of appropriations, any reasonable request for purchase of all commercially exploitable reversionary rights of the inventor in the patent application.

CARTER W. CLARKE
Colonel, GSC
Acting Deputy, A.C. of S., G-2
SUBJECT: Release of Patent Application Serial No. 443,320

TO: Commanding General
Army Security Agency

1. The subject patent application covers a cryptographic means and device for automatic encipherment and decipherment of teletypewriter signals and was filed in the U. S. Patent Office on 16 May 1942 in the name of the undersigned and Frank B. Rowlett, as co-inventors.

2. The principles involved in the subject application have been utilized in Converter M-228 and Converter M-294.

3. It is requested that the subject application be officially declassified in order that it may be allowed to go to issue, whereupon the right and title will revert to the undersigned and Frank B. Rowlett, subject to an irrevocable, non-exclusive, and royalty-free right and license remaining vested in the United States of America.

4. This action is desired because of the commercial applications of the invention, interest in which is believed to exist on the part of the U. S. communication companies.

5. Declassification of the patent application does not necessarily involve the declassification of the specific embodiments thereof represented in the apparatuses mentioned in paragraph 2.

WILLIAM F. FRIEDMAN
1. All previous instructions pertaining to the above subject are rescinded.

2. Research Laboratories Division is charged with the primary responsibility for making recommendations related to the control and evaluation of all patents and patent applications affecting cryptologic equipment and processes. In view of the above, the following procedure will be adopted for the handling of requests relating to the release of patents held in secrecy:

   a. If the request is received by Research Laboratories Division, comments and recommendation will be forwarded by AS-70 to AS-20 after coordination with AS-80 and AS-90.

   b. If the request is received by the Deputy Chief, it will be forwarded to AS-70 who will coordinate with AS-80 and AS-90 and return comments and recommendation to AS-20.

3. Comments should include sufficient background material to determine that recommendation is in accord with current policy on release of cryptographic principles, a copy of which is attached. The last sentence of paragraph 1a of attached policy will be interpreted on the basis that the Army Security Agency could expect to solve communications which may be passed therein, assuming the device were to be used in a practical manner by adequately trained personnel and resulting in a normal military or commercial traffic expectancy.

1 Inc1
Memo for Ch, ASA fr ACoFS, G-2 dtd 29 Apr 46 subj: Release of Cryptographic Principles

/s/ Harold G. Hayes
Harold G. Hayes
Colonel, Signal Corps
Chief, ASA

CYS FURNISHED
AS-14
23
24
SUBJECT: Release of Patent Application Serial No. 443,320

TO: Mr. William F. Friedman, WDGSS-14

1. Reference your letter dated 27 September 1945, subject as above, the attached memorandum from the Acting Deputy Assistant Chief of Staff, G-2, outlines the War Department policy on the release of cryptographic principles.

2. Analysis of the policy would indicate that:

   a. Patent application No. 443,320 will not be released unless it can be shown that the employment of the principles involved are susceptible to cryptanalysis under all circumstances; and

   b. If not released, a request for purchase of all commercially exploitable reversionary rights may be entertained provided it can be shown that Frank B. Rowlett and yourself were not directed or employed to experiment on or to invent the principles or improvements embodied in Converter M-228 or Converter M-294.

3. If it is felt that subject Patent Application should be released under (a) above; or if and when it is felt a case should be presented for purchase of rights in conformity with stipulations contained in (b) above, an application for release or purchase, containing pertinent facts and necessary proofs, may be prepared and submitted to the Director of Intelligence through the Chief, Army Security Agency.

1 Incl
Cy ltr dtd 29 Apr 46
subj: "Release of Cryptographic Principles

/s/HAROLD G. HAYES
Colonel, Signal Corps
Chief, Army Security Agency

SECRET
29 April 1946

MEMORANDUM FOR THE CHIEF, ARMY SECURITY AGENCY:

SUBJECT: Release of Cryptographic Principles.

1. The following policy is announced to be effective immediately:

   a. Cryptographic principles or devices developed by officers, enlisted men, or civilians employed in any War Department Agency, or patents or patent applications on such principles or devices which are owned by, assigned to, or licensed for use of the War Department will not be released for use of foreign governments or for foreign or domestic commercial or private use until such time as necessary information is available and a procedure established in the Army Security Agency whereby information which is cryptographed by means of such principles or devices can be cryptanalyzed and read under any and all circumstances.

   b. Where it is in the interest of the Government of the United States that an employee have no patent rights in cryptographic principles or devices to dispose of, and for the Government to own the entire interest for security reasons throughout any foreseeable future; and where discovery or invention of cryptographic principles or devices has been made by a civilian employee and does not relate to a matter as to which the employee was specifically directed to experiment with a view to suggesting improvements nor was produced as a result of any specific employment or contract to invent a specific device or article; and where an application for patent on such principles or devices has been filed with an assignment-in-trust to the Government for the purpose of maintaining such application in secrecy, the Military Intelligence Division will support, subject to the availability of appropriations, any reasonable request for purchase of all commercially exploitable reversionary rights of the inventor in the patent application.

   /s/ CARTER W. CLARKE
   Colonel, GSC
   Acting Deputy, A.C. of S., G-2
These are my original work sheets of Hebern Solution

W.F.A.
REF 126886

1936

FRIDAY, NOV.

27

332 34
Pre look this over at your earliest convenience + then call me. I think this is a good way to go at the problem.

You might suggest rearrangement of the order of the enclosures - I am not sure it's the best as I have it now.
1st Ind

William F. Friedman, WDGAS-14  11 April 1947

TO: Chief, Army Security Agency

1. Reference is made to paragraph 1a of the inclosure to the basic letter. In view of the interpretation made of the meaning of that paragraph, as set forth in ASA Memorandum dated 10 April 1947, Subject: "Procedure for Release of Information Concerning Secrecy Patents", information is requested as to the bearing that interpretation has on the question dealt with in the basic letter in regard to the status of Patent Application No. 443320. It is also requested that clarification be made as to what rights, if any, the inventors may have in regard to Patent Application No. 443320 under paragraph 1b of the policy directive forming Inclosure 1 to basic letter, in the light of the recent interpretation of the meaning of paragraph 1a thereof.

2. This indorsement is submitted on the premise that it would be to the advantage of the Army Security Agency, the War Department, and the Government as a whole, as well as to the inventors as individuals, to seek some clarification of the rights of inventors of equipment which must be safeguarded and held in a classified status for a relatively long period of time, since a clarification of this point might assist in formulating
a policy which would be most conducive to the stimulation of invention by Army Security Agency personnel.

3. In connection with the foregoing, there are submitted herewith, as information pertinent to the circumstances, nine closures listed below.

4. This matter has been discussed with Mr. F. B. Rowlett, co-inventor in the case of Patent Application No. 443320, and this indorsement is submitted on behalf of both inventors.

WILLIAM F. FRIEDMAN

9 Incl
1. Ltr dtd 27 Jan 47 to President from Acting Secretary of War w/incl-3
2. Cy of Memo for Record, dtd 19 December 46, Subj: Conference on Proposed Patent Policy
3. Cy of Brief by Chief of the Patents and Inventions Br., Legal Div., OCSig0
4. Cy of Memo for Judge Advocate General, dtd 14 Apr 44
5. Cy of 2nd Ind from JAGO to Asst. Sec. of War, dtd 17 Jan 36
6. Cy of 2nd Ind from JAGO to Adj. General, dtd 19 Apr 35
7. Cy of Brief by Chief of Patents and Inventions Br., Legal Div., OCSig0
8. Cy of Ltr from Patents & Inventions Council, Legal Div., OCSig0, dtd 10 June 46 to Mr. W.F. Friedman
SUBJECT: Release of Patent Application Serial No. 443,320

TO: Mr. William F. Friedman, WDGSS-14

1. Reference your letter dated 27 September 1945, subject as above, the attached memorandum from the Acting Deputy Assistant Chief of Staff, G-2, outlines the War Department policy on the release of cryptographic principles.

2. Analysis of the policy would indicate that:

   a. Patent application No. 443,320 will not be released unless it can be shown that the employment of the principles involved are susceptible to cryptanalysis under all circumstances; and

   b. If not released, a request for purchase of all commercially exploitable reversionary rights may be entertained provided it can be shown that Frank B. Rowlett and yourself were not directed or employed to experiment on or to invent the principles or improvements embodied in Converter M-228 or Converter M-294.

3. If it is felt that subject Patent Application should be released under (a) above; or if and when it is felt a case should be presented for purchase of rights in conformity with stipulations contained in (b) above, an application for release or purchase, containing pertinent facts and necessary proofs, may be prepared and submitted to the Director of Intelligence through the Chief, Army Security Agency.

   1 Incl
   Cy ltr dtd 29 Apr 46, subj: "Release of Cryptographic Principles"

HAROLD G. HAYES
Colonel, Signal Corps
Chief, Army Security Agency
MEMORANDUM FOR THE CHIEF, ARMY SECURITY AGENCY:

SUBJECT: Release of Cryptographic Principles.

1. The following policy is announced to be effective immediately:

a. Cryptographic principles or devices developed by officers, enlisted men, or civilians employed in any War Department Agency, or patents or patent applications on such principles or devices which are owned by, assigned to, or licensed for use of the War Department will not be released for use of foreign governments or for foreign or domestic commercial or private use until such time as necessary information is available and a procedure established in the Army Security Agency whereby information which is cryptographed by means of such principles or devices can be cryptanalyzed and read under any and all circumstances.

b. Where it is in the interest of the Government of the United States that an employee have no patent rights in cryptographic principles or devices to dispose of, and for the Government to own the entire interest for security reasons throughout any foreseeable future; and where discovery or invention of cryptographic principles or devices has been made by a civilian employee and does not relate to a matter as to which the employee was specifically directed to experiment with a view to suggesting improvements nor was produced as a result of any specific employment or contract to invent a specific device or article; and where an application for patent on such principles or devices has been filed with an assignment-in-trust to the Government for the purpose of maintaining such application in secrecy, the Military Intelligence Division will support, subject to the availability of appropriations, any reasonable request for purchase of all commercially exploitable reversionary rights of the inventor in the patent application.

/s/ CARTER W. CLARKE
Colonel, GSC
Acting Deputy A.C. of S., G-2
SUBJECT: Patent Application Serial No. 443,320

TC: The Judge Advocate General
FROM: Director of Intelligence
ATTN: Chief, Patents Division

DATE: 19 Feb 48
COMMENT No. 4
Capt. Ramsbo/147 Est 462

1. With reference to the request contained in Comment No. 2, a search of the files of the Army Security Agency fails to reveal the specific evidence upon which the Signal Corps Patent Board based its decision regarding subject patent application.

2. The following information from the files of the Army Security agency is submitted as evidence which may have been considered by the Signal Corps Patent Board in reaching its decision.

3. Mr. Friedman has been a civilian employee of the Department of the Army since 31 December 1921. His duties as described in the original appointment were: the compilation and preparation of all methods for secret correspondence to be used in the Army; the supervision of instruction of commissioned personnel in the proper use of codes and ciphers; preparation of instructions and papers on such subjects; and compilation of special problems for instruction purposes (Inclosure 2). Formal job descriptions of the type currently in use for civilian employees were not initiated within the OCSign until 1942 and therefore no such formal job descriptions are available for periods before 1942. However, in the case of Mr. Friedman, written indications of his duties in a form somewhat equivalent to that followed in the currently used job descriptions were found for the years 1930 and 1942. In 1930, Mr. Friedman's job was designated as that of "Principal Cryptanalyst," P-6, and in the year 1942 this title was changed to read "Head Cryptanalyst," P-7, concomitant with a promotion to the next grade (Inclosure 2). Mr. Friedman has held a comparable position since his original appointment under Section 10, Rule II, on 30 December 1921. The responsibilities of the position have greatly increased with the growth of the Army Security Agency, but the basic duties of the position are essentially those for which he was originally appointed (Inclosure 2).

4. Mr. Rowlett was appointed "Junior Cryptanalyst," P-1 in the year 1930. His duties were largely of an independent nature, under the general supervision of "Principal Cryptanalyst," Mr. Friedman. As in the case of Mr. Friedman, his duties remained relatively the same through the years, although his title changed in accordance with his promotions. Descriptions of the duties performed by Mr. Rowlett for the years 1936 and 1941 are enclosed (Inclosure 3). No written descriptions of the work performed by Mr. Rowlett are available between these years for reasons cited in the case of Mr. Friedman, paragraph 3 above.

5. Relative to the rights of Mr. Rowlett in the subject invention, he has been contacted personally and states that he has full knowledge of his rights in the matter and that he concurs fully with the action being taken by Mr. Friedman.

FOR THE DIRECTOR OF INTELLIGENCE:

COPIES FURNISHED:
AS-7/F
Mr. Friedman
Mr. Rowlett

3 Inclos.
1. n/c
Added 2 inclos
2. Job info on Mr. Friedman
3. Job info on Mr. Rowlett

SIGNED AND SENT OUT

FEB 20 1948

HAROLD C. HAYES
Colonel, Signal Corp
Chief, Army Security Agency
SUBJECT: Patent Application Serial No. 443,320

TO: JAG
FROM: D/I, GSUSA

29 DEC 1947

Colonel McGarr/6967/rmr

1. Mr. William F. Friedman, a civilian government employee of the Army Security Agency, Intelligence Division, has requested certain information on which to prepare a case looking towards disposition to the Government of all commercially exploitable reversionary rights as an inventor in the subject patent application.

2. The policy of the then War Department, A. G. of S., G-2, as announced 29 April 1946 (Tab B-1 of Incl 4), is that where it is in the interest of the Government an employee have no patent rights for security reasons in a device he was not specifically directed to invent, the ID will support any reasonable request for purchase of commercially exploitable reversionary rights of the inventor.

3. The Signal Corps Patent Board has rendered a decision that the subject invention was not the result of "-- specific designation to invent --", Tab B-1 to Incl 5.

4. It is considered that the secrecy order now standing against the subject application must be continued (Incl 4).

5. From a legal viewpoint, information is requested on the actions to recover outlined in paragraph 2 a and b of subject letter 8 December 1947 by Mr. Friedman, and the manner in which final action should be accomplished.

FOR THE DIRECTOR OF INTELLIGENCE:

/s/ Bruce W. Bidwell
BRUCE W. BIDWELL, Col, GSC
Assistant Executive

Incl

Ltr dtb 8 Dec 47
w/incls (5)

FILE No. JAGP 1948/103-8 (5 Jan 48) SUBJECT As above

TO FROM DATE 7 JAN 1948 COMMENT NO. 2
Chief Signal Officer Patents Division, Col. G. W. Garde/6922
ATTN: Mr. Percio, Chief, JAG
Legal Division.

Reference is made to paragraph 3, Comment No. 1, which states that the Signal Corps Patent Board has rendered a decision that the subject invention was not the result of "specific designation to invent". It is requested that this office be advised of the underlying facts determined by the Board in connection with the employee's status and assignment, including his job designation, which resulted in above decision.

FOR THE JUDGE ADVOCATE GENERAL:

/s/ George W. Garde
GEORGE W. GARDES, Col, JAGD
Chief, Patents Division

ncl: n/c
1. In accordance with telephone conversation 14 January 1948 with Colonel Gardes, JAG Patent's Division, the inclosed correspondence is forwarded for your direct reply for the reason that subject patent application is now being prosecuted and is under the general jurisdiction of the Army Security Agency, and also because the joint inventors are now employees of the Army Security Agency.

2. A search of the files in this Office failed to reveal any written or documentary evidence upon which the Signal Corps Patent Board based its decision that the subject invention was not the result of specific designation to invent.

3. It is noted that the other joint inventor, Mr. Rowlett, has not entered into the question being raised by Mr. Friedman. It is believed that the rights of Mr. Rowlett in the subject invention must also be taken into account in this matter.

FOR THE CHIEF SIGNAL OFFICER:

/s/ J. E. Pernice
JOHN E. PERNICE
Chief, Legal Division
MEMORANDUM FOR RECORD

1. Pursuant to an invitation from Captain Safford to participate in a meeting with engineers from Teletype Corporation, the undersigned, accompanied by Dr. Kullback and Dr. Sinkov went to Captain Safford's office at 1000 hours on 9 September 1947.

2. Captain Safford explained that the Teletype engineers were delayed and that he really did not know why they were coming or whether they were bringing any model or models.

3. While waiting for the Teletype engineers to appear, Captain Safford demonstrated two recently completed developments of his own laboratory:

   a. A modification of Converter M-228 (SIGCUM) to be known as CSP-3300. This equipment is designed to give improved security for SIGCUM usage especially in connection with the transmission of intercept traffic for OP-20-2. The modified machine eliminates the 131 mixing cabinet and uses relays mounted underneath the frame of the SIGCUM for this purpose. These relays also are used in connection with a baud transposition feature so that the plain text bauds undergo transposition before Vernam-rule substitution. The motion of the rotors has also been modified, with the introduction of reversed stepping in the case of two of the five rotors as an added feature. Off-line (tape) operation was demonstrated but it was my understanding that provision has been or will be made for on-line operation also. This machine is worth ASA's study; however, it will only operate from tape and hence its application is limited.

   b. A modification of SIGABA for the production of one-time key tapes. The output of the cryptographic rotors is reduced to 5-unit code symbols. The control and cryptographic rotors are subjected to a different motion control than in SIGABA. The purpose of this equipment is to permit local stations to produce "one-time tapes" from machine settings, so as to have the equivalent of "one-time" intercommunication among a large number of stations when conditions permit.
Otherwise, the one-time tape can be produced by a central station and distributed to users by courier, as is normally the case. Captain Safford claims that the output is perfectly random. This machine also should be investigated by ASA.

4. Since the noon hour was approaching and the Teletype engineers had not yet arrived, the ASA representatives left, with the statement that other representatives would replace them for a meeting at 1400.

5. The other ASA representatives, Messrs. Rosen and Barlow from AS-70 and Messrs. Kuhn and Brann from AS-80 attended the conference in the afternoon. Mr. Rosen reported to me that the Teletype engineers brought nothing with them, stating that the model of the HOCM would not be completed until sometime in November. The project is apparently not going forward as had been anticipated.

6. The ASA representatives were then shown the model of CSP-3300 discussed under Paragraph 3a above. Mr. Rosen reports that he regards the equipment as too complex, that it uses relays which will not stand up under ordinary usage, and will not perform the functions required of the Converter MX-519()/TG. Mr. Brann, having read the foregoing, makes the following comment:

"It might be noted that Navy is placing the greater emphasis upon modification of existing equipments instead of development of new ideas. It is believed the CSP 3300 will cause very awkward operational practices in that transmission and encryption will have to be on-line with reception on-line and consequent decryption off-line. This method of operation would not be acceptable to any of the Army using services."

Mr. Kuhn adds the following:

"In addition to the remarks made by Mr. Brann in connection with the CSP 3300 I believe it might be more economical in the end to build a complete new unit rather than attempt to convert the H-228 unit. The work involved would exceed that now being done to convert a SIGABA to a SIGROD."

WILLIAM F. FRIEDMAN
Chief, Communications Research
Ext 215
A means of providing an irregular wheel movement in Cipher Machine using cipher wheels.

The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: when a key is depressed, two contacts are closed, namely, (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding
thereby to move forward.

Figure 1 is a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; 21 is the indicating device; and 22 is the connection to the universal contact which may be connected to any contact of the rings of contacts 11 on end plate 19.

Fig. 2 shows one manner in which the ring of contacts on end plate 20, through which the current passes to the selector magnets, are connected to the wheel selector magnets.
A means of providing an irregular wheel movement in Cipher Machine of the Hebern and Enigma type.

The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: When a key is depressed, two contacts are closed, namely, (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding
Figure 1 is a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 the reversing switch; 21 is the indicating device; and 22 is the connection to the universal bar contact which may be connected to any one of the rings of contacts 11 on end plate 19.

Fig. 2 shows the manner in which the ring of contacts on end plate 20, through which the current passes to the selector magnets, are connected to the wheel selector magnets.
A means of providing an irregular wheel movement in a cipher machine of the Hebern and Enigma type.

The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: When a key is depressed, two contacts are closed, namely, (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding...
thereafter move forward.

Figure 1 is a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates; 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the "key to lamp" current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 is the reversing switch; 21 is the indicating device; and 22 is the connection to the universal bar which may be connected to any one of the rings of contacts 11 on end plate 19.

Fig. 2 shows the manner in which the ring of contacts on end plate 20 through which the current passes to the selector magnets are connected to the wheel selector magnets. A random selection of these contacts may be made for connection to the selector wheel selector magnets. Also, current may enter at one or more points on the opposite end plate, effectively a movement of one or more wheels per cycle.
A means of providing an irregular wheel movement in a cipher machine of the Hebern and Enigma type.

The basic principle of this invention utilizes the cipher wheels of the cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts, which contacts are independent of the first mentioned set of contacts, but are connected to each other in an irregular manner, analogous to the manner in which the first mentioned set of contacts are connected. Also the end plates will bear a double ring of contacts which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in Figs. 1 and 2 of the attached drawing.

The action of the machine is as follows: When a key is depressed, two contacts are closed, namely: (1) the key contact which allows a current to pass through one of the above-mentioned rings of contacts to operate an indicating device giving the encipherment of the letter corresponding to said key and (2) a universal bar contact which permits current to enter at a single contact of the other of the aforementioned rings of contacts on one of the end plates, pass through one of the contacts of the corresponding rings of contacts of all the cipher wheels, and pass out at one of the contacts on the corresponding ring of contacts of the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding
thereeto to move forward.

Figure 1 is a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the hereinbefore described cipher wheels; 19 and 20 are the end plates, 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the current passes to the wheel selector magnets; 12 and 14 are the rings of contacts through which the 'key to lamp' current passes; 15 is the key contact; 16 is the above-mentioned universal bar contact; 17 is the source of power; 18 is the reversing switch; 21 is the indicating device; and 22 is the connection to the universal bar which may be connected to any one of the rings of contacts 11 on end plate 19.

Fig. 2 shows the manner in which the ring of contacts on end plate 20 through which the current passes to the selector magnets are connected to the wheel selector magnets.
A means of providing an irregular wheel movement in cipher machine of the Hebrew type and Enigma type.

The principle of this invention is to utilize the cipher wheels of the Hebrew cipher machine to provide an irregular selection of the particular wheel which is to be moved. A method of effecting this selection is to provide, in addition to the present ring of 26 contacts on each face of the wheel, a second ring of 26 contacts which contacts are independent of the first set of 26 first mentioned set of contacts, that are connected to each other in an irregular manner, analogous to the manner in which the first mentioned contacts are connected. Also the end plates providing a means of will bear a double ring of contacts.
which coincide exactly with the two rings of contacts on the face of each cipher wheel. These two rings of contacts on each end plate are connected as indicated in the attached drawing, and in the description thereof which follows. From the key the current of the action of the machine will flow as follows: When a key is depressed, two contacts are closed, namely, the key contact which will allow a current to pass through one of the copper contacts to operate an indrawing device giving the encipherment of the letter corresponding to that key, and a universal contact which permits current to enter at a single contact of one of the copper rings of contacts and the contacts of the corresponding rings of contacts of all the cipher wheels and each at one of the corresponding rings of contacts on the other end plate, and thence to a selecting magnet which permits the cipher wheel corresponding thereto to move over forward.
Figure 1 shows a schematic diagram of the invention. 1, 2, 3, 4, and 5 are the hereinbefore described eigher wheels; 19 and 20 are the end plates; 6, 7, 8, 9, 10 are the wheel selector magnets which allow a mechanism to step one of the wheels forward at each depression of a key; 11 and 13 are the rings of contacts through which the wheel stepping selector magnets; 12 and 14 are the rings of contacts which the key would 'damp' current passes; 15 is the key contact; 16 is the above mentioned universal bar contact; 17 is the source of power to the reversing switch; 21 is the indicating device; and 32 is the connection to the universal bar which may be connected to any one of the proper contacts by means of contact 19.

Fig 2 shows the manner in which the rings of contacts on each plate 20 are connected to the wheel selector magnets.
Inventor: W. F. Friedman

Rank, position or employment: Capt., Artillery

Permanent address: Wash., D.C.

Title of Invention: System for Randomizing the Relations of Electrical Circuits

Description of Invention:

Dates and places of Invention:

(1) Conception by inventor: June 15, 1935 at Wash., D.C.

(2) Disclosure to others: June 24, 1935 at Wash., D.C.

(3) First sketch or drawing: June 24, 1935 at Wash., D.C.

(4) First written description: June 24, 1935 at Wash., D.C.

(5) Completion of model or full sized device: June 24, 1935 at Wash., D.C.

(6) First test or operation of invention: June 24, 1935 at Wash., D.C.

Results of tests, and extent of use of invention:

None

Names of persons having knowledge of facts stated under (d) and (e):

None

Prior Reports:

None

Patents and Patent applications: None other than present application

Rights of U.S. Government: None

Licenses or Assignment:

None

Contracts involved:

Contractors
Address

Contract No. and date

Subject matter

Location of Plant

Official title or status of employment of inventor:

Signature of witness and date:

Signature of inventor and date:

Remarks of Forwarding Officer:

Signature of Forwarding Officer and date:

W-692, A.S. Rev. 6/2/24
The following information will be given under the headings indicated:

(a) The inventor should give his permanent address. He should also give his rank, corps, position or status of employment at the time invention was made.

(b) The title of the invention should start with words indicating the class to which the invention belongs, such as "Method of" or "Process of" in case the invention relates to a method or process; or the name of the article, device or type of machine in case the invention relates to an article, device or machine, or the name of the material or composition in case the invention is an improvement in material or composition.

(c) The description of the invention may be brief, provided reference is made to detailed specifications and drawings, which should be identified by date and file number if official, or should be attached to the report if not part of the official records of the War Department. In either case, all drawings and descriptive pamphlets relating to the invention should be listed.

(d) Care should be taken to give the earliest date on which the invention suggested itself to you, even though it was not completely in mind. If the invention comprises different inventive ideas, give the dates with reference to each part of the invention separately, taking care to identify each part clearly in the description of the invention.

(e) State whether or not the invention was found to be operative, and the degree of success attained at each test of the model or full sized device. In stating the extent of use of the invention, separate "use by the Government" from "commercial use".

(f) State the names of persons who had knowledge of the invention and facts concerning it on or about the dates mentioned.

(g) Has description of invention or report of test, if any, been submitted to officers of the War Department? If so, when and to whom? Give references to all prior reports, including all information, needed to locate same in files.

(h) List all applications for patents by filing dates, serial number and title. List all patents by patent number, date of grant, and title.

(i) Has tender to the United States been made? If so, when and to whom? If not, tender the use of the invention to the United States or explain why not.

(j) State what, if any, rights in the invention have been granted to others; including extent of interest granted and date of recording assignment or license in Patent Office.

(k) If contracts have been placed for the invention, or if the invention was made in connection with the performance of a contract in which the United States is interested, the facts should be given briefly, including contractor's name and address; Contract No. and Date of Contract; Subject Matter; Location of Contractor's Plant where work was done; and Official Title or Status of Employment of Inventor.

(l) It is desirable that the witness be familiar with the facts stated concerning the invention and have a sufficient understanding of the invention to describe its construction and operation.

(m) The forwarding officer should give his opinion of the value of the invention to the U.S. and whether or not the prospective development or the art to which the invention relates would make it advisable to protect the invention and the Government's right to use the same by an application for patent.
Report of M-228

1. Col. Corderman

1. There is appended herewith a report on the security of the M-228. The material on which this study was based was taken from War Department channels and is a true indication of the type of security which may be expected from usage of this equipment.

2. The recommendations given below were arrived at in a conference among Major Rosen, Major Hiser, Captain Douglas and myself:

a. It is recommended that a study be undertaken immediately by the ablest cryptanalysts in SSS to determine if it is possible to reconstruct the cryptographic elements used in the M-228 under the conditions stated in the appended discussion.

b. It is further recommended that the M-228 be used for confidential and lower classification on radio, and then only under special conditions where complete supervision and control can be exercised by personnel properly trained in handling the M-228 both from operational and security standpoints; that for such use special keys will be arranged; that typing perforators or equivalent equipment be used; and that under no circumstances will conference calls be permitted.

c. It is further recommended that no change be made in the present use of the M-228 on circuits such as land lines which are reasonably secure from interception.

d. It is further recommended that a study be undertaken to determine the most expeditious method of handling traffic over channels similar to the
Washington-London, Washington-Brisbane, or Washington-Algiers channels. This study should be directed towards evaluating the relative merits of fully automatic versus systems using the 134-C and usual transmission agencies.

Att: Report w/o Incls.

Frank B. Rowlett
Major, Sig.C.
SPSIS-4
8 June 1943
Report To: Colonel Corderman

Subject: Report on the M-228

1. The M-228 is the mechanism for generating a key which is used for the encipherment of plain-text signals generated by a teletypewriter mechanism. The invention of the cryptographic principle was made at SSS and reduced to practice at the SGGDL. The electrical application of the cryptographic key generated by the M-228 is almost identical with that proposed by Gilbert S. Vernam in 1918 and later. (See Vernam patents attached.) The M-228 was proposed initially for encipherment of messages to be transmitted on land lines. It was not contemplated that it should be used for enciphering signals to be transmitted by radio.

2. The relationship between the teletype, the M-228 (key generator) and the device (applique unit) which "scrambles" the plain-text signals is shown in the schematic diagram of Fig. 1. The teletype generating the plain-text signals is standard equipment which feeds the signals into a group of relays inside the applique unit. The M-228 consists of a set of 5 cipher wheels which, in conjunction with a teletype distributor head, generate an extremely long sequence of impulses similar to the plain-text signals. The impulses of the M-228 are fed into the relays of the applique unit where the combination of the plain-text and key impulses are effected as described below, to produce cipher text. On the receiving end the conditions are reversed. The signals of the enciphered text are fed into the relays of the applique unit where the key generated by the M-228 is removed and the remaining plain-text signal is fed into a standard teletype printer to produce the plain text version of the message.

3. a. Cryptanalytically, the encipherment effected by the applique unit can be expressed as a mathematical equation with elements of a limited binary system of 32 combinations. The Baudot Code used by the teletype is nothing more than the expression of 32 conditions by means of combinations of elements referred to hereinafter as + and −. The equation stating the conditions of encipherment is simply $P + K = C$.

b. In the case of the encipherment of a single letter, say the first letter of a message, the specific equation will become $P_1 + K_1 = C_1$. Likewise, the second, third, and fourth
encipherment, etc., may be expressed by the same type of equation using the appropriate subscripts, \( F_2 + K_2 = C_2 \) etc. Given the conditions that two messages are enciphered by the same key, if the second message is represented by primes, these equations may be written as \( F_1' + K_1 = C_1' \) etc.

2. Given the first letters of two messages enciphered by the same key the equations pertaining to those two letters are:

\[
F_1 + K_1 = C_1 \\
F_1' + K_1 = C_1'
\]

Since \( C_1 \) and \( C_1' \) are the cipher texts of the messages which will be available to the cryptanalyst, \( C_1 \) and \( C_1' \) may be considered as known, giving 2 equations with 3 unknowns. By subtracting one equation from the other, the \( K_1 \)'s can be eliminated giving \( F_1 - F_1' = C_1 - C_1' \), a single equation with 2 unknowns. This equation can be solved since the condition that \( F_1 \) and \( F_1' \) must be plain-text letters can be applied. Practically, this would be affected by considering several equations at one time and examining a probable word for either the \( F \) or the \( F' \), as indicated in the following paragraphs.

3. a. There is attached a chart which gives the Baudot equivalents of the 26 letters of the alphabet plus the 6 functions of the teletype giving a total of 32 distinct combinations. As stated above in Par. 3b these combinations may be considered as elements of a system of binary notation and the customary processes of addition, subtraction, multiplication, and division may be applied. The cryptographic function of the reays of the applique units is to perform addition of the 5 impulses of the plain text letters generated by the teletypewriter with the 5 impulses generated by the M-228. Since all 32 possible combinations are generated by the M-228, a total of 32 x 32 conditions will arise from the addition of a plain-text signal and a key signal. This can be best demonstrated by performing an example in addition which simulates the action of the reays. Suppose the plain text to be enciphered is the plain-text word THE. The Baudot equivalents for the 3 letters are shown below:

\[
T = - - - \cdot + \\
H = - - + - + \\
E = + - - - - \\
\]
Let it be assumed that the key generated by the M-228 at the
instant is:

1st Key combination: + - + + +
2nd Key combination: - + + - +
3rd Key combination: + - - - +

If reference is made to the accompanying chart (Incl. No. 2), it
will be noted that the first key combination corresponds to the
letter X, the second to the letter V, and the third to the letter
Y. The addition performed by the relays of the applique unit
can be effected by the application of the following rule: If two
like elements are added a + is obtained; if two unlike elements
are added, a - is obtained. The addition in this case will
be non-carrying, and since only two elements are used in the
system it will be noted that addition and subtraction produce
identical results. Based on this rule, the addition of T and the
first key combination produces a combination which corresponds
to the letter L; H and V give Y; and E and Y give J, as shown
hereafter:

<table>
<thead>
<tr>
<th>Key Combination</th>
<th>T</th>
<th>H</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Letter</td>
<td>+ + + +</td>
<td>+ + +</td>
<td>+ + + +</td>
</tr>
<tr>
<td>2nd Letter</td>
<td>+ - + +</td>
<td>+ + +</td>
<td>+ - + +</td>
</tr>
<tr>
<td>3rd Letter</td>
<td>+ - + -</td>
<td>+ - +</td>
<td>+ + + +</td>
</tr>
</tbody>
</table>

As stated above, the addition of each of the 32
elements with itself and all the other elements gives (32)^2
combinations. These combinations are represented in table
attached (Incl. No. 3). Reference to this table permits rapid
addition of plain text and key to give cipher, or an addition of
cipher and key to produce plain text. The table is reciprocal
in nature and may be used as follows: The plain-text letter is
sought in the sequence at the left hand side of the table; the
key letter is sought in the sequence at the top of the table;
at the intersection of the row and column so defined, the cipher-
text letter is found.
c. The solution of the equation referred to in Par. 3.2
\[ P_1 \cdot P_1' = C \] can be effected empirically for two texts enciphered
by the same key as follows. If the assumption is correct the
exact key used for its encipherment can be obtained by use of
the chart. This key can then be applied to either of the two
superimposed messages to produce the plain text corresponding
thereto, as demonstrated in the following paragraph.
Page Denied
There are attached as Tables 5, 6, 7, 8 etc., examples of messages appearing on War Department radio circuits using the M-228 for which identical setting of cipher wheels were used. The solution of these messages is fairly simple. It can be greatly speeded up by application of machine methods and detailed worksheets are appended. A description of the method used, while fairly simple, is not within the scope of this paper.

5. The M-228 is misleading in appearance. The fact that it uses the same type of cipher wheels as the SIGABA immediately suggests to the observer that it effects the same type cryptographic treatment as the SIGABA. The SIGABA uses an entirely different cryptographic principle, and consequently its security is much greater than that of the M-228. The fallacy in assuming that the M-228 affords equal or comparative security with the SIGABA is dangerous since it produces a false feeling of security in the minds of those who do not appreciate the cryptographic principles about which the two machines are constructed.
6. Insofar as the security of the M-228 itself is concerned, considering the machine as it is now being used, the writer is aware of no method for reconstructing the wheels in case a large portion of the pure key is available. However, this appears to be a difficult problem, but in view of the fact that the principle is new in the art and that no extensive study of it has been made, there is some doubt in the writer's mind as to the validity of the assumption that the wheels can not be reconstructed under the circumstances of its present usage. For example, in the solution of the messages of Table 5, 6, etc., considerable pure key was recovered, which might be sufficient to permit a complete solution of the system.

7. A primary weakness of the M-228 lies in the fact that transmission can be made in the clear due to failure of contacts of the applique unit, or a simple failure on the part of the operator to throw a switch to cipher. In tape transmission on certain circuits the entire message could be transmitted without the operator's being aware that the message had gone out in the clear. It is therefore necessary to monitor all M-228 transmissions between the time of the encipherment and the time at which the impulses are fed into the transmission medium.

8. In view of the fact that the M-228 was designed for rapid handling of messages to be cryptographed, retransmissions of messages are made without paraphrasing. This happens most frequently with new operators and in general it is due to operational difficulties rather than functional or machine difficulties. No security study has been made to determine the effect of such transmissions on the fundamental security of the system.

9. The M-228 lends itself for use in conference calls. The nature of the language and text appearing in such a call cannot be readily controlled from the standpoint of security, and it is possibly more stereotypic in nature than any other type of communication other than "synoptics". This is because conferences usually consist of questions and answers, and if a simultaneous recording is made of both channels, the assumption of plain text by the cryptanalyst is simplified considerably. Such things as OK, CAR RESET, LINE FEED, GAPLS, and THAT IS ALL, will appear and can be readily recognized. If the system has any inherent weakness this type of usage will permit of its utmost exploitation.
10. In the foregoing discussion the emphasis was placed on solution of two messages sent in the same key. No fair estimate of the security of a properly phrased, well-composed, and correctly cryptographed message can be given. However, for such communications the security of the M-228 can be estimated as lying somewhere between one tenth and one fourth that afforded by the SIGABA. In view of this statement, if the SIGABA is considered as the ultimate in security and the criterion of secret classification is based on the security afforded by it, it would appear that the M-228 on radio would afford only "confidential" security. When it is considered that the bulk of traffic will tend to move on M-228 channels this estimate makes it appear doubtful as to whether the M-228 should be used for messages of secret classification, when such channels are subject to interception.
REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE

THE PROBLEM

1. To determine the U.S. position toward the United Kingdom's proposals in RFC 5/99 (attached as Appendix "A") that:

   (1) there be a full and complete interchange of cryptographic principles and policy on a reciprocal basis.

   (2) if the U.S. Chiefs of Staff cannot agree to (1) above, they authorize the disclosure of the principles of the ECM (SIGABA) so that these may be incorporated in a new British Cipher Machine.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. Of the two foregoing proposals, the first is unacceptable. The United States Government adheres to the following generally accepted basic principle of national sovereignty and security: the means and methods which a government employs for the protection of its own communications constitute a private matter not to be shared in toto with any other government. This principle is sound because it is impossible to be certain that a former ally will not be someday overrun by a common enemy or may even become a foe, in which case a well-forged weapon may be turned against its originator.

As regards the effects of such a contingency, the primary danger in the cryptologic field is not that the security of communications may be destroyed or impaired but that the sources of communication intelligence may be dried up.
3. With regard to the second or alternative proposal, it is felt that this solution should be accepted by the United States, for the following reasons:

a. In the spring of 1947 there were Combined discussions on this same subject. These resulted in a decision to withhold the ECM and to study possible improvements in the GCM. The results of this study have been largely negative, the only possibility being the ECM, a machine which represents some improvement in security over the GCM but not deemed sufficient in degree to meet with British acceptance. Moreover, the modifications which would be required in the British Typer machine to convert it into a ECM are such that there is grave doubt as to their accomplishment. Also, the British have decided that they must replace the Typer in any case and the introduction of a suitable replacement would be expensive in terms of time required for research, development and service testing. It would be to the advantage of the U.S. as well as to the British if such a delay could be avoided so that British equipment suitable also for Combined Communications would become available at an early date.

b. During the Combined discussions referred to above, the British indicated that they were aware of the principles of the ECM. They described them quite accurately and indicated that they considered their security to be of the highest order. They admitted, in fact, that they had incorporated those cryptographic principles in a radioteletype cipher machine for their own use. Furthermore, even as regards the engineering know-how which went into the construction of the ECM, this knowledge has been disclosed to the British, since they were provided with $581$ 1700. This machine was simply an ECM chassis with certain of the ECM cryptographic features eliminated.
c. Disclosure of the ECM to the British and its adoption by them would give the two governments a suitable piece of equipment ensuring the highest degree of security for vital combined U.S. - British communications.

d. Disclosure of the ECM will not leave the U.S. without equipment unique to the U.S. As a matter of fact, a modification of the ECM has already been developed (CSP-2900) and is available in quantity. This modification, which improves the security of the ECM, does so without in any way impairing its use as an ordinary ECM or as a CCM. By means of a simple switching arrangement it is possible to make the CSP-2900 serve as a device purely for U.S. communications, or as an ECM for U.S. - British combined communications, or as a CCM. However, the principles of the CSP-2900 would not be disclosed to the British.

e. Release of the ECM to the British would leave the way open to the adoption of the CCM for North Atlantic Pact communications if such a decision should be found to be necessary in the national interest. British - U.S. use of the ECM would be easily adaptable to North Atlantic Pact communications since the addition of a simple already available adapter to either the ECM or the CSP-2900 would permit communication with any North Atlantic Pact nation holding the CCM. In addition, disclosure of the CCM to the other signatories to the North Atlantic Pact would not impair the security of U.S. - British communications since the CCM system would then be reserved for that specific purpose.

f. At the time of the 1947 Combined discussions on this subject, one of the principal U.S. objections to disclosing the ECM to
the British was the increased danger of compromise arising from the wider distribution of the equipment if the British were permitted to have it. This increased danger is recognized but it is believed that the advantages cited above outweigh this objection.

g. Also at the time of the 1967 Combined discussions there were indications that the British did not provide and enforce physical security protective measures for their crypto-equipment equal to those required and enforced by the U.S. services. Because of this it was agreed on a Combined level that a prerequisite to further discussions regarding a replacement for the CES would be a Combined agreement covering the measures both governments would apply in the handling and protection of combined cryptomaterial. Such an agreement has been concluded and concurred in by both Governments (CCB-295, 11 Oct 1949). A review of that document in order to insure identity in security regulations applicable to the CES and an acceptance of such changes therein as may be deemed necessary by the U.S. should be a preliminary to entering upon discussions leading to a Full disclosure of the CES to the British.

CONCLUSIONS

4. It is concluded that:

a. The first proposal made by the United Kingdom in
RDC 5/99 of 13 July 1949 should be rejected.

b. The details of construction of the CES (SIGABA) should be disclosed to the U.K. in discussions which will include a review and acceptance by both Governments of identical security regulations to insure the physical protection and proper use of the equipment.
RECOMMENDATIONS

5. It is recommended that:
   a. A memorandum substantially as in Appendix "B" be forwarded to the British Joint Services Mission.

COORDINATION

6. Coordination with AFCIAC has been effected.
REPLACEMENT OF THE PRESENT COMBINED CIPHER MACHINE

(Proposed reply to the British Joint Services Mission)

1. The U.S. Joint Chiefs of Staff have carefully considered the proposals made in RDC 5/99 of 13 July 1949 concerning the replacement of the existing Combined Cipher Machine. The U.S. Joint Chiefs of Staff regret that they are unable to accept the proposal for a full and complete interchange of cryptographic principles and policy on a reciprocal basis. However, they are prepared to authorize discussions which can commence in Washington at any time, leading to the disclosure of the principles of the ECH (SIGABA) so that these may be incorporated in a new British Cipher Machine, these discussions to be preceded by a review and acceptance by both governments of identical security regulations to provide for the physical protection and proper use of the equipment.
MEMORANDUM FOR: CHIEF, ARMY SECURITY AGENCY

SUBJECT: Replacement of the CCM

REFERENCE: (a) AFCIAC Document 13/4 of 14 Sept 49

1. a. In connection with reference (a), it is deemed advisable to note that the ECM-SIGABA is covered by a number of patents or patent applications.

b. Certain of these patents or patent applications are owned by the Teletype Corporation. The exact number of these cases, their serial numbers, and specific nature are unknown to this Agency, as they are being handled under Navy control.

c. There are certain other patents or patent applications, covering certain subsidiary features which were invented by Navy personnel. Details of ownership are not known to this Agency.

d. The basic cryptographic principles employed in the equipment are covered by the following patent applications, still in a secrecy status under the "Three-Year Rule" (Sec. 4894, R.S., as amended) and also under Public Law No. 700 (War-time secrecy for patent applications):

<table>
<thead>
<tr>
<th>App. Serial No.</th>
<th>Inventors</th>
<th>Date filed</th>
</tr>
</thead>
<tbody>
<tr>
<td>682,096</td>
<td>Friedman</td>
<td>25 July 1933</td>
</tr>
<tr>
<td>70,412</td>
<td>Friedman &amp; Rowlett</td>
<td>23 Mar 1936</td>
</tr>
</tbody>
</table>

In each of these two cases the U. S. Government owns the entire right, title and interest in the invention, throughout the U.S. and territories and dependencies thereof, but not elsewhere; the inventors have an irrevocable, assignable, and exclusive license to make, use and/or sell and to license others to make use and/or sell the invention. Attached hereto is a copy of the assignment in each case. (Incl. 1 and 2).
For a half century following the close of the Civil War, cryptology in the United States enjoyed a period of hibernation from which it awoke, not refreshed, as did Rip Van Winkle, but weaker. This is perhaps understandable if we take into account the fact that the United States was able to enjoy a long era of peace, broken only briefly by one short war, the Spanish-American War of 1898. For over three decades there was no need for cryptologic operations except such as were required for the communications of the Department of State. The military and naval services apparently felt that peace in their time of peace there was need for their cryptography or cryptanalysis, and hence, the training of the peace apparently to peace for as long an indefinitely long time, those services did not think it necessary or desirable to engage in cryptologic studies. Of course, the War Department and the Army still had their routine and cipher desks, the Navy Department and the Navy had their desks for producing monoalphabetic ciphers, and the Department of State had a crypt code specifically designed for the transaction of business on the subject of international affairs. But as long as the U.S. was quiet, let Europe fight—it was no part of our way of life or our affair.
The long-interminating period was briefly broken by one episode that may interest you. I had not planned to bring it to your attention in this brief history but certain events in the very recent past lead me to tell you about it. I refer here to the very small majority by which Democratic candidate Kennedy won the presidency over Republican candidate Nixon, and the consequent talk about the possibility of an upset when the electoral college scene to do its work. The very same situation occurred in the presidential election of 1876, in which Democratic candidate Samuel J. Tilden was pitted against Republican candidate Rutherford B. Hayes. (In the days of early returns Tilden seemed to be clearly the Hayes' margin's going to bed on election night, November 1876, Hayes conceded to Tilden and the newspaper next morning in fact reported Tilden victory. But a couple of days after the election it began to appear that perhaps Tilden's victory was not sure, and his supporters began maneuvers to try to make it certain by taking advantage of our peculiar system of electing a president, because it is the electoral, not the popular vote which determines who is to be president. Two days
ref A62844

The people had voted B for the President but the reversal was not acceptable to the political experts. Both who were interested in the political experts of the Republicans and the Democrats will find excellent readings in the following report.

The telegrams remained unknown for months. But the outcome of the election remained in doubt because in four states—Florida, South Carolina, Louisiana, and Oregon—each sent two groups of electors, an event not foreseen and provided against in the Constitution. A crisis arose and the country seemed on the verge of civil war. By an act of 29 January 1877, Congress created a special electoral commission to settle the disputed votes in the four states. The commission voted in favor of the Hayes electors in each case and Hayes entered the White House. But it was only some months afterward that the telegrams to which I have referred were brought to light and a situation arose within Congress felt it had to look into. Somehow or other the telegrams came into the possession of an Republican newspaper, The New York Tribune, and two members of its staff succeeded in solving those in cryptographic form.
Hassard, John R.G.


The Congressional House Committee designated to conduct the investigation was named "The select committee on alleged frauds in the Presidential Election of 1876." In the course of the investigation, the committee called upon Prof. Edward S. Holden, of the United States Naval Observatory in Washington. I think he was a captain in the Navy and specialized in mathematics. The Tribune had brought him into the picture and Prof. Holden solved the cipher but only after two. John R.G. Hassard, the chief of the Tribune staff, and his colleague, Dr. William M. Groves, also of their staff, had reached a solution.

Prof. Holden's testimony is of considerable interest. He presented his solution of the many 200 ciphers proposed in evidence. His testimony is summarized in a letter dated 21 February 1879 and it sets forth all the cryptograms used by both parties, together with their keys and full details. In that letter, Prof. Holden makes the following statement: "By September 7, 1878, I was in possession..."
In a paper by which any key to the most difficult
organisms of these (the transportation cipher)
researched by Holden, it was stated that any key
in all 10 different keys, two for messages of 10 words,
two for messages of 15 words, etc., to two for messages of
30 words. Here is the complete table of keys:

<table>
<thead>
<tr>
<th>Key</th>
<th>10 words</th>
<th>15 words</th>
<th>30 words</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

One suspects that the sequences of numbers were drawn up at random but were derived from a word of phrases.

Perhaps some of you may like to make the attempt. You will notice that in the odd-numbered keys the positions of adjacent digits reflect an underlying word or phrase.

In addition to transportation this system involved the use of code words to represent the names of certain persons, places, and numbers. Here are also a few initials. Here is the entire vocabulary:
You may be wondering why there are two transposition keys for each length of message from 10 to 30 in multiples of 5. The two keys constitute a pair and are correlation of each other, related to each other by something which one of the Tribonacci cryptanalyst termed "correlative," but which we now would call an "inverse" or "verse-inverse" an encipher-decipher relationship. Either sequence may be used to encipher, the other, then, can be used to decipher a message. For example, key III consists of the following: 8-4-1-7-13... etc., and the correlation cipher key IV, is 3-7-12-2-6... etc. A message of 15 words can be deciphered either by (1) numbering the words consecutively and then assembling the words in the order 8-4-1-7-13 etc., or by (2) writing the sequence 3-7-12-2-6... above the words of the cipher message and then assembling the words according to the sequence 1-2-3-4-5... Thus, there were, in reality, not 10 different transposition keys but only five. In fact, every pair of keys one of them must have been the inverse of it, exactly the same sequence.
Prof. Holden adds some comments, which are worth presenting:

The essence of this ingenious and novel system consists in taking apart a sentence written in plain English (disregarding it as it were) and again writing all the words in a new order, in which they make no sense. The problem of deciphering it consists in determining the order, according to which the words of the cipher should be written, in order to produce the original message.

There is one way, and only one way, in which the general problem can be solved, and that is to take two messages, A and B, of the same number of words, and to number the words in each; then to arrange message A with its words in an order which will make sense, and to arrange the words of message B in the same order. There will be one order — and only one — in which the two messages will simultaneously make sense. This is the key.

It appears that Prof. Holden did not note the verse—verse relation in each pair of sequences, or, if he did, he failed to mention it, as Hascard did in his article.
There were enough messages to permit of establishing the meanings of the code words used, so that the plain text of practically all the messages in this the most complicated of the cryptosystems involved in this bizarre political episode, became quite clear.

First there were several other systems involved, but I am going to have to pass them by because they hardly deserve attention in this brief history. I do, however, want to call your attention to the very close resemblance between what is characterized by Prof. Holdon as "the most difficult and ingenious" of the ciphers he solved, and the USMTC route cipher as the USMTC route cipher as described in the preceding lecture. Yet, not only he but also the Tribune cryptanalyst solved these ciphers without too much difficulty, although I think their work confirms my own appraisal of the weakness in the security of the route cipher. Let us now go on with cryptologic history after this political digression into the realm of what may be called political cryptology. I do not know what the Department of State used.
Another system used by the conspirators used a 2-letter for one substitution and was based upon a 10 x 10 checkboard. Apparently Prof. Holden nor the Tribune cryptanalysts recognized the latter principle, nor did they find that the coordinates of the checkboard employed a key phrase, which appropriately enough was "His Patient."

Nor did they realize that the same checkboard, with numerical coordinates, was used for the 2-digit for one letter substitution. Here are two of the messages exchanged by the conspirators, one in the letter cipher, the other in the

\[
\begin{array}{cccc}
& & & \\
& & & \\
& & & \\
& & & \\
& & & \\
\end{array}
\]

leave 1/4 page space

They are long enough for solution, if you wish to try to solve them and find the key phrase, which will amuse you by its appropriateness.
for cryptographic communications in the years following the Civil War. Probably it was a small code, even an adaptation of some commercial code. But in an article entitled "Secret Writing," which appeared in Century Magazine, Vol. XXXVII, a man named John T. Naismith, apparently a clerical clerk in the Department of the Interior, referred to a new code, in the following terms:

The cipher of the Department of State is the most modern of all in the service of the Government. It embraces the valuable features of its predecessors and the merits of the latest inventions. Being used for every species of diplomatic correspondence, it is necessarily copious and unrestricted in its capabilities, but at the same time it is
economic in its terms of expression. It is simple and speedy in its operation, but so ingenious as to secure absolute secrecy. The construction of this expier, like many ingenious devices whose operations appear simple to the eye but are difficult to explain in writing, would actually require the key to be furnished for the purpose of an intelligible description of it.

Only four years later a telegraph operator and code clerk of the State Department proved how vulnerable the Department's system of enciphered code really was. His name was Herbert D. Yardley and many of you may know about him because of his infamous book, *The American Black Chamber*, published by *Bobbins-Mariell* in 1931. As far as I know it is the only book which cannot legally be reprinted in the United States because it speaks laws forbid...
Yardley was quite wrong in thinking that his was the first successful attempt to solve a problem in an encrypted code, for in Europe successful attempts on more complicated cases were often the rule and I imagine that British cryptanalysts should have and perhaps did read cryptanalysts were quite successful in reading State Department messages only more or less regular letters. For in Europe, cryptanalysis studies were going on apace during the years of American neglect of such studies.

In our Navy the monosyllabic cipher continued in use until the middle of the eighties when several naval officers were designated to prepare a more suitable system based upon a code particularly for naval communications. The system they worked out was "cipher book" almost as large. In addition to these
[Incoherent and unclear text.]

The message seems to be about a library register and its use in the early 1800s, possibly mentioning the U.S. Patent Office and the Library of Congress. However, the text is too fragmented and unclear to provide a coherent summary.
As to the nature of the code, I will quote from Slater's own "Short explanation of the mode of using the work":

It is a numbered Telegraphic Dictionary of the English language, of which each word bears a distinctive No., and the method of using it is by an interchange of Nos., in accordance with a private understanding between correspondents, that a further No. is to be added to or deducted from the No. in the code, if the word telegraphed or written, to indicate the real-word intended, thus a "Symbolic" or "Dummy Word" is telegraphed, the meaning of which can only be read by those who have the key to the secret of how many should be added to or deducted from the No. in the Code, of the "Dummy Word", to find the word meant. Here we have a sentence of 116 words with a meaning which is quite murky but I think you will gather its import. The system is what we now call an additive or subtractive method. But in the detailed instructions Slater goes one step further and suggests that instead of telegraphing the code numbers resulting from addition or subtraction, the actual words standing alongside the sum (or difference) of the mathematical operation be sent.
in the construction of a vocabulary list, students' progress can be assessed through the use of a cumulative grade book. The grade book can be prepared using digital tools or traditional pen and paper methods. Example:

Grammar rules and exceptions:

Example: 

ASSIGNMENT: Compile a list of words with similar meanings to the example given. Use a dictionary to check the meanings and write them in the correct order. 

Example:

ASSIGNMENT: Compile a list of words with similar meanings to the example given. Use a dictionary to check the meanings and write them in the correct order. 

Example:

ASSIGNMENT: Compile a list of words with similar meanings to the example given. Use a dictionary to check the meanings and write them in the correct order. 

Example:

ASSIGNMENT: Compile a list of words with similar meanings to the example given. Use a dictionary to check the meanings and write them in the correct order. 

Example:

ASSIGNMENT: Compile a list of words with similar meanings to the example given. Use a dictionary to check the meanings and write them in the correct order. 

Example:

ASSIGNMENT: Compile a list of words with similar meanings to the example given. Use a dictionary to check the meanings and write them in the correct order. 

Example:
to General Sheridan, Commanding Army of the U.S., to explain the beauty of the new code. Again because I'm afraid you won't place too much credence in what I'm telling you, the confidential letter is printed in full in Appendix I, to the letter to which I have added the "Introduction" that Col. Gregory has placed to the instructions for using the code.

Believe it or not, this was the code that the War Department and the Army used during the Spanish-American War. It was apparently used with simple additives in a copy in my collection.

It was written on the inside of the front cover. It was 777. In The American Black Chamber, the author throws an interesting sidelight on this code system:

The compilation of codes and ciphers was, by General Orders [The meant Army Regulations], a Signal Corps function, but the war [1917] revealed the unpreparedness of this department in the United States. How much so is indicated by a talk I had with a higher officer of the Signal Corps who had just been appointed a military attaché to an Allied country. It was not intended that attachés should actually
encode and decode their own telegrams, but as a part of an intelligence course they were required to have a superficial knowledge of both processes in order that they might appreciate the importance of certain precautions enforced in safeguarding our communications.

When the new attaché, a veteran of the old Army, appeared, I handed him a brochure and rapidly went over some of our methods of secret communication. To appreciate his attitude, the reader should understand that the so-called additive or subtractive method for garbling a code telegram (used during the Spanish-American War) is about as effective for maintaining secrecy as the simple substitution cipher which we children read in Poe's *The Gold Bug*.

He listened impatiently, then growled: "That's a lot of nonsense. Whoever heard I was going to all that trouble? During the Spanish-American War we didn't do all those things. We just added the figure 1898 to all our figure code words, and the Spaniards never did find out about it."
Although the American Balance Chamber abounds with exaggerations and distortions, what the author tells about the inadequacies of United States codes and ciphers in the years just before our entry into World War I are true enough and Yardley's impatience and satires in this regard are fully and unfortunately, fully warranted.

We have noted how inadequately the Army and the War Department were equipped for cryptographic communications in the decades 1890-1910. Let us see how well equipped the Navy and the Navy Department were. For this purpose I have an example and one of great historical significance and interest. You will recall my mention of the appointment of a board of Navy officers to prepare a suitable cryptosystem for the Navy and I told you about the basic codebook and its almost gargantuan book of companions, one incorporating the code groups. For the time being, February 25, 1918, a low Saturday, the Secretary of the Navy,

John Denio...
story we go back to the time of President McKinley, whose election brought Theodore Roosevelt, a former member of the Civil Service Commission, back to Washington as Assistant Secretary of the Navy. Teddy was an ardent advocate of military and naval preparedness and frankly favored a strong foreign policy, looking forward, in fact, to the ultimate withdrawal of the European powers from the Western Hemisphere. With vigor, he set to work to make the Navy ready. When the Battleship Maine was blown up in Havana harbor on 15 February 1898, Roosevelt sharpened his efforts. During a temporary absence of his chief, John D. Long, he took it upon himself to inaugurate the preparations which he had in vain asked the Secretary to make. He ordered great quantities of coal and ammunition, directed the assembling of the Fleet, starched the arsenals and navy yards to activity. On a Saturday afternoon, ten days after the Maine was blown up, and still in the absence of Secretary Long, Teddy sat down and wrote a cablegram to go to Commodore George Dewey. Here it is, with his bold signature at the bottom:

[signature]
That was the message which alerted Dewey and which resulted in our taking the Philippines from the Spanish in the war which was declared ten days later by Spain.

I don’t know when that classification

"Secret and Confidential" was crossed out but it must have been years later, for those three words appear in the plain text of the deciphered and decoded cablegram. Here is a picture of the cablegram as it was received in Hong Kong:

![Image of cablegram]

And now I show you the deciphered and decoded text, which I produced myself by courtesy of the Chief of the Navy Security Group, who permitted me to borrow the books from Navy archives.

To translate a message three steps are necessary. First, the cable words (peculiar to English—CENTENNIAL, WASSERREIF, PAUSAUTRA, BADANADOS, etc.) are sought in the cipher book, and their accompanying number set down. WASSERREIF yields 99055; PAUSAUTRA yields 62399; BADANADOS, 11005; CENTENNIAL, 16820.

The next step is to append the first digit of each word to the last digit of the first cable word number. Thus 99055 becomes 990556. The six-digit number is then sought in the basic code book and its meaning is found to be "Secret and Confidential." The translation
demonstration of a straightforward mathematical method of solving the Vigenère cipher was published in Berlin during the mid-period of the Civil War in America. If the book created as much impression in Europe it was altogether unappreciated; in America it remained unheard of until after the advent of the 20th Century. Although Kasiski's method is ex-
plained quite accurately in the first text on cryptography, Capt. Parker Hitt's Manual for the Solution of Military ciphers (Fort Leavenworth, Kansas: Army Service Schools Press, 1916), the name Kasiski doesn't even appear in it. Other books on cryptologic subjects appeared during this period, among which the more important were the following:

Of the foregoing two deserve special mention. The first, by Commandant Bagaries, is a book notable not for its general contents, which are presented in a rather disorganized, illogical sequence, but for its presentation of a cipher device invented by the author, the so-called cylindrical cipher device, a picture of which is
I now show you. But our own Thomas Jefferson anticipated Bayeux by a century and here are two slides describing Jefferson's Wheel Cypher copied from the original manuscript among the Jefferson Papers in the Library of Congress. The second book deserving of attention is the one by de Vario, in which the present methods for solving cryptograms prepared by the Bayeux envelope cylinders or Jefferson's Wheel Cypher.

It was in the period during which books of the foregoing nature were written and published that the chanceries of European Governments operated the so-called Black Chambers for organized for solving the secret communications of one another. Intercept was unnecessary because the governments owned and operated the telegraph systems and traffic could be obtained simply by making copies of messages arriving, departing or in transit through them. This was true for every country in Europe with one exception: Great Britain. The story is highly interesting but I must condense it to a few sentences.
In England from about the year 1540 onward, a black chamber was in constant operation. It was one of two organizations called The Secret Post Office and the Office of Decipherer. In the activities of the Office of Decipherer, one famous mathematician, John Wallis, took part in the copying of the letters and the deciphering of the ciphers. Copies of letters were made, and if there were no seals, duplicates were made. Copies of letters in ciphers were sent to the Office of Decipherer for solution and the results sent to the Foreign Office, a scandal involving these two secret offices caused Parliament to close them down so that from 1844 until 1914 there was no black chamber at all in Britain. As a consequence, World War I broke out on the first of August 1914. England's black chamber had to start from scratch, but British brains and ingenuity within a few months built a cryptologic organization which contributed very greatly to Allied victory in 1918.

Perhaps the greatest and most important achievement of Room 40, the British secret intelligence service, was the interception and solution of what is deservedly called the most important single cryptogram in history. On 8 September 1918, I gave an account of this cryptogram, its interception, its solution.
and how the solution was handed over to the United States, bringing America into the war on the British side, without disclosing to the Germans just how the plaintext was obtained. Last of all, that it had been obtained by cryptanalysis, my talk took two and a half hours and I didn't quite succeed in telling the whole story, which you will find in great detail except for some technical data not yet available to the public in a book entitled The Zimmermann Telegram, by Barbara Tuchman. Also, you should consult a book entitled Eyes of the Navy, by Admiral Sir William James. Both books deal at length with the Zimmermann Telegram and tell how astutely Sir William Reginald Hall, Director of British Naval Intelligence in World War I, managed the affair so as to get the maximum possible advantage from the fact accomplished by the British Black Chamber. To summarize as I must, this fascinating true tale of cryptanalytic conquest, let me first show you the telegram as it passed from Washington to Mexico City.
the day that

Former Ambassador Page sent his 5/28/17
gram to President Wilson on (24 February 1917) quoting
the English translation of the Zimmerman Telegram
in the form in which it had been forwarded by German Ambassador von
Bernstorff in Washington to German Minister von
Eckhardt in Mexico City, the entrance of the United
States into the war as a belligerent on the side of
the Allies was assured. The English text appeared
in our newspapers on 1 March, 1917, and on 6 April 1917
that the United States declared war on Germany and the
Central Powers. The date was 6 April 1917.

In the War Department, the pace set
for preparing for active operations quickened.

There was at the moment an organization, Army
in the Navy—Army-Navy Board—Army-Navy
Committee of the State Department, Navy,
and others. These committees were advisory
in nature, but it is true that there was a
large amount of activity in the
American cryptographic
organization. There was, it is true,
that the Navy and the State
Department maintained an
unofficial
relationship with the authorities in Washington
and

(continued on next page)
For instance, here is the bold black headline in the New York Times of 1 March:

**GERMANY SEEKS ALLIANCE AGAINST U.S.**

**ASKS JAPAN AND MEXICO TO JOIN HER**

**FULL TEXT OF HER PROPOSAL MADE PUBLIC**

The New York World had a series of headlines and subheads that extended halfway down the page, beginning with:

**MEXICO AND JAPAN ASKED BY GERMANY TO ATTACK U.S. IF IT ENTERS THE WAR**

**BERNSTORFF A LEADING FIGURE IN PLOT**

There followed nine full lines of subheads to what was a most amazing and dramatic story.

"Still not withstanding all these fears that the disclosure of the Zimmerman Telegram created in America, President Wilson still hesitated. And it was not until more than a month later, and after several American ships were sunk without warning on 18 March, that..."

There were plenty of senators and representatives who disbelieved the story. It was too fantastic; it was a British plot, improved; Wilson was being taken in, etc., etc. But when Zimmerman himself publicly acknowledged that he had indeed sent such a telegram, disbelief changed quickly into vehement anger. Surely war would now be declared on Germany!
You may like to know what we regarded ourselves very instruction materials; there was much but among the sparse literature in English there was a small book which had been prepared by a Captain Parker Hitt and printed at the Army Press at the Service Schools at Fort Leavenworth, in 1916. The Signal Corps was then a part of the Service Schools and there at Leavenworth and there a few lectures were given by two or three officers who, when World War I broke out in August 1914, took an interest in the subject of military ciphers. Later they realized that there might be a need for knowledge and training. Captain Hitt's Manual was then and still is a model of compactness and practicality. Here is its title page.

It was the succinctness of the Manual that caused us to demand much. I later came to know and revere and admire its author, whose photograph I show you.

There was one other item of training literature which we studied. For a very small pamphlet entitled Advanced Problems in Cryptography and its Solution, put out by the Same Leavenworth Press in 1914. Here is its title page, and a photograph.
At that period in our history, our relations with Mexico were in a bad state so that U.S. attention was concentrated southward. Therefore practically all the messages sent to Riverbank were those of the Mexican Government.

cable offices in Washington. Under my direction Riverbank operations of this group which was successful in solving all of nearly all these ciphers was given, returning the solutions to Washington very promptly. It was also soon after war was declared on Germany the Riverbank laboratories established a school for training Army and Navy officers sent there to learn something about cryptography. In lecture II (Fig. 27) there is a picture of the last of the classes sent by the Adjutant General of the Army to Riverbank for training. It should be noted that this instruction was conducted at Colonel Fabyan's own expense as his patriotic contribution to the U.S. war efforts. Upon completion of the last training course I was commissioned as first lieutenant and ordered immediately to proceed to France where I became a member of the German Code and Ciphers Section of the General Staff G-2, A-6, GHQ - A.E.F. As the expanded designation implies, the operation were conducted in two principal sections, one devoted to working on German military field ciphers, the other to working on German field codes. There were other very small groups working on other materials, such meteorological messages, for direction finding bearings and what we now call intelligence, that is, the intercepting messages无意 to determine enemy orders of battle flow intelligence an analysis of the bearing of the direction of and flow of enemy traffic and other data sent back from our direction finding operations at our own near intercept stations.
In connection with the last-mentioned operations, you will no doubt be interested to see what is perhaps the earliest, if not the very first, chart showing the results of traffic analysis, enemy intentions from a mere study of the ebb and flow of enemy traffic.

This particular chart was drawn up from data based solely upon the ebb and flow of messages in what was called the ADFGVX cipher, which was devised by German cryptographers and often used by German High Command communications. Theoretically, it was very secure because it combined both substitution and transposition principles. Here is a diagram which, if you study carefully, will give you a clear understanding of its method of usage.

If you should wish further details, I suggest you consult documents available in the Training Literature Department Division of the NSA Office of Training. In this lecture, there is only time to tell you that although individual or isolated messages in that system appeared at that time to be absolutely impenetrable, a great many messages against protection.

*Initially, this cipher employed only the letters A,D,F,G, and X. For a matrix 5x5, later, the letter V was added, for a matrix 6x6.
messages transmitted in the ADFGVX system were read by the Allies. You may be astonished by the foregoing statement and may desire some enlightenment here, and now on this point. Well, in brief, there were three different methods of attacking the traffic in that cipher. Under the first method two or more messages with identical [beginning/plain-text] would be used to uncover the transposition as the first step. Once this had been done, the cryptanalyst had then to deal with a simple substitution in which two letter combinations of the letters ADFGVX represented single plain-text letters. The messages were usually of sufficient length for this purpose. Under the second method, two or more messages with identical plain-text endings could be used to uncover the transposition, and this was even easier than in the case of identical beginnings. You might think that cases of messages with identical beginnings or endings would be rather rare, but the stereotypic phraseology in German military mentality was them—and perhaps still is—so conformist that cases were almost invariably found in each
The day's traffic. This is astonishing considering that the keys changed daily. This system first came into use on March 1918, three weeks before the last and greatest spring offensive by the German Army. Its appearance was almost coincidental with that of other new codes and ciphers. The number of messages in the ADFGVX cipher varied from about 25 a day when the system first went into use, to as many as about 150 at the end of two months. It took about a month to figure out a method of solution, and this was done by the very able French cryptanalyst named Capt. Georges Carmouzine of the French Cipher Bureau.

The ADFGVX cipher was used quite extensively during May and June of 1918 but then the number of messages dropped very considerably. How many different keys were solved by the Allies? Not many—10 in all, that is; the keys for only 10 different days were found. Yet, because the traffic on those days was heavy about 50% of all messages sent in that cipher were solved and a great deal of valuable intelligence derived. On one occasion, a solution was so rapid that an important German operation disc
closed by one message was completely frustrated. Although the ADFGVX cipher came into use first on the Western Front, it later began to be employed on the Eastern Front, with keys that were first changed every two days but later every three days. On 2 November 1918 the key for that and the next day was solved within a period of an hour and a half because two messages with identical endings were found. A full part message in that key gave the complete plan of the German retreat from Romania.

During the whole year of the life of the ADFGVX cipher, no general solution for it was devised by the Allies despite a great deal of study. However, members of the own Signal Intelligence Service, in 1933, and while still students undergoing instruction in cryptanalysis, devised a general solution and proved its efficacy. Pride in their achievement was not diminished when in the course of writing up and describing their method in a book by French similar one was encountered in General Livierie (Cours de Cryptographie), published in 1925.
The ADFGVX cipher was not the only one used by the German Army in World War I, and there will be time to mention only very briefly two others. The first of these was a polyalphabetic substitution cipher called "the Wilhelm" which used a cipher square with a set of 30 fairly lengthy keywords. The cipher square is shown in Fig. 00 and the set of keys in Fig. 00. Just why the square contains only 22 rows instead of 26 is unknown. Certainly the rows within the square are not random sequences, nor are the keys sequences of random letters. To reconstruct the real square and the real keys, the latter problem should be relatively easy, as to the former, I really don't know. I have never tried it myself but I suspect some systematic rearrangement...

The other cipher to be mentioned is the double transposition, solution of which usually depended upon finding two messages of identical length. No general solution was known to the Allies during World War I. Occasionally an operator would apply only the first transposition and when this happened, solution was easy. Then the key thus recovered could be used to decipher other messages which had been correctly enciphered...
by the double transposition. Again, students of
the Signal Intelligence Service devised a general
solution for the double transposition cipher and
during World War II were able to prove to our
British Allies that such ciphers could be solved
without having to send two messages of identical
length. Having demonstrated, properly employed, it
probably was withdrawn from usage by the British, but we
were not told directly that this was done. I should
add that the devising of a general solution for the
two double transposition cipher represents a real
landmark of progress in cryptography without the
aid of high-speed, electronic equipment. I do
not doubt that, with such equipment, this cipher
could hardly be thought to be safe for modern
military communications.

We come now to the code systems used
by the belligerents in World War I. And first let us
see quickly what the Americans differentiated those
used for diplomatic communications from those
used for military communications. What post did the
German Foreign Office use? We have noted how
the British Black Chamber, "Room 40, B.,” dealt
with stupendous success on the code used for the transmission of the Zimmermann Telegram. But that's only part of the story—the most important part remains to be told and unfortunately I cannot divulge that part yet. But the version of that telegram as it passed from Washington to Mexico City was in one version of a basic code which had several other versions, all quite similar in basic construction and equally vulnerable to cryptanalytic attacks. Excessive pride in German achievements, and a disdain for the cryptanalytic prowess of enemy cryptanalysts, laid German diplomatic communications open to solution by the Allies to the point where nothing the German Foreign Office or its trade representatives abroad could reveal was secret, for those of you who would like to learn some details, I refer you to the first monograph on the subject by Charles J. Mandelsohn: Studies in German Diplomatic Codes Employed During the World War, Government Printing Office, 1937. This monograph is confidential; that copies are available in the Office of Training, NSA.
At the time, we had an unexplored field in the United States. Dr. Maudlin, a former member of the British agency, said: "About a year later we received from the British agent a copy of a partial reconstruction of the German Code 13040 (about half of the vocabulary of 19,200 words and 800 of the possibly 7,600 proper names). This code and its variations are used in the German Foreign Office and the German embassy in Washington up to the time of the rupture in relations, and our files contain a considerable number of messages, some of them of historical interest, which were now read with the aid of this code book." The vocabulary of the German diplomatic code contained 189 pages containing exactly 100 words or expressions to the page, arranged in two columns of 50 each accompanied by numbers from 00 to 99. In each column, the groups in the left-hand column, for instance, 00-09, 10-19, etc., were blocks of 10. The pages in the basic code were numbered from 1 to 139 and from this code several were made by the use of conversion tables. This code was the original framework for conversion and several different communications were made by means of these tables for converting the page numbers in the basic code into different page numbers in the derived code. In addition, there were tables for converting the page numbers from one code to another, for example, pages 15-18 in code 13040 became pages 55-58 in code 5950; pages 19-22 in 13030 became pages 192-195 in 5950, etc. Then there were tables for converting line numbers from one code to another, and this was done in blocks of 10. For example, the fifth block of the fifth figure (penultimate figure 4) became the first (penultimate figure 0) and the 12th, 2nd, and 4th blocks were moved down one place.
The other five blocks (far right-hand side of the page) were rearranged in the same manner.

It is obvious that codes derived in such a manner from a basic code by no means represent the equivalents of being different codes; they were all rather equivalents of one another. Also to be mentioned is the fact that in certain cases 3-digit numbers were added to or subtracted from the code numbers of a message and that in practically every case it was not difficult to determine the additive or subtractive.

In none of the cases or codes mentioned thus far was there one that could at least be considered to be a randomized, "hatted," or true two-part code. (To continue on p. 33).
It is my belief that the conversion tables were not used by the code clerks but by the compiling authorities in Berlin. In other words, the various versions of the basic code were actually printed but that the original, page number, mixed page was altered as separate books containing code sheets were written by hand. The original number being crossed out and another different number appearing, the new number
written either at the top or bottom of the page, perhaps in both places. Similarly, the block numbers were probably changed by hand. In both cases the alterations were made in accordance with some system, the idea of randomness seems foreign to the German mentality and for the Germans never do anything by random. I am sure that if randomness were a desideratum, they would figure out a system therefor.
So much for German diplomatic secret communications. What about German military crypto-communications? In this area it is necessary to mention a situation which is somewhat unique. When World War I commenced, the German Army was very poorly prepared to meet the requirements for secure communications. It seems that up until the Battle of the Marne in 1914 several German Army radio stations went into the field without any provision having been made or even foreseen for the need for crypto-communications. Numerous complaints were registered by German commanders concerning extensive loss of time occasioned by the far too complicated methods officially authorized for use and the consequent necessity for sending messages in the clear. Not only did this reveal intelligence of importance to their opponents but what is equally important, the practice permitted the British and the French to become thoroughly familiar with the German telegraphic procedures, methods of expression, terminology and style, and these items became of great importance in cryptography. For the German Army learned quickly and developed its shortcomings in this area of warfare and began to improve to the point where we must credit the Germans with being the initiators of most of the new and very important developments.
ments in military cryptography. In fact, the develop-
ments and improvements began not long after the out-
break of the Great War and continued steadily until the end. When
on 11 November 1918 the armistice ended active operations,
German military cryptography had attained a remarkably
high state of efficiency. The astonishing fact is that,
although very proficient in cryptographic invention,
they were apparently quite deficient in the science
and practice of cryptanalysis. In all the years since the
end of World War I no books or articles telling of German
success with Allied traffic during that war have appeared
save for one very brief article by a not very bright German
cryptanalyst. One could, of course, assume that they
kept their successes very well hidden, but the German
archives taken at the end of World War II contain
nothing significant in regard to cryptanalysis during
World War I although a great deal of important
information in this field during World War II was
found. A detailed account of the war between the
Allied and German forces in World War II would
require scores of volumes, but [continue over].

In this lecture, however, we are prin-

cipally concerned with German military cryptography
during World War I, and I have already told you
There is one source of information which I can highly recommend to those of you who would like to know more details of the cryptologic warfare between the belligerents in World War I. That source is a book written by a Swedish cryptanalyst, Yves Gylden, under the title "Chifferbyråernas Insatser i Världskriget Till Lands," a translation of which, with some comments of my own in the form of footnotes, you will find on file in the Office of Training, NSA, under the title "The Contribution of the Cryptographic Bureaus in the World War," Government Printing Office, 1956.
something about the cipher systems that were used. It was the German Army which first proved that the old idea that codebooks were impractical for use in the combat zone for tactical communication was wrong. They had two different types of field codes, one we called the "three-number code", the other the "three-letter code". The former was a special code with a large number of words and expressions, which included everything. The "three-number code" was designed for use in all forms of communication within or to and from the 3-kilometer front-line danger zone. Although this code was not put into use until the opening day of the last and greatest German offensive, 10 March 1918, the new code was sent to all four groups in the very same day because an operator who was
Here as on p. 3 DJ
field codes used by the
German Army
unequal to translate a message in the requested and
received a
preparation in the old code, the three-letter code, and i
the latter had been solved to an extent which
made it possible to identify homologous code
groups in both messages. The three-letter proved
rather easy to solve on a daily basis and much
useful intelligence was obtained thereby.

The three-letter code, however, proved
much more difficult. In the first place, it had a
much larger vocabulary, with nulls and many
variants for frequently-used words and numbers;
in the second place and what constituted
just what became the real stumbling block to
solution was the fact that it was a true two-
part randomized or "hatted" code; and in the
third place, each sector of the front used a
different edition of the code, so that traffic
not only had to be identified as to the
sector from which it belonged but also it
was not possible to combine all the messages for
the purpose of building up frequencies of usage
of code groups. Working with the sparse
amount of traffic in a quiet sector of the front
and trying to solve few integrated in the code
was really a painfully slow, very difficult, and
generally frustrating experience. On my reporting for duty Colonel Frank Moorman, who was chief of the whistle unit and whose photograph I show you here, asked me whether I wished to be assigned to the cipher staff section or to the code section. Having had considerable experience with the solution of the former types of cryptosystems but none with the latter, and being desirous of gaining such experience, I chose asked for an assignment to the code polynig unit. I gained the experience I wanted and needed to broaden my cryptology but little did I realize what a painful and frustrating period of learning and training I had undertaken. Still, I have never regretted the choice I made; in fact, it turned out to be a very wise and useful one. If any of you would like to read about my experience in this area, let me refer you to my monograph entitled Field Codes Used by the German Army during the World War. Copies of which are on file in the Office of Training, NSA. I will quote a few [insert]

What sort of cryptosystems did the French Army use? First, as for ciphers, they put
Paragraphs from my "estimate" of the three-letter code, taken as it appears on p. 65 of that monograph.
much trust in transposition methods and here is an example of one type:

As for codes, like the Germans they called their system "Carnot Reducto," they had a small front-line booklet, with different editions of the front and I will show a picture of one of them. Then, in addition, there was a much more extensive code which was not only a two-part, randomized book, but a superencipherment was applied to the code messages when transmitted by radio or "TPS," that is, "telegraphic parcel," or earth telegraphy. Here is one of the tables used for enciphering (and deciphering) the code groups:

And here is the example given in the code in my collection:

You will notice that the enciphering process breaks up the 4-digit groups in a rather clever manner by adding the first digit of the first code group separately: the second and third
digits of the first group are enciphered as a pair, then the last digit of the first group and the first digit of the second code group are enciphered as a pair, and so on. This procedure succeeds in breaking up the code groups in such a manner as to reduce very greatly the frequency of repetition of 4-digit groups representing words, numbers, phrases, etc., of very common occurrence in military messages. My appraisal of this French Army cryptosystem is that it certainly was the most secure of all the systems used by the belligerents, but I don't know how much usage was made of it. I venture the opinion that it was not used often or successfully, with the superenciphering method provided for the basic code.

Now how about the cryptosystems used by the British Army? First, they used the Playfair Cipher, a system of digraphic substitution considered in those days to be good enough for unimportant messages in the combat zone. But today, of course, its security is known to be so low as to be unworthy of placing any reliance in it. The British also used a field code. It contained many common military expressions and sentences, grouped under various
readings or categories, and, of course, a very small vocabulary of frequently used words, numbers, punctuation, etc. It was always used with super
encipherment, the nature of which was not disclosed even to their Allies, so I unfortunately am not in a position to describe it. I don't have a copy of
their code—only a typewritten transcript which was furnished us quite reluctantly, and I will show a typical page thereof.

What about the cryptosystems used by the Italian Army? You may find it hard to believe but it was a simple variant of the very old Vigenere cipher and I show you a picture of it here.

Whether a code book was used in addition, I do not know.
What about the cryptosystems used by the Italian Army in World War I? The general level of cryptologic work during that period was quite low in character, a fact which is all the more remarkable when we consider that the birthplace of modern cryptology was in Italy several centuries before this period. There appears to have been a knowledge of cryptologic techniques in the 15th and 16th centuries than in the 19th paradoxical as this may seem to us today. Perhaps this can be considered as one of the consequences of a policy of secrecy which hides away in dusty archives records of cryptanalytic successes, a desiderata but also prevents those who might have been born with what it takes to develop a skill for cryptologic work from profiting from the progress of predecessors who have been successful in such work. Should we be astonished to learn, therefore, that when Italy entered into World War I the Italian Army put its trust in a very
Simple variation of the ancient Vigenere cipher, a system called the "cifrario militare tascabile" or the "pocket military cipher," as well as several others devised by the same Italian "expert," were solved very easily by the Austrian cryptanalysts during the war. The Italian Army also used codes; no doubt, but since encryption of codes consisted in adding or subtracting a number from the page number on which a given code number group appeared, the security of such systems was quite illusory. As late as in 1927 the Italian "expert" announced his invention of an absolutely indecipherable cipher system which, Ryden says (p.23) "still further demonstrates the astonishing lack of comprehension of modern cryptanalytic methods on this part."

What about Russian cryptologic work in World War I? So far as Russian cryptographic work is concerned we know that there was during Czarist days an apparently well-organized and effective black bureau for diplomatic codes and cipher, organized by a Russian named Savinsky,
formerly Russian minister to Stockholm. He had all codes and ciphers in use up to then improved, introduced strict regulations for their use, and kept close watch over the service. He also was head of a cryptanalytic activity and it is known that Turkish, British, Austrian and Swedish diplomatic messages were solved. After the Bolshevik revolution of 1917, some of the Russian cryptanalysts managed to escape from their homeland and I had the pleasure of meeting and talking with one of the best of them during his service in the black chamber of one of our allies in World War I. He wore with great pride on the index finger of his right hand a ring in which was mounted a beautiful large ruby, the ring having been presented to him by the last Czar in recognition of his cryptanalytic successes while in his service.

But, the story is altogether different as regards cryptology in the Russian army. The military cryptographic service was poorly organized and, besides, it had adopted
a cryptographic system which proved to be too complicated for the ignorant and poorly trained Russians, cipher and radio operators to use when it was placed into effect toward the end of 1914. Here is an example of that cipher, which has an enciphering and a deciphering table.

In the enciphering table, the Russian alphabet in random order appears in the top line; the 2-digit groups within the 8 rows below are their cipher equivalents and these are in random order also. Thus rows therefore constitute a set of 8 cipher alphabets each of which is preceded by a key number from 1 to 8 in random order, also subject to change. Indicators were used to indicate how many letters were enciphered in each alphabet, the indicator consisting of one of the digits from 1 to 9 repeated five times. The alphabets were then used in key-number sequence in enciphering a long message. The cipher operator could change the number of letters enciphered consecutively by inserting another indicator repeated five times, and then continuing with the next alphabet in the sequence of alphabets. The cipher
text was then sent in 5-digit groups. The use of the
deciphering table hardly requires explanation but the
question may be in order: Why to the use of zeros and to the use of double digits
such as 11, 22, 33, etc? This remains a puzzle to me.

I have told you that this cipher system proved too difficult to use, so difficult that
messages had to be repeated over and over, with
great loss of time. It is well known that
the Russians lost the Battle of Tannenberg in
the autumn of 1914 largely because of faulty
communications. Poor cryptography or failure to
use even simple ciphers properly on the field
of battle, and not brilliant strategy on the part of
the enemy, was the cause of Russia’s defeat in that
and in subsequent battles. The contents of Russian communic-
cations became known to the German and Austrian
High Command within a few hours after transmis-
sion. The dispositions and movements of Russian
troops and Russian strategic plans were no secrets
to the enemy. The intercepted and absolutely reliable
information obtained by intercepting and reading the
Russian communications made it very easy for the
German and Austrian commanders not only to take
proper counter-measures to prevent the execution of
Russian plans, but to launch attacks at the
weakest parts of the Russian front. Although the Russian
ciphers were really not complicated, their cipher clerks
and radio operators found themselves unable to exchange
messages with accuracy and speed. As a matter of fact, they
were so exasperated not only were their cipher messages easily solved, but also they made so many errors, that the recipients themselves had considerable difficulty in deciphering the messages even with the correct keys. In some cases this led to the use of plain language, so that the German and Austrian forces did not even have to do anything but intercept the messages and translate the Russians. To pass our dispositions, movements, immediate and long-range plans in plain language was, of course, one cardinal error. Another was to encipher only words and phrases deemed the important ones, leaving the rest in clear. Another cardinal error, made when a cipher was superseded, was to send a message to a unit that had not yet received the new key and then repeat the identical message in the old one. I suppose the Russians committed every error in the catalog of cryptographic crime.

No wonder they lost the Battle of Tannenberg, which one military critic said was not a battle but a massacre, because the Russians lost 100,000 men in the 3-day engagement, on the last day of which the Russian Commander-in-Chief committed suicide. Three weeks later another high Russian commander followed suit.
and the Russian Army began to fall apart, completely disorganized, without leadership or plans. Russia itself began to go down in ruins when its Army, Navy, and Government failed so completely, and this made way for the birth of the October revolution, ushering in a regime that was too weak to put things together again and to hold them together. The remnants, picked up by a small band of fanatics with military and administrative ability, with treachery, violence and cunning, welded together what has now become a mighty adversary of the Western World, the USSR.
I have left to be treated last in this lecture the
cryptosystems used by the American Expeditionary
Forces in Europe during our participation in World War I.

When the contingents of the AEF arrived in France
in the summer of 1917, there were available for secret
communication within the AEF but three authorized means.
The first was that extensive code, the administrative telegraph
 correspondence, the 1915 edition of the War Department
Telegraph Code, about which I have already told you
something. Although it was fairly well adapted for that
type of communication, it was not at all suitable for
rapid and efficient strategic or tactical communications
in the field, nor was it safe to use without a clumsy
surrounding apparatus. The second cryptosystem available
was that known as the repeating-key cipher, which
used the Signal Corps Cipher Disk, the basic principle
of which were described as far back as about the year
1500. The third system available was the Playfair
Cipher, which had been frankly copied from the British
who had used it as a field cipher for many years before
World War I and continued to use it. In addition to
these authorized means there were from time to time
current in the AEF apparently several — how many,
no one knows—authorized, locally—improvised "codes" of varying degrees of security, mostly nil. I show one of these in Fig. 0.0, and will let you assess its security yourself.

Seen in retrospect, when the AEF was first organized, it was certainly unprepared for handling secret communications on the field, but it is certain that it was no more unprepared in this respect than any of the other belligerents upon their respective entries into World War I, as the indicated previously in this lecture. This is rather strange, because never before in the history of warfare had cryptology played so important a role. When measured by today's standards it must be said that not only was the AEF unprepared as to secret communication means and methods and as to cryptanalysis, but for a limited time it seemed almost hopeless that the AEF could catch up with the times, because their British and French allies were at first most reluctant to disclose much of their hard-earned information about these vital matters.

Nevertheless, and despite so inauspicious a commencement, by the time of the Armistice, in
November 1918, not only had the AEF caught up with their allies 
but they had surpassed them in the preparation of sound 
codes, as may be gathered from the fact that their allies 
had by then decided to adopt the AEF system of field 
codes and methods for their preparation, printing, dis-
tribution, and usage.

Just as the invention of Morse wire telegraphy 
had a remarkable effect upon military communications 
during the American Civil War, 
as related in the preceding lecture, so the invention 
of radio also played a very important role in field 
communications during World War II. Now, although 
it can hardly be said that all commanders from the 
very earliest days of the use of radio in military com-
 munications recognized one of the most important 
disadvantages of radio—namely, the fact that radio 
signals may be more or less easily intercepted by the 
enemy—it was not long before the consequences of a 
complete disregard of this obvious fact impressed 
themselves upon most commanders, with the result 
that the transmission of plain language became the 
exception rather than the rule. This gave the most 
monotonous stimulus to the development and increased 
use of cryptology that this service had ever experienced.
Let us review some of the accomplishments of the Code Compilation Service under the Signal Corps, AEF. It was organized in January 1918, and consisted of one captain, three lieutenants and one enlisted man. Until this service was organized, that is, from the summer of 1917 until the end of that year the AEF had nothing for cryptocommunications except those three inadequate means she mentioned. When it had been determined that field codes were needed little time was lost in getting on with the job that had to be done. Since I had no part in this effort I can say without danger of being misunderstood as to motives, that the Code Compilation Service executed the most remarkable job in the history of military cryptography up to the time of World War II.

The first work entrusted to it was the compilation of a first-hand "Trench Code," by which 1000 copies were printed, together with what were called "distortion tables." These were simple monosyllabics for encrypting the 2-letter groups of the code. I show a picture (p. 62) of this code and of one of the "distortion tables."
The danger of capture by these codes was recognized as being such that the books were not issued below battalion. Hence, to meet the needs of the front line, a much smaller book was prepared and printed, called the "Front Line Code." Distortion tables, 30 of them in all, were issued to accompany this code, of which an edition of 3,000 copies was printed—but not distributed, because a study of its security showed defects. AEF cryptographers were groping in the dark, with little or no help from allies and with inexperienced in cryptanalysis. Finally, the light broke through: the Code Compilation Service began to see the advantages of the German 3-letter randomized 24-bit code known as the "Satzbuch." The AEF told you about this code and what the AEF learned about its advantages. Here, then, was the origin of the AEF real Trench Codes—copying from the experience of German code compilation and then going them one better. The first code of the new series, known as the "Potomac Code," the first of the so-called "American River Series," appeared on 24 June 1917, in an edition of 2,000 copies. It contained approximately 1,700 words and phrases and, as the official report
successively states, "was made up with a coding and decoding section in order to reduce the work of the operators at the front." The designation "two-part" or "randomized", or even "hatted" code was still unknown — but the principle was there, nonetheless. Let us see what the official report goes on to say on this point; let us listen to some sound commence pause:

"The main point of difference from other Army codes lay in the principle of reprinting these books at frequent intervals and depending largely upon the rapidity of the reissuance for the secrecy of the codes. This method did away with the double work at the front of ciphering and deciphering [sic!], and put the burden of work upon general headquarters, where it properly belonged. Under this system one issue of codes could be distributed down to regiments; another issue held at Army Headquarters; and a third issue held at General Headquarters. As a matter of record this first book, the Penomac, was captured by the enemy on July 20, just one month after issuance, but within two days, it had been replaced throughout the entire Army in the field."
The replacement code was the Susquehanna, the next in the River Series, followed by the Wabash, Allegheny, and the Hudson, all for the American First Army. In October 1918 a departure in plan was made and different codes were issued simultaneously to the First and Second Armies. This was done in order not to jeopardize unnecessarily the life of the codes by putting in the field at one time 5,000 and 6,000 copies of any one issue. Thus the Champlain, the first of what came to be called the "Lake Series," was issued with the Colorado of the "River Series" for the First Army; these were followed by the Huron and the Osage, the Seneca and the Niagara, in editions of 2,500 each.

In addition to the foregoing series of codes were certain others that should be mentioned, as for example, a short code of 2-letter code groups to be used by front line troops as an emergency code; a short code list for reporting casualties; a telephone code for disguising the names of commanding officers and their units; and so on. But there was in addition to all the foregoing one large code that must be mentioned, a code to meet the requirements for secure transmission of message among the higher commands.
in the field and between the EAB and 21NA. This was a test of considerable magnitude and required several months' study of messages, confidential papers concerning organization, replacement, operations, and military documents of all sorts. The code was to be known as the AEF Staff Code. In May 1918 the manuscript of this code was sent to press and the printing job was done in one month by the printing facilities of the AEF Adjutant General. Considering that the code contained approximately 30,000 words and phrases, accompanied by code groups consisting of 5-figure groups and 4-letter groups, the task completed represents a remarkable achievement by field printing organization and I believe that this was the largest and most comprehensive codebook ever printed by an army in the field. More than 50,000 telegraphic combinations were sent in tests in order to test out combinations liable to error in transmission. One thousand copies of this code were printed and bound. With this code as a superen.wikipedia system there were issued from time to time "distortion tables." There remain only to be said that the war was over before this.
code could be given a good work-out, but I have no doubt that during the few months it was in effect it served a very useful purpose. Moreover, the excellent vocabulary was later used as a skeleton for a new War Department Telegraph Code to replace the edition of 1915.

One more code remains to be mentioned: a "Radio Service Code," the first of its kind in the American Army. This was prepared in October to be used instead of a French code of similar nature. Finally, anticipating the possible requirement for codes for use by the Army of Occupation, a series of three small codes, identical in format with the war-time trench codes of the river and lake series, was prepared and printed. They were named simply Field Codes No. 1, 2, and 3, but were never issued because there was turned out to be no need for them in the quietude in Germany after the Army of Occupation marched into former enemy territory but now very friendly territory.

I will bring this lecture to a close now by referring those of you who might wish to learn more about the successes and exploits of the cryptographic organization of the AEF.
In World War I to my monograph entitled American Army Field Codes in the American Expedi-tionary Forces during the First World War Government Printing Office, 1942. In that monograph you will find many details of interest which I have had to omit in this talk, together with many photographs of codes and ciphers produced and used not only by the AEF but also by our allies and enemies during that conflict.

1. Converter M-134 A—On 25 July 1933 a secret patent application (Serial No. 682,096) was filed by the Chief Signal Officer, on my behalf, covering Converter M-134-T2, the predecessor of Converter M-134 C (Sigaba). The principle disclosed in Serial No 682,096 is of highest importance in that it was the first invention and disclosure covering Electrical control (as distinguished from mechanical control) of a set of cipher rotors in cascade, permitting a departure from the regular and periodic or metric angular displacements of such cipher rotors.

The following is quoted from a Secret Navy report† on the history of the development of the Sigaba (ECM):

"However, under date of 25 July 1933, The Chief Signal Officer filed on behalf of Friedman a patent application (Serial No. 682,096) covering a cryptographic system and machine in which the stepping of the code wheels was very irregular and under the control of a keying tape. Electric Control thus made its first appearance!"

A complete assignment of all rights to my invention was made to the Secretary of War on 10 September 1936, and the patent application was placed in the secret category on 9 September 1936, where it still remains.

Two service test models of Converter M-134-T2 were constructed by the Signal Corps Laboratories at Fort Monmouth, New Jersey in 1936 and service tests were conducted by an exchange of cryptograms between the War Department, Washington, and The Panama Canal Department, Balboa, C.Z., in November 1936. It demonstrated that the machine was operable at the rate of 30-35 words per minute and afforded the highest degree of security yet attained by any cryptographic machine for cryptonet communication (multiple holders of the same cryptographic key).

On 19 February 1937 the military characteristics of Converter M-134 were approved, soon thereafter a contract for the construction of 12 machines was placed with Wallace and Tiernan, Indiana, of Belleville, New Jersey. The machines were delivered to Washington on 2 August 1938.

I developed and wrote the cryptographic keying instructions and in October 1938 first shipment was made of the machines, two each, for the Headquarters of the Ninth Corps Area (San Francisco), Panama Canal, Hawaiian, and Philippine Departments. Four machines were kept in Washington. The machines were promptly put into service for all the highly secret communications between the War Department and the headquarters indicated. Later, as more machines became available, a further distribution was made to equip all Corps Areas and Departments, including the Puerto Rican, with a sufficient number of machines to meet...

† See Enclosure labelled "Exhibit A"
requirements. Eight machines were placed in the War Department Code Center. Only 75 of these machines were built in all but they formed the backbone of the equipment for high command secret and confidential communications of the War Department and the Army from the date of their introduction into service until the end of 1941, when they were replaced by Converter M-134-C, the Sigaba. In 1940 the War Department sent by special officer courier two of these machines to the U. S. Military Attache in London, to meet the very urgent needs for high speed, high-security communication between Washington and London. Later two more were sent there, making four for the Military Attache.

On 29 November 1941 the War Department provided the Department of State with four machines, two for Washington and two for the American Embassy in London; later on, four or more additional machines were provided the Department of State. During the vital years 1940-1942, confidential and secret intercommunication between these two points and among the offices indicated could not have been successfully conducted without these machines.

In January 1942 arrangements were made to use the M-134-A for direct communication between the President and the British Prime Minister and it was used for this purpose for a number of months. Later this machine in that circuit was replaced by Converter M-134 C, in a special adapter made under my supervision by the Signal Corps and the Western Union. This permitted of high speed, secure communication between the White House and Downing Street at a very critical period.

The M-134 was also used to a large degree by the Signal Intelligence Service itself for forwarding intercept traffic to Washington from overseas intercept stations. It replaced Cipher Device M-138 for this purpose and thus greatly facilitated the prompt receipt of the raw traffic for cryptanalysis.

Later on, a number of them (totaling 29 or 30 at the end) as they became available, were provided the Office of the Coordinator of Information (later the Office of Strategic Services) for secret communication between Washington, London and other capitals where the OSS maintained headquarters. Some of these machines (about 16) maybe and probably are still in service.

During the years from 1939 to 1942, when Converter M-134 was replaced by Converter M-134-C (Sigaba) it is doubtful if the voluminous secret and confidential traffic of the highest echelons of the Army and the War Department could have been handled as successfully as it was, had it not been for the invention, development and availability of this machine.

There is not a scrap of evidence in Ticom reports that either the Germans or the Japanese or any other government was able to solve any of the traffic enciphered by this machine.
2. Converter M-134-C (Sigaba).—In the course of studies of Converter M-134-T2 and before manufacture of the latter machine was well under way, my principal assistant, Mr. Frank B. Rowlett, and I investigated various means of improving the cryptographic machine with a view to eliminating the perforated tape which controlled the aperiodic stepping of the rotors. Various schemes were studied, including cam wheels with different diameters and variable "off" and "on" pin arrangements. About 15 June 1935 Rowlett conceived an idea which finally resulted in making it possible to eliminate the tape control. Basically his invention was that of using a set of rotors as a key generator, that is, using the rotors to generate a long keying sequence by sending electrical impulses through a set of rotors which themselves were caused to step in a regular manner. The successive elements of the keying sequence, as they were generated could control the stepping of the rotors actually employed to encipher the letters of the message to be enciphered. Rowlett and I then jointly developed the idea by setting down on paper various methods by which it could be applied to replace the tape control employed in Converter M-134-T2, and although no models were built the results of our theoretical studies were incorporated in a patent application filed on 23 March 1936 (Serial No. 70,412) in our name as joint inventors. A complete assignment of the invention to the Secretary of War was made on 2 April 1936 and the patent application was placed in the secret category, where it still remains.

The Navy was then trying to improve its own machine (Mark I E C M), the security of which was unsatisfactory. Though this machine generated a long keying sequence the number of available starting points in that sequence was so limited that considerable "depth", that is, messages enciphered in exactly the same key, could be expected every day and thus solution potentially made relatively easy. On three occasions, at Navy request, the drawings and principles later embodied in Serial No. 70,412 were shown and explained to Navy representatives several times in October and November of 1935, with the result that the Navy initiated a development contract with the Teletype Corporation and work thereon was started in January 1938. This was done, however, without advising us or anybody else in the Signal Corps until March 1939, when the Teletype Corporation engineers brought to Washington the first completed set of drawings of the Mark II E C M. Rowlett and I were invited to the conference with the Teletype engineers and in the course of the discussions it was brought out and acknowledged that the Navy had based the cryptographic features of the new machine upon the Army's disclosure. A first model was then built and delivered on 3 February 1940, when Major General Mauborgne, then Chief Signal Officer, Rowlett, and I were invited by Admiral Noyes and Captain Safford to see the model. On that occasion Captain Safford acknowledged, in the presence of all those witnessing the demonstration, the fact that the Navy had used the Friedman-Rolett invention. Further development of the machine was thereafter on a joint Army-Navy basis, and on 19 June 1940 the Signal Corps added its order of an initial 85 machines to the Navy order, at a cost of $1856.90 each.
The Mark II ECM (Navy nomenclature)—Converter M-134-C was adopted by the Army to replace Converter M-134 A, not because the former might afford greater security than the latter but because the M-134 C was not only a much more rugged, reliable and rapid machine but also because it dispensed with perforated tapes, thus being more practical than the M-134 C. The following is quoted from the Navy Department's "History of the ECM:"

"Electric control of the ECM by means of the Friedman-Rowlett 'Stepping Maze' is the essential feature that places the Mark II ECM in a class by itself as regards security."

On 17 March 1941 the first 10 machines were delivered to the Signal Corps and were given a prompt service test, which proved the machines to be highly satisfactory. On 4 October 1940 action was initiated by the Signal Corps to procure an additional 149 machines, and thereafter, in successive contracts several thousand more of them were procured, the production schedule in July 1942 calling for the delivery of the machines to the Signal Corps at the rate of 150 per month. By 31 August 1942 a total of 373 Sigabas had been delivered and 364 were already in service; by 30 April 1943 the total number ordered was 1867, the number delivered was 862, and the number in use 807; by 28 March 1944 a total of 333 machines had been ordered, 1827 delivered, and 1681 were in service. In all, the Signal Corps actually procured a total of 3392 of these machines for Army use, and the Navy procured more than that number for Navy use. In the Army the machines were distributed to all commands down to and including headquarters of Divisions. They were also used in all the important fixed headquarters in the Communications Zone, in all theaters and in the U. S. Under special precautions they were used in U. S. installations in foreign countries where we had no troops, as for example, in Moscow, for our special military mission. Whenever and wherever the late President went during the war, the Sigaba went too. They were installed in the late President's signal center whenever he visited his home at Hyde Park; they were on board the Presidential Train, etc.

The fact that identical machines were employed by the Army and the Navy at all high and intermediate headquarters not only speeded up the exchange of classified messages of all categories (secret, confidential, and restricted) within each of the Services but also facilitated Joint Communications. The following is also quoted from the Navy's History of the ECM:

"This use of an identical machine with interchangeable code wheels has been of great military value, particularly in the early stages of the war, when distribution of machines and code wheels was incomplete. In the Philippines, Java, Australia, and even in North Africa, Navy wheels have been used in Army ECM's, Army Wheels in Navy ECM's; machines have been borrowed back and forth between the two services; Army messages have been sent in Navy ECM ciphers and Navy messages sent in Army ECM ciphers."
We know now from Ticom reports that neither the Japanese nor the Germans had the slightest success in their efforts to solve messages in the Sigaba, though the Germans certainly tried hard enough. The absolute security of Army and Navy high command and high echelon communications throughout the war was made possible by the Sigaba. In view of the fact that the high-level communications of the German, Italian, and Japanese Governments and Armed Forces were successfully attacked by the U. S. and the British communications intelligence staffs, and that the intelligence resulting therefrom was of highest diplomatic, strategic, and tactical importance, whereas our own high-level communications were inviolate, it may be said that the Sigaba contributed materially to the successful outcome of the war.

3. **Converter M-228 (Sigcum, Sighuad).**—The need for a cryptographic mechanism to protect land-lines teletype communications was felt even in World War I. In 1936 the Army was anxious to have something practical developed for this purpose and studies that had been underway for a number of years culminated in 1939, when Rowlett and I, applying Rowlett's idea of using cascade rotors as a key generator, then jointly conceived the principles underlying what later became Converter M-228 (Sigcum). Patent Application Serial No. 443,320 was filed on 16 May 1942; assignment of rights to the Secretary of War was signed on 13 May 1942 and the application was placed in the Secret category, where it still remains.

On 16 July 1941 military characteristics were approved by The Adjutant General and the Signal Corps Laboratories at Fort Monmouth, New Jersey, undertook the development. On 12 March 1942 a satisfactory service test and working demonstration of the first two models of Converter M-228 was made; one machine was at Fort Monmouth, the other at the Bell Laboratories, New York City. The provided for automatic on-line keyboard encipherment, transmission, reception, decipherment and printing of messages at the rate of over 360 characters (= approximately 60 words) per minute, with good security.

On 7 April 1942 the budget for FY 1943 included provision for procurement of 2400 machines at $500 each, a total of $1,200,000.

On 18 June 1942 representatives of the Signal Corps and the Navy witnessed a demonstration of the machine in New York and as a result the Navy decided to procure 200 for its use.

On 24 November 1942 action was initiated to purchase 1467 machines and on 25 December the first 10 machines were shipped from the factory to Washington.
Although Converter M-228 was not intended for radio-teletype usage, the urgent need for speed in overseas communications and the availability of radio-teletype circuits practically forced the use of the machine on these circuits to protect these communications. On 9 January 1943, the first official message using Converter M-228 on a radio circuit was sent from Washington to Algiers, and thereafter extensive use of the machines for radio-teletype communications was made, although it was decided, for security reasons, to transmit only confidential and restricted messages by this means. (Secret and Top Secret Messages had to be enciphered by Sigaba or by Sigtot, the one-time tape System).

By 11 September 1943 a total of 3867 machines had been ordered, and 3044 had been manufactured. The rate of production was 500 per month. By that date the "stop-gap" teletype-encipherment system using two short loops of key tape was discontinued, because general distribution of the M-228 had been completed. On 31 May 1943 the A. C. of S., G-2, War Department, approved the installation of this machine for use on the Defense Teletypewriter Network linking the several U. S. Army Headquarters in the United Kingdom.

In April 1944 the War Department approved a policy under which the machine could be turned over to the British for the specific purpose of use in Combined Operations; and on 23 May 1944 the A. C. of S., G-2, War Department, approved disclosure of the principles of the machine to the British.

By 5 June 1944 a total of 3200 of these machines had been built and 1488 issued for use, including 200 to the Navy. The machine was employed to encipher a tremendous volume of traffic, including raw material for cryptanalysis from all intercept stations. Under the special conditions and with some modification (Sighuad) the machine was also used in special circuits in Washington, between Arlington Hall Station, the Military Intelligence Service in The Pentagon, of the highest classification. This same modification (Sighuad) permitted the machine to be used by the Air Forces in the U. S. and in the Pacific, to transmit, by radio meteorological and weather data, thus greatly facilitating operations.

The British did not have any machine similar to the Sigcum or Sighuad and only at the end of the war was their long-standing desire to be able to use it granted. The Germans had teletype encipherment equipment but a large volume of traffic in the various types of machines they built was solved and read on a current basis by the British. Toward the end of the war the Germans had improved models which resisted solution, but they came too late. The Japanese had no such equipment at all.
Results of Ticom operations have established that neither the Germans nor the Japanese were successful in their efforts to solve our Sigcum traffic, despite its great volume, and it is my belief that had we used this machine for secret radio-teletype communications no serious harm to our security would have followed. Although it was not used for secret radio-teletype communications, the machine was nevertheless widely used for secret, confidential, and restricted communications by land-line teletype and for a great volume of confidential and restricted communications by radio-teletype in the U. S. as well as in all overseas theaters. The Sighuad version of this machine was, however, used to a limited extent for secret traffic by radio. Had we not possessed such a machine our rapid communications would have been severely handicapped by the necessity of encipherment by slower means.

4. Cipher Device Type M-138.—Early experiments with the old cylindrical Cipher Device M-94, which had been introduced into the U. S. Army and U. S. Navy in about 1922, began in about 1933. Various modifications, in the form of a flat cipher device using variable, instead of fixed alphabets, were made, culminating in a device on which a patent application in my name was filed (Serial No. 300,212) on 19 October 1939. On 16 July 1940 the application, which the usual license rights were assigned to the Government on 16 October 1939, was placed in the secret category under the provisions of the Act of 6 October 1917 as amended 2 July 1940.

About five thousands of these devices were manufactured under War Department Contracts. They were used throughout the war and are still used by a large number of military fixed and mobile headquarters. In fact, until the manufacture of the automatic cipher machine (Sigaba) had progressed to the point where a sufficient number had been produced to meet distribution requirements, the Strip Cipher System using Cipher Device M-138 formed the backbone of Army Secret and Confidential communications; thereafter it served and still serves as the secondary or back-up system for the holders of the Sigaba. For stations not equipped with the Sigaba the Strip Cipher System still constitutes the principal means for such communications. At the present in the U. S. all Posts, Camps and Stations use this device as the primary cryptographic means. Until recently it was also the primary means for communication between the War Department and all Military Attaches as well as for intercommunication among military attaches; at present it is employed only for circular messages to or among military attaches.

The same device was also provided by the War Department in large quantities for use by the Department of State, for Secret and Confidential Communications between that Department and its Embassies, Legations, and Consulates, as well as for intercommunication among those offices.
Certain Allied Services, such as the British, Italian, and Russian were also provided with these devices in small quantities both by the War and the Navy Departments. The U.S. Navy also adopted the device at first in practically identical form; the Navy produced some minor improvements later on and employed and is still employing the device very extensively in its own communications. In addition the Strip Cipher System was used during the war as a Joint Army-Navy system and as a Combined System. The fact that the same device was used by both the Army and the Navy greatly facilitated Joint Communications. The production of the paper strips bearing the variable cipher alphabets employed in the device presented numerous problems which were successfully solved by me or by people under my direction. I conceived the first rotary cutter for cutting the strips apart and had the first cutter built at the Government Printing Office. This machine greatly facilitated the production of the strips and made the matter practical.

5. General.—Throughout the years mentioned, in my capacity as Head Cryptanalyst and later as the Director of Communications Research, many problems directly related to our communications security were brought to my attention and I believe that my long experience in the field formed a solid foundation for mature, sound judgment in arriving at proper, practical, and satisfactory answers to those problems.

Before our Converter M-228 was ready for distribution the urgent need for a means of enciphering teletype communications for the Military Intelligence network in the United States led to my suggesting the adoption of a temporary expedient for this purpose. This took the form of double-loop, key-tape encipherment system which had been tried out in a small way at the end of World War I. Having studied this method in 1919-1921 and knowing the pitfalls to which such a system is subject from the security point of view, I was able to suggest ways of usage to minimize the dangers inherent in a double-tape encipherment method. The system was used for a number of months not only within the U.S. but also within theaters of operations, thus meeting an urgent need for teletype encipherment until the M-228 was ready for distribution.

Later on, when the one-time tape or Sigtot System was being considered for secret and top secret radio-teletype communications, I was consulted and in view of my experience with all preceding teletype encipherment systems was able to give technical approval on the new proposal and to insure that the production of keying tapes was properly safeguarded.
For a number of years prior to 1941 I had been more or less intensively studying all the various cryptographic devices and machines which had been invented and produced by private inventors both in the United States and in foreign countries. Files of patents issued domestically and abroad were kept, and theoretical studies made to ascertain the security of the products of invention in this field.

This resulted in improvements in the security of the machine and led finally to the adoption of Converter M-209 as a field instrument. Over 100,000 of them were manufactured, and used by both the Army and the Navy. While the machine was by no means perfect, it met a need that could hardly have been fulfilled otherwise.

For a number of years I served on the Joint and the Combined Codes and Ciphers Committee and the Joint and Combined Security Committee. I was a member of a special Ad Hoc Committee, consisting of two Navy officers, General (then Colonel) Corderman, and myself, appointed by the Joint Communications Board in 1944 to investigate the security of communications in all non-military bureaus and departments of the Government, making recommendations for improvement therein. The deliberations of the Ad Hoc Committee resulted in the establishment, by President Truman, of the Cryptographic Security Board for U.S. Government communications, consisting of the Secretaries of the three Departments, State, War, and Navy.

As technical adviser to the Chief, Signal Security Agency and to the Chief of the Security Division, I was constantly consulted by them in connection with the many problems affecting communications security. I also served in an advisory capacity in connection with all research and development of communications security equipment, including ciphony and cifax. One of my important contributions in this capacity was to urge the development of the voice security equipment, now known as the Sigsaly system, at a time when that project had been practically abandoned.

The new Synchronous Polarity Reversal System of Cifax recently developed by us is based upon an invention of mine (Serial No. 478,193) filed on 3 June 1943 and assigned to the Secretary of War on 18 October 1943. Lieutenant Colonel Rosen's invention of the important feature whereby the polarity reversals in the interaction of keying and picture elements are synchronized made the system practical and highly secure; in fact, there is reason to believe that the security of cifax transmissions by the Friedman-Rosen inventions can be made almost absolute.
In 1941 I undertook a study of the general basis of the distribution of Army cryptographic systems, evolving the new idea of "cryptonets", and thus improving security of communications. By isolating cryptographic systems according to levels of command and reducing the amount of intranet traffic within any one system, the security of all systems is enhanced at the same time that provision is made for inter-net traffic. The cryptonet system has worked in a highly satisfactory manner in practice.

B. Important Contributions to Communications Intelligence, 1939-1945

1. Solution of Japanese Diplomatic Communications.—On February 1939 the Japanese Foreign Office began using a new machine called by them the "B-Machine" for the highly secret communications between Tokyo and its embassies throughout the world. We had been successfully solving and reading practically all of the communications of the Japanese Foreign Office up to that time; many of them were in a machine ("A Machine") which we had also solved and reconstructed by pure analysis in about the year 1937, but a large number were also in hand operated systems involving a small code, superenciphered by various schemes, usually transposition.

The urgency of solution of the new machine, in view of the increasingly difficult relations between the United States and Japan, was apparent. However, in view of the small number of trained cryptanalysts available, the pressure of work in the sections operating on currently readable systems and in the sections producing our own codes, ciphers, and key lists, the number of people who could be placed on this new and very difficult problem was very limited. By August 1939, no important progress having been made, the Chief Signal Officer directed that I drop, so far as practicable, certain administrative duties as assistant chief of Signal Intelligence Service (Major W. O. Reeder had been brought in as officer in charge in April 1938) and to participate actively in the studies of the "B Machine," in addition to generally supervising the technical cryptanalytic and cryptographic work of the office. Thus, from that month until success was attained, the "B-Machine" studies were under my active supervision but at the same time I had to carry on some other duties from which, it was impracticable to relieve me.

By the end of 1939, the machine having been in use almost a full year, hundreds of messages had accumulated; very occasionally a tiny fragment of a message was read; rarely, longer fragments. But no message was read in its entirety. Nevertheless important progress had been made. Intensive work was continued by me and my technical staff.
of half a dozen cryptanalysts, with the clerical assistance of another half dozen people, and the occasional assistance of our two Japanese translators. On 20 September 1940 came the very first indication that we were on the right path and might be successful in solving the machine; under the pressure of great excitement, working almost day and night, by 27 September the first two translations representing the very first actual solution to the B-Machine were sent to G-2.

There remained, however, much work to be done, since only the data applicable to but one out of the whole set of 120 indicators were at hand. By 14 October 1940 solutions for over one-third of the 120 indicators were available and certain current messages could be read.

By careful analytical reasoning, by studying the external cryptographic phenomena manifested by the system, by correct reasoning and a knowledge of cryptographic mechanisms, the principles underlying the cryptographic functioning of the B-Machine were soon derived by induction and deduction. A hand-operated, crude model using flashlight bulbs was hurriedly constructed, while at the same time parts were ordered for two fully automatic, keyboard-operated machines, which were then constructed as rapidly as possible. All of this work also was under my general direction as Principal Cryptanalyst. By November 1940 the two fully automatic machines had been constructed and were in successful operation. We had, it is true, reconstructed the Japanese "A-machine" by pure analysis, too, but so far as I am aware, this is the first time in cryptanalytic history that a machine capable of deciphering traffic of the complexity of that produced by the Japanese B-Machine was completely reconstructed by pure analysis. When we began the study we had no inkling as to the nature of the machine; soon thereafter we had ascertained that the cryptographic textual letters fell into two classes, but to this day we have never seen a complete Japanese machine in working order. Some time in 1942, long after our work of analysis had been completed, we did see the smashed, burned and almost unrecognizable remains of a B-Machine which the Japanese had destroyed on or about 5 December 1941 in Mexico and which remains came into possession of the F. B. I., who were anxious to reconstruct the machine if possible; also, and as a result of European Ticom operations, we did find two or three of the rotary-switch assemblies in a box taken from the ruins of the Japanese Embassy in Berlin, but of course these glimpses of one of the most important elements of the machine were by this time only of academic interest.

In January 1941 a Joint Army-Navy Cryptanalytic Mission to GC and CS took with it one machine and a complete story of how to decipher diplomatic messages enciphered by the Japanese B-Machine. This system was one of the very few which had resisted all of GC and CS efforts to solve it.
As to the importance of the solution of the B-Machine, or Purple System, as it was designated soon after solution, I need only refer to the disclosures of the current Joint Congressional Investigation of the attack on Pearl Harbor and to certain statements relative to the solution of the Japanese diplomatic machine contained in the letter dated 27 September 1944, which the Chief of Staff sent to Mr. Dewey, a copy of which is attached hereto. While that solution represents the achievement of a cooperative effort by a number of people, it was made possible by good coordination and proper technical direction of a fair number of skilled cryptanalytic personnel who were selected and trained by me and who worked under my direction for over 18 months as a harmonious team. In addition, certain of the cryptographic phenomena which ultimately led to the solution were uncovered by me in the course of those studies. A more detailed history of the solution is attached hereto.

We know that the German cryptanalytic staffs tried to solve the B-Machine and failed; as noted above, even as competent as was the British staff, it also failed to solve this machine and we gave them the solution. There is reason to believe that the Russian staff did not succeed, if they even undertook the problem, which we do not know. I believe it is true that as a result of our reading certain messages early in 1941 the State Department was able to give the Russian Government early information as to the coming secret offensive by the Germans, which began on 21 June 1941. Had the Russians been able to read the Purple, this would not have been necessary. As to the Japanese diplomatic communications in other systems, their messages in those systems were being read as promptly as facilities and personnel permitted, with priority being given those in the Purple System, although many important messages were also read in the various other systems, such as PA-K2, CA, and LA.

2. General.—As Head Cryptanalyst in the years 1939-1941, I was in technical charge of a staff of people numbering several thousand, working on all problems in the communications intelligence field, and also supervised the selection and training of new personnel. Some of the problems being worked on during those years and successful in their outcome were those involving the diplomatic communications of several other governments than the Japanese such as the Italian, German, and Mexican. During the succeeding years, 1941-1945, the Agency accomplished many feats in cryptanalysis, too numerous to mention.

The diplomatic communications of many countries were read, some almost in toto; the communications of the Japanese Army and Air Force were read to a very large degree, contributing greatly to our victory in the Pacific.
The extent to which the Agency engaged in the research, development, and use of high speed analytic equipments to facilitate the application of cryptanalytic techniques and processing is worthy of mention and my technical advice and collaboration was used in all these cases. I was largely responsible for urging the development of the "oo3" equipment and had general supervision over its design, construction, and installation by the Bell Telephone Laboratories and the Western Electric Company. The fruits of that equipment and the modifications which followed and which were applied to the solution of German Enigma traffic represent some of the best achievements of the Agency. Our important developments in the field of photo-electric rapid analytical machinery also resulted from my insistence upon embarking upon such developments. In all these matters my advice was sought and obtained by the Chief of the Agency and special reports were prepared for him from time to time on these subjects. These equipments aided considerably in the solution of the diplomatic and military communications which were worked on by the Agency.
Introduction to Cryptology - IV

BY WILLIAM F. FRIEDMAN

Confidential

Cryptology in the Civil War.

A detailed account of the...

[Handwritten notes: "National War College"]

Approved for Release by NSA on 04-15-2014 pursuant to E.O. 13526
This lecture, the fourth in the series, deals with the crypto-
systems used by both sides in the Civil War, the War of the Rebellion,
the War Between the States - choose your own designation for that
vicious, bloody, and very costly strife, when brother was pitted against
brother. Civil strife is unhappily always very bitter and leaves scars
which heal only extremely slowly with the passage of many years.

A detailed account of the codes and ciphers of the Civil War in
the United States of America can hardly be told without beginning
with a bit of biography about the man who became the first signal officer
in history and the first Chief Signal Officer of the United States Army,
Albert J. Myer, the man in whose memory that lovely little U.S. Army
post adjacent to Arlington Cemetery was named. Myer was born on 20 Sep-
tember 1827. After an apprenticeship in the then quite new science of
electric telegraphy at Morse's Patent U.S. Office in 1847, he entered
Hobart College, Geneva, New York, from which he was graduated in 1847.
From early youth he had exhibited a predilection for artistic and scien-
tific studies, and upon leaving Hobart he entered Buffalo Medical College,
receiving the M.D. degree four years later. His graduation thesis, "A
Sign Language for Deaf Mutes," contained the germ of the idea he was
to develop several years later, when, in 1854, he was commissioned a
1st Lieutenant in the Regular Army, made an Assistant Surgeon, and ordered
to New Mexico for duty. Myer's idea involved the development of an
efficient system of military "aerial telegraphy", which was what systems
of visual signaling were then called. He had plenty of time at this
distant outpost to think about this. I emphasize the word "system"
because, strange to say, although instances of the use of lights and other
visual signals can be found throughout the history of warfare, and their
use between ships at sea had been practiced by mariners
for centuries, yet down to the middle of the 19th Century surprisingly
little progress had been made in developing methods and instruments for
the systematic exchange of military information and instructions in the
system of electric
means by means of signals of any kind. Morse's practical telegraphy,
developed in the years 1832-35, served to focus attention within the military systems and methods upon the matter of inter-communication by means of both visual and electrical signals, and in the years immediately preceding the Civil War, the U.S. Army took steps to introduce and to develop a system of visual signaling for general use in the field. It was Assistant Surgeon Myer who furnished the initiative in this matter.

In 1856, two years after he was commissioned assistant surgeon, and had devoted much of his leisure time to the study of visual signaling and its development, Myer drafted a memorandum on a new system of visual signaling was obtained a patent on it. Two years later, a board appointed by the War Department to study Myer's system reported favorably. After some demonstrations by Myer, and after various the War Department fostered a bill in Congress, which gave its approval to the system. But what is more to the point, Congress appropriated an initial amount of $2,000 to enable the Army and the War Department to develop the system. The money, as stated in the Act was to be used "for the manufacture of purchase of apparatus and equipment for field signaling." The act also contained another important provision: it authorized the appointment, on the Army staff, of one Signal Officer with the rank, pay, and allowances of a major of cavalry. On 2 July 1860, "Assistant Surgeon Albert J. Myer (was appointed) to be Signal Officer, with the rank of Major, 27 June 1860, to fill an original vacancy." Two weeks later Major Myer was ordered to report to the Commanding General of the Department of New Mexico for signaling duty. The War Department also directed that two officers be detailed as his assistants. During a several months' campaign against hostile Navajos, an extensive test of Myer's new system, using both flags and torches, was conducted with much success. In October 1860, a Lieut. J.E.B. Stuart, later to become famous as a Confederate cavalry leader, tendered his services to aid in signal instruction; interest in demonstrating his system before the board, which made a study of Myer's system before it was adopted by the Army, was a Lieut. E.P. Alexander, Corps of Engineers. We shall hear more about him presently, but at the moment I will say that on the outbreak of the War, Alexander organized the Confederate Signal Corps, which was established by the Act of the Confederate Congress: "To organize a Signal Corps." The Act was approved on 17 April 1862 -- nearly a year earlier than the Signal Corps of the Federal Army was likewise established as a separate service.
Less than a year after Major Myer was appointed as the first and, at that time, the only Signal Officer of the U.S. Army, Fort Sumter was attacked and, after a 36-hour bombardment, surrendered. The bloody four-year war between the North and the South began. The date was 14 April 1861. Myer's system of aerial telegraphy was soon to undergo its real baptism under fire, rather than by fire. But with the outbreak of war, another new system of military signal communication, signaling by the electric telegraph, began to undergo its first thorough test in combat operations. This in itself is very important in the history of cryptography. But far more significant in that history is the fact I mentioned at the close of the last lecture, viz., that for the first time in the conduct of organized warfare, rapid and secret military communications on a large scale became practicable, because cryptography and electric telegraph were now to be joined in a continuous, but lasting weld. For when the war began, the electric telegraph had been in use for less than a quarter of a century. Although the first use of electric telegraphy in military operations was in the Crimean War in Europe (1854-55), its employment was restricted to communications exchanged among headquarters of the Allies, and some observers were very doubtful about its utility even for this limited usage. It may also be noted that in the annals of that war there is no record of the employment of electric telegraphy together with means for protecting the messages against their interception and solution by the enemy.

On the Union side in the Civil War, military signal operations began with Major Myer's arrival in Washington on 3 June 1861. His basic equipment consisted of kits containing a white flag with a red square in the center for use against a dark background; a red flag with a white square for use against a light background; and torches for night use. It is interesting to note that these are the elements which make up the familiar insignia of our Army Signal Corps. The most pressing need which faced Major Myer was to get officers and men detailed to him wherever signals might be required, and to train them in what would come to be called the "vigor system," of which are depicted in Fig. 1. This training included learning something about codes and ciphers, and gaining experience in their usages.

But there was still no such separate entity as a Signal Corps of the Army. Officers and enlisted men were merely detailed for service with Major Myer for signaling duty. It was not until two years after the war started that the Signal Corps was officially established and organized as a separate branch of the Army, by appropriate Congressional action. In the meantime, another signaling organization was coming into being — an organization which was an outgrowth of the
government's taking over control of the commercial telegraph companies in the United States on 25 February 1862. There were then only three in number: the American, Western Union, and Southwestern. The telegraph lines generally followed the railroads. The then Secretary of War, Simon Cameron, sought the aid of Thomas A. Scott, of the Pennsylvania Railroad, who brought some of his men to Washington for railroad and telegraphic duties with the Federal Government. From a nucleus of four young telegraph operators grew a rather large military telegraph organisation which was not given formal status until on 28 October 1861 President Lincoln gave Secretary Cameron authority to set up the U.S. Military Telegraph Department under a man named Anson Stager, who, as general superintendent of the Western Union was called to Washington, commissioned a captain (later a colonel) in the Quartermaster Corps, and made superintendent of the Military Telegraph Department. Only about a dozen of the members of the Department became commissioned officers, and they were made officers so that they could receive and disburse funds and property. All the rest were civilians. The U.S. Military Telegraph "Corps", as it soon came to be designated, without warrant, was technically under Quartermaster, but for all practical purposes it was under the immediate and direct control of the Secretary of War, a situation admittedly acceptable to Meigs. There were now two organizations for signaling in the Army, and it was hardly to be expected that no difficulties would ensue from the duality. In fact, the difficulties began very soon, as can be noted in the following extract from a lecture before the Washington Civil War Round Table, early in 1954, by Dr. George R. Thompson, Chief of the Historical Division of the Office of the Chief Signal Officer of the U.S. Army:

The first need for military signals arose at the important Federal fortress in the lower Chesapeake Bay at Fort Monroe. Early in June, Meier arrived there, obtained a detail of officers and men and began schooling them. Soon his pupils were vigwaging messages from a small boat, directing the fire of Union batteries located on an islet in Hampton Roads against Confederate fortifications near Norfolk. Very soon, too, Meier began encountering trouble with commercial wire telegraphers in the area. General Ben Butler, commanding the Federal Department in southeast Virginia, ordered that wire telegraph facilities and their civilian workers be placed under the signal officer. The civilians, proud and jealous of their skills in electrical magic, objected in no uncertain terms and shortly an order arrived from the Secretary of War himself who countermanded Butler's instructions. The Army's signal officer was to keep hands off the civilian telegraph even when it served the Army.

Note that at the time of this episode the Signal Officer had no facilities for electric telegraph signaling - he was given control of such facilities in southeast Virginia by the commanding general of the Department, General Butler, and he kept them for only a few hours.
I have purposely selected this extract from Dr. Thompson's presentation because in it we can clearly hear the first rumblings that lengthy and acrimonious feud between two signaling organizations whose uncoordinated operations and rivalry greatly reduced the efficiency of all signaling operations of the Federal Army. As already indicated, one of these organizations was the U.S. Military Telegraph "Corps", hereafter abbreviated as USMTC, a civilian organization which operated the existing commercial telegraph systems for the War Department, under the direct supervision of the Secretary of War, Edwin M. Stanton. The other organization was, of course, the infant Signal Corps of the United States Army, which was not yet even established as a separate branch, whereas the USMTC had been established in October 1861, as noted above. Indeed, the Signal Corps had to wait until March 1863, two years after the outbreak of war, before being established officially.

In this connection it should be noted that the Confederate Signal Corps had been established a full year earlier, in April 1862. Until then, as I've said before, for signaling duty on both sides, there were only officers who were individually and specifically detailed for such duty from other branches of the respective Armies of the North and the South.

Trouble between the USMTC and the Signal Corps of the Union Army began when the Signal Corps became interested in signaling by electric telegraphy and began to acquire facilities therefor.

As early as in June 1861, Chief Signal Officer Myer had initiated action toward acquiring or obtaining electrical telegraph facilities for use in the field but with one exception nothing happened. The exception was in the case of the military department in southeast Virginia, commanded by General Benjamin Butler, an episode that clearly foreshadowed the future feud for the Signal Corps in regard to electrical signaling. The road was to be closed and barred to electrical signaling. The telegraph train, which had been ordered by Myer many months before, was delivered in January 1862 and cut out in an experimental fashion, under considerable difficulties, the most disheartening of which was the active opposition of persons in Washington, particularly the Secretary of War. So, for practicality the whole of the first two years of the war, signal officers on the Northern side had neither electrical telegraph facilities nor Morse operators - they had to rely entirely on the wig-wag system.
However, by the middle of 1863 there were thirty "flying-teleguaph" trains in use in the Federal Army. Here's a picture of such a train. The normal length of field telegraph lines was five to eight miles, though in some cases the instruments had worked at distances as great as twenty miles. But even before the Signal Corps began to acquire these facilities, there had been agitation to have them, as well as their Signal Corps operating personnel, all turned over to the USMTC, which had grown into a tightly-knit organization of over 1,000 men in Washington, and had become very influential especially by virtue of its support from Secretary of War Stanton. As a consequence, the Telegraph-Corps had its way. In the fall of 1863, it took over all the electric telegraph facilities and telegraph operators of the Signal Corps. Colonel Myer sadly wrote: "With the loss of its electric lines the Signal Corps was crippled". 

So now there were two competing signal organizations on the Northern side: The U.S. Army's Signal Corps, which was composed entirely of military personnel with no electric telegraph facilities (but was equipped with means for visual signaling), and the USMTC, which was not a part of the Army, being staffed almost entirely with civilians, and which had electric telegraph facilities and skilled Morse operators (but no means or responsibilities for visual signaling or "serial telegraphy" which, of course, was old stuff) "Electric telegraphy" was now the thing. The USMTC had no desire to share electric telegraphy with the Signal Corps, a determination in which the Corps was most ably assisted by Secretary of War Stanton, for reasons that fall outside the scope of the present lecture.

However, from a technical point of view it is worth going into this rivalry just a bit, if only to note that the personnel of both organizations, the military and the civilian, were not merely signalmen and telegraph operators: they served also as cryptographers and were therefore entrusted with the necessary cipher books and keys. Because of this, they naturally became privy to the important secrets conveyed in cryptographic communications and they therefore enjoyed status as VIP's. This was particularly true of members of the USMTC, because they, and only they, were authorized to be custodians and users of the cipher books, cipher books and keys. Because of this, they naturally became privy to the important secrets conveyed in cryptographic communications and they therefore enjoyed status as VIP's. This was particularly true of members of the USMTC, because they, and only they, were authorized to be custodians and users of the cipher books, cipher books and keys. Not even the commanders of the units they served had access to the cipher books. For instance, on the one and only occasion when General Grant forced his cipher operator, a civilian named Beckwith, to turn over the current cipher to a colonel on Grant's staff, Beckwith was immediately discharged by the Secretary of War and Grant was reprimanded. A few days later, Grant apologized and Beckwith was restored to his position. But Grant never again demanded the cipher held by his telegraph operator.
The Grant-Beckwith affair alone is sufficient to indicate the lengths to which Secretary of War Stanton went to retain control over the USMTC, including its cipher operators, and its cipher book. In fact, so strong a position did he take that on 10 November 1863, following a disagreement over who should operate and control all the military telegraph lines, Myer, by then full Colonel, and bearing the resounding title "Chief Signal Officer of the United States Army", a title he had enjoyed for only two months, was peremptorily relieved from that position and put on the shelf. Not long afterward, and for a similar reason, Myer's successor, Lieut. Col. Nicodemus, was likewise summarily relieved as Chief Signal Officer by Secretary Stanton; indeed, he was not only removed from that position—he was dismissed from the Service without even the formality of trial by court martial. Stanton gave "phony" reasons for dismissing Col. Nicodemus, but I am glad to say that the latter was restored his commission in March 1865 by direction of the President; also by direction of the President, Colonel Myer was restored to his position as Chief Signal Officer of the U.S. Army on 25 January 1867. As for what happened to Colonel Myer, the record shows that he executed his commission in July 1864; Colonel Nicodemus lasted about six months after he superseded Myer, and Colonel Benjamin F. Fisher became Chief Signal Officer on 26 December 1864, but his appointment was never confirmed by the Senate. (Photo page 316, 331) In August 1865 Colonel Myer requested that he be restored to the position of Chief Signal Officer of the Army. Accompanying his application were letters of recommendation from several high-ranking officers of the Army and the Navy, and Myer's application was forwarded to Lieutenant General Grant, who returned the application to the President, saying, "Unless there are reasons of which I know nothing, I deem A. J. Myer entitled to the position of Chief Signal Officer of the Army and recommend it accordingly." In a letter dated 30 July 1866 to Secretary of War Stanton, General Grant recommended "the appointment of Albert J. Myer to the place of Chief of the Signal Corps as provided for by Act of Congress. Colonel Myer is the inventor of the system used both in the Army and Navy, which would seem to give him a claim to the position of Chief, which he once held and which the Senate have refused to confirm any other person in." Apparently this last letter produced results, for Colonel Myer was appointed Chief Signal Officer on 25 February 1867, to date from 28 February 1867. Nevertheless, it is this part of the story. When Col. Myer was relieved from duty as Chief Signal Officer in November 1863, he was ordered to
Cairo, Illinois, to await orders for a new assignment. Very soon thereafter he was either designated (or he may have himself decided) to prepare a field manual on signaling and there soon appeared, with a prefatory note dated January 1864, a pamphlet of 148 pages, a copy of which is now in the Rare Book Room of the Library of Congress. The title page reads as follows:


Even in this first edition, printed on an Army press, Myer devoted nine pages to a reprint of an article from Harper's Weekly entitled "Curiosities of Cipher", and in the second edition, 1866, he expanded the section on cryptography to sixty pages. More editions followed and I think we may well say that Myer's Manual in its several editions, was the pioneer American text on military signaling. But I'm sorry to say that as regards cryptology it was rather a poor thing. Poe had done a little better twenty years before that in his essay entitled "A few words on secret writing".

Because of its historic nature, you may like to see what Myer's original "wig-wag code" was like. It was called "a two-element code" because it employed only two digits, 1 and 2, in permutations of 1, 2, 3 and 4 groups. For example, A was represented by the permutation 22; B, by 2122; C, by 121, etc. In flag signaling, a "1" was indicated by a motion to the left, a "2" by a motion to the right. Later these motions were reversed, for reasons which must have been good but are now not obvious. Here is Myer's two-element code which continued to be used until 1912:

**GENERAL SERVICE CODE**

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>2122</td>
<td>121</td>
<td>222</td>
<td>12</td>
<td>2221</td>
<td>2211</td>
<td>222</td>
<td>122</td>
<td>1122</td>
<td>221</td>
<td>221</td>
</tr>
</tbody>
</table>

Note: No. 3 (end of word) was made by a forward downward motion, called "front". There were about a dozen more signals, for numerals, for frequently used short sentences, etc.

We must turn our attention now to the situation as regards the organization for signaling in the Confederate States Army. As indicated a few minutes ago, the first great engagement of the war, that of the First Bull Run battle, the Confederate Signal Corps was formally established nearly a year earlier than...
its Federal counterpart. Perhaps this arose as a result of the far greater success that the Confederate Signal Officers enjoyed during the first great battle of the campaign, Bull Run, than the Union Signal Officers had. The Confederate signal officers were fortunate enough that young lieutenant, E. P. Alexander, who had assisted Major Myer in demonstrating the wig-wag system before a board appointed by the War Department to study Myer's system. Alexander, a Captain in grey, used Myer's system during the battle, which ended in disaster for the Union forces; and it is said that Alexander's contribution of signaling was an important factor in the Confederate victory. Dr. Thompson, whom I have quoted before, says of this battle:

Thus the fortunes of war in this battle saw Myer's system of signals succeed, ironically, on the side hostile to Myer. Because of general unpreparedness and also some disinterest and ignorance, the North had neither wig-wag signals nor balloon observation.

During the first battle of Bull Run the only communication system which succeeded in assisting the Union Army was the infant USMC. But the Confederate system under Alexander, off to a good start at Bull Run, throughout the war and operated with both visual and electric telegraphy, and the Confederates thought highly enough of their signal service to establish it on an official basis, less than a year after that battle. The Signal Corps of the Confederate Army was established, by an Act of the Confederate Congress on 19 April 1862, as a separate corps to be attached either to the Adjutant and Inspector General's Department or to the Engineer Department. The Confederate States Secretary of War on 29 May 1862 attached the Signal Corps to the former organization. Thus, although the Confederate Signal Corps never became a distinct and independent branch of the Army as did the Union Signal Corps, it received much earlier recognition from the Confederate Government than did the Signal Corps of the Federal Government. Again quoting Dr. Thompson:

The Confederate Signal Corps was thus established nearly a year earlier than its Federal counterpart. It was nearly as large, numbering some 1,500, most of the number, however, serving on detail. The Confederate Signal Corps used Myer's system of flags and torches. The men were trained in wire telegraphy, too, and impressed wire facilities as needed. But there was nothing in Richmond or in the field comparable to the extensive and tightly controlled civilian military telegraph organization which Secretary Stanton ruled with an iron hand from Washington.

We come now to an understanding of the codes and ciphers used by both sides in the war, and in doing so we must take into consideration the fact that on the Union side, there were, as I have indicated, two separate organizations for signal communications; the Signal Corps and the USMC. After warfare between them had been settled by ruthless action by Secretary of War Stanton, the Signal Corps had responsibility only for signaling by visual or serial telegraphy, the USMC had responsibility for signaling by electric telegraphy. We should therefore not be
too astonished to find that the cryptosystems used by the two competing organizations were different. On the other hand, on the Confederate side, as just noted, there was only one organization for signal communications, the Signal Corps of the Confederate States Army, which used both visual and electric telegraphy, the latter facilities being taken over and employed when available.

There were reasons for this marked difference between the way in which the Union and the Confederate organized and administered their signal operations. Those who were strange to say, had to do with the difference between the crypto-communication arrangements in the Union and in the Confederate Armies.

We will discuss the cryptosystems used by the Federal Signal Corps first and then that of the Confederate Signal Corps. Since both corps used visual signals as their primary means, we find them employing Myer's visual-signaling code as shown above. At first both sides sent unenciphered messages; but soon after learning that their signals were being intercepted and read by the other side, each side decided to do something to protect its messages. Initially both decided on the same artifice, viz., changing the visual-signaling equivalents for the letters of the alphabet, so that, for instance, "22" was not always "A", etc. This sort of changing-about of values soon became impractical, since it prevented memorizing the wig-vag settings forever once and for all. The difficulty in the Union Army's Signal Corps was solved by the introduction into usage of a cipher disk invented by Myer himself. A full description of the disk in its various embodiments will be found in Myer's Manual, but here's a picture of three forms of it. You can see how readily the visual wig-vag equivalents for letters of the alphabet can be changed according to some pre-arranged indicator for setting the cipher disk. In my Fig. 3, the two left-hand Fig. 1 of Myer's Plate XXVI) show that when letters are xvopped into justaposition, the letter A is represented by 112, B, by 22, etc. By moving the two circles to a different justaposition a new set of equivalents will be established. Of course, if the setting is kept fixed for a whole message, the encipherment is strictly monoalphabetic; but Myer recommends changing the setting in the middle of the message or, more specifically, at the end of each word, thus producing a sort of polyalphabetic cipher which would delay solution a bit. An alternative way, Myer states, would be to use what he called a "countersign word", but which we call a keyword, each letter of which
would determine the setting of the disk for a single word or for two consecutive words, etc. Myer apparently did not realize that retaining or showing externally, the lengths of the words of the plain text is very seriously impair the security of the cipher. A bit later we shall discuss the security afforded by the Myer disk in actual practice.

In the Confederate Signal Corps, the system used for encipherment of visual signals was apparently the same as that used for enciphering telegraphic messages, and we shall soon see what it was. Although Myer's cipher disk was captured a number of times, it was apparently disdained by the Confederates, who preferred to use a wholly different type of device, as will be described presently, for both visual and electric telegraphy.

So much for the cryptosystems used in connection with visual signals by the Signal Corps of both the North and the South, systems which we may designate as "tactical ciphers." We come now to the systems used by the two Military-Telegraph Corps (one in the North, one in the South), which had responsibility for what we may call "strategic ciphers", because the latter were usually exchanged between the seat of Government in the field, or among high commanders in the field. In the case of these communications the cryptosystems employed by each side were quite different.

On the Northern side / the Military-Telegraph Corps used a system based upon what we now call transposition but in contemporary accounts they were called "route ciphers" and that name stuck. The designation isn't too bad, I think, because the processes of encipherment and decipherment, though described not with the individual letters of the message but with entire words, involved following a diagram in which the message is written. I know no simpler or more succinct description of the route/cipher than that given by one of the USMTC operators, J. E. O'Brien, in an article in Century Magazine, XXXVIII, September 1889, entitled "Telegraphing in Battle":

The principle of the cipher consisted in writing a message with an equal number of words in each line, then copying the words up and down the columns by various routes, throwing in an extra word at the end of each column, and substituting other words for important names and verbs.

A more detailed description in modern technical terms would be as follows: A system in which the words of the plain-text message are inscribed within a prescribed number of rows and columns, inscribing the words within the matrix from left to right, in successive lines and rows downward as in ordinary writing, and taking the words out of the matrix, that is, transcribing them according to a prearranged route, to form the cipher message.
The specific routes to be followed were set forth in numbered
booklets designated as "War Department Cipher" folios
by six number. In referring to them hereafter I shall
use the term "cipher books," or sometimes, more simply,
the term "ciphers," although the cryptosystem involves
both cipher and code processes. It is true that the

basic principle of the system, that of Transposition, makes
it partake of the nature most nearly of a cipher system
as defined in our modern terminology, but the use
of "arbitrary" or "arbitrary" numbers or letters to represent
the names of persons, geographical points, important

nouns and verbs, etc., makes the system partake also
of the nature of a code system as defined in our
modern terminology.

There were in all about a dozen cipher
books used by the USMTC throughout the war. For
the most part they were employed consecutively,
but sometimes two different ones were employed
concurrently. They contained not only the specific
routes to be used but also indicators for the routes
and for the sizes of the matrices; and, of course, there
were lists of code words with their meanings.
invention of Anson Stager, whom I have mentioned before in connection with the
establishment of the USMTC, and who is said to have first devised such ciphers
for General McClellan's use in West Virginia, in the summer of 1861, before
McClellan came to Washington to assume command of the Army of the Potomac.

Anson Stager thought that he was the original inventor of the
stated cipher system, but I have been quite in error; word-transposition methods were
in use hundreds of years before his time. For instance, in 1685, in an unsuccessful
attempt to invade Scotland in a conspiracy to set the Duke of Monmouth on the
throne, Archibald Campbell, 9th Earl of Argyll, suffered an unfortunate "accident".
He was taken prisoner and beheaded by order of James the Second. The communica-
tions of the poor Earl were not secure, and when they fell into government hands
they were soon deciphered. The method Argyll used was that of word transposition,
and if you are interested in reading a contemporary account of how it was solved,
look on pages 56-59 of that little book I mentioned before as being one of the
very first books in English dealing with the subject of cryptology, that by
James Falconer, entitled Cryptomysis Patefacts: Or the Art of Secret Information
Disclosed Without a Key, published in London in 1685. There you will find the
progenitor of the route ciphers employed by the Federal Army in the
years 1861-65, fully described in a book entitled The Military Telegraph
during the Civil War, by Colonel William R. Fline, published in Chicago in 1872.

I think Fline's description of them is of considerable interest and I recommend
his book to those of you who may wish to learn more about these systems.

If I show you one example of an actual message and explain its encipherment
and decipherment I will have covered practically the entire gamut of the route
ciphers used by the USMTC, so basically very simple and uniform were they. And
yet, believe it or not, legend has it that the Southern signalmen were unable to
solve any of the messages transmitted by the USMTC. This long-held legend I find
hard to believe. In all the descriptions I have encountered in the literature
not one of them, save the one quoted above from O'Brien, tries to make these
ciphers as simple as they really were; somehow, it seems to me, a subconscious
realization on the part of Northern writers, usually ex-USMTC operators, of the
system's simplicity prevented a presentation which would clearly show how utterly
devoid it was of the degree of sophistication one would be warranted in expecting
in the secret communications of a great modern army in the decade 1860-1870, three
hundred years after the birth of modern cryptography in the papal states of Italy.
Let us take the plain text of a message which Plum (page 58) uses in an example of the procedure in encipherment. The cipher book involved is No. 4 and I happen to have a copy of it so can easily check Plum's work. Here's the message to be enciphered:

Washington, D.C.
July 15, 1863

For Simon Cameron

I would give much to be relieved of the impression that Meade, Couch, Smith and all, since the battle of Gettysburg, have striven only to get the enemy over the river without another fight. Please tell me if you know who was the one corps commander who was for fighting, in the council of war on Sunday night.

(Signed) A. Lincoln

Simon Cameron was Lincoln's Secretary of War until Jan. 1862, when he was replaced by Edwin M. Stanton. If this message cited by Plum is authentic, and there is no reason to doubt this, then Cameron was still in friendly contact with Lincoln, possibly as a special observer.

Plum shows the word-for-word encipherment in a matrix of seven columns and eleven rows. He fails to tell us why a matrix of those dimensions was selected; presumably the selection was made at random, which was certainly permissible.

<table>
<thead>
<tr>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
<th>Column 4</th>
<th>Column 5</th>
<th>Column 6</th>
<th>Column 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incubus</td>
<td>Stewart</td>
<td>Brown</td>
<td>Norris</td>
<td>Knox</td>
<td>Madison</td>
<td>null</td>
</tr>
<tr>
<td>Washington, D.C.</td>
<td>July 15</td>
<td>15th</td>
<td>15</td>
<td>60</td>
<td>3</td>
<td>for</td>
</tr>
<tr>
<td>sigh</td>
<td>man</td>
<td>Camper</td>
<td>on</td>
<td>Flee</td>
<td>(Period)</td>
<td>I</td>
</tr>
<tr>
<td>Simon</td>
<td>much</td>
<td>give</td>
<td>give</td>
<td>much</td>
<td>to be</td>
<td>trammelled</td>
</tr>
<tr>
<td>much</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>relieved</td>
</tr>
<tr>
<td>Toby</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>serenade</td>
</tr>
<tr>
<td>the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>of the</td>
</tr>
<tr>
<td>to</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>impression</td>
</tr>
<tr>
<td>be</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>that</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Burns</td>
<td>bear</td>
<td>ex</td>
<td>cat</td>
<td>children</td>
<td>and</td>
<td>all</td>
</tr>
<tr>
<td>Neade</td>
<td>(comma)</td>
<td>Couch</td>
<td>(comma)</td>
<td>Smith</td>
<td>and</td>
<td>will</td>
</tr>
<tr>
<td>since</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>get</td>
</tr>
<tr>
<td>bat</td>
<td>(comma)</td>
<td>the</td>
<td>the</td>
<td>battle</td>
<td>of</td>
<td>Gettys</td>
</tr>
<tr>
<td>(comma)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ties</td>
</tr>
<tr>
<td>large</td>
<td>have</td>
<td>have</td>
<td>striving</td>
<td>only</td>
<td>to</td>
<td>get</td>
</tr>
<tr>
<td>burg</td>
<td>(comma)</td>
<td>(comma)</td>
<td>(comma)</td>
<td>only</td>
<td>to</td>
<td>get</td>
</tr>
<tr>
<td>(comma)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>village</td>
<td>over</td>
<td>the</td>
<td>without</td>
<td>another</td>
<td>another</td>
<td>optic</td>
</tr>
<tr>
<td>the</td>
<td>enemy</td>
<td>river</td>
<td>without</td>
<td>another</td>
<td>fight</td>
<td>bound</td>
</tr>
<tr>
<td>shiloh</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Period):</td>
</tr>
<tr>
<td>Please</td>
<td>tell</td>
<td>me</td>
<td>if</td>
<td>you</td>
<td>no</td>
<td>know</td>
</tr>
<tr>
<td>Please</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>who</td>
</tr>
<tr>
<td>was</td>
<td>the</td>
<td>Harry</td>
<td>one</td>
<td>Madrid</td>
<td>corps</td>
<td>locust</td>
</tr>
<tr>
<td>was</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>commander</td>
</tr>
<tr>
<td>the</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>who</td>
</tr>
<tr>
<td>was</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>who</td>
</tr>
<tr>
<td>for</td>
<td>opposing</td>
<td>fighting</td>
<td>town</td>
<td>in the</td>
<td>council</td>
<td>war</td>
</tr>
<tr>
<td>for</td>
<td>(comma)</td>
<td>(comma)</td>
<td></td>
<td></td>
<td></td>
<td>of</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>on</td>
<td>Tyler</td>
<td>Rustle</td>
<td>upright</td>
<td>Adrian</td>
<td>bless</td>
<td>hit</td>
</tr>
<tr>
<td>on</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(null)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Null</td>
<td>(monkey)</td>
<td>(girl)</td>
<td>(horse)</td>
<td>(Suicide)</td>
<td>(null)</td>
<td>(null)</td>
</tr>
</tbody>
</table>

[Notes: Ruled paper was provided to aid in accuracy. In the diagram, the upper row is the plain text, the lower row is the cipher text. The Plain text is: 'Incubus Stewart Brown Norris Knox Madison null'.]
Note the "null" (non-significant, or "blind" word) at the bottom of each column, these being added to confuse a would-be decipherer. At least that was the theory, but how effective this subterfuge was can be surmised, very likely, once it became known that this was the usual practice. Note also the two "nulls" (bless him) at the end of the last line to complete this line of the matrix.

The cipher message is then copied down following the route prescribed by the indicator "BLONDE", as can be seen on page 7 of Cipher Book No. 4. The indicator could have also been "LINDEN".

To explain the diagram at the top of the picture I will first show you the "Directions for Use" which appear on the reverse side of the title page of "War Department Cipher No. 4", because I'm afraid you wouldn't believe me if I merely quoted from those "Directions". Here's a picture of the title page and I follow it with a photograph of what's on its reverse side of the title page:

---

To explain the diagram at the top of the picture I will first show you the "Directions for Use" which appear on the reverse side of the title page of "War Department Cipher No. 4", because I'm afraid you wouldn't believe me if I merely quoted from those "Directions". Here's a picture of the title page and I follow it with a photograph of what's on its reverse side of the title page:

---

Dear Madam:

Note the "null" (non-significant, or "blind" word) at the bottom of each column, these being added to confuse a would-be decipherer. At least that was the theory, but how effective this subterfuge was can be surmised, very likely, once it became known that this was the usual practice. Note also the two "nulls" (bless him) at the end of the last line to complete this line of the matrix.

The cipher message is then copied down following the route prescribed by the indicator "BLONDE", as can be seen on page 7 of Cipher Book No. 4. The indicator could have also been "LINDEN".

If you examine the diagram at the top of the picture I will explain it. The sketch who was responsible for getting this cipher book approved ever thought about what he was doing when he caused those "Directions for Use" to be printed? If it doesn't seem possible. All he would have had to ask himself was, "Why put this piece of information in the book itself? Suppose the book falls into enemy hands, can't be read, too, and at once learn about the intended deception? Why go to all the trouble of including "phony" routes in the book? If the book doesn't fall into enemy hands what good are the "phony" routes anyway? Why not just indicate the routes in a straightforward manner, as had been done before? Thus: "Up the 6th column (since "6" is the first number at the left of the diagram), down the 3rd, up the 5th, down the 7th, up the 1st, down the 8th and down the 2nd. This matter is so incredibly fatuous that it is hard to understand how sensible men - and they were sensible - could be so misguided as to have concept of thinking "Directions for Use" illogical in their processes. But there they stand, for all the world to see and to judge.

Now for the transposition step. The indicator "BLONDE" signifies a matrix of seven columns and eleven rows, with the route set forth above, viz., up the 6th column, down the 3rd, etc., so that the cipher text with a "phony" address and signature becomes as follows:

TO A. HARPER CALDIEL, Washington, D. C.

Cipher Operator, Army of the Potomac:

Blonde bless of who no optic to get and impression I Madison square Brown cam er Toby as the have turnip me Barry bitch rustic silk Adrian counsel locust you another only of children serenade Lisa Knox County for wood that av ties get hound who was war him suicide on for was please village large that Bryan give sigh incubs Harry Norris on tramped cat knit striven without if Madrid quall upright martyr Stewart man much bear since ass skeleton tell the oppressing Tyler monkey.

(Signed) C. HOMER BATES

It was the usual practice to use for address and signature the names of the USMRC operators concerned.
Note that the text begins with the indicator "BLONDE". In decipherment the steps are simply reversed. The indicator tells what size matrix to outline; the words beginning "bless of who no optic . . ." are inscribed within the matrix: up the 6th column; then omitting the "check word" or "null" (which in this case is the word "square") down the 3rd column, etc. The final result should correspond to what is shown in Fig. 70. There then follows the step of interpreting orthographic deviations, such as interpreting "sigh", "men", "camer", and "on" as Simon Cameron; the word "wool" for "would", etc., which these reproduces the original plain text.

Save for one exception to be discussed in a moment here, all the route ciphers used by the USMTC conformed to this basic pattern. The things that changed from one cipher book to the next were the indicators for the dimensions of the matrices and for the routes; and the "arbitraries" or code equivalents for the various items comprising the "vocabulary", the number of them increasing from one edition to the next, just as might be expected. The sole exception to this basic pattern by the USMTC is to be seen in Cipher Book No. 9 and on only one page of the book. I will show you that page:

What we have here is a deviation from the straightforward route transposition, up the . . . A down the . . . A. By introducing one diagonal path in the route (the 6th, 7th, 8th, 9th, 10th words in a message of five columns, and the 1st, 2nd, 3rd, 4th, 5th, and 6th words in a message of six columns) the simple up and down route no longer holds true. The words on the diagonal interrupt the normal up and down paths and introduce complexities in the method. In fact, the complexities seemed to be a bit too much for the USMTC cipher operators because, as far as available records show, these complicated routes were never used.
I now wish to make a number of general and a few specific comments on Plum's description of the cryptosystems used by the U/S/M/T/C. 


---

First, we note that although Anson Stager, later Colonel Stager, has been credited with inventing the type of cipher under consideration in this study, he was anticipated in the invention by about 200 years.

Also, he is given the lion's share of the credit for devising those ciphers although he did have a number of collaborators and Plum names four of them, presumably because he thought them worthy of being singled out for particular attention. Plum and others tell us that copies of messages handled by the U/S/M/T/C (sometimes were) intercepted by the enemy but not solved. He cites no authority for this last statement, merely saying that such intercepts were published in the newspapers of the

The hope that somebody would come up with the Confederacy with requests for help in their solution. But it may be noted that none of the Confederate accounts of war activities cite instances of the solution of intercepted U/S/M/T/C messages, although there are plenty of citations of instances of interception and solution of enciphered
visual transmissions of Federal Army's Signal Corps. Douglass-Freeman's

In referring hereinafter to the cryptographic books used by the U.S.M.T.C., I shall use the term "cipher books," or sometimes simply "ciphers," although the cryptosystems involves both code and cipher processes. Its underlying transposition feature makes it partake of the nature of a cipher system according to modern terminology, but the heavy use of "arbitraries," that is, of arbitrary words to represent the names of persons, places, rivers, etc.; important nouns and verbs, etc., makes the system partake of the nature of code.

Plum states that 12 different cipher books were employed by the Telegraph Corps, but I feel sure there were only eleven. The first one was not numbered, and this is good evidence that a long war was not expected that there were no preparations for a long war, and that hasty improvisation on the outbreak was the rule. This first cipher book had 16 printed pages. But for some reason, now impossible to fathom, the sequence of numbered books thereafter was as follows: Nos. 6 and 7, which were much like the first (unnumbered) one; then came Nos. 12, 9, 10--
that strange order; then came Nos. 1 and 2; finally came Nos. 3, 4, and 5.

(Apparently there was no No. 8, or No. 11.) It would be unsafe to think
that the irregularity in numbering the successive books was of communication-
but there are other things about these books and the cryptosystem that add
security. There must have been some reasons, but what they were is now
unknown. Plum states that No. 4, the last one used in the war, was placed
into effect on 23 March 1865, and that it and all other ciphers were
discarded on 20 June 1865. However, as noted, there was a No. 5, which
Plum says was given a limited distribution. I have a copy of it, but
whether it was actually put into use I do not know. Like No. 4, it had
40 pages, about 20 copies were sent to certain members of the Military
Telegraph-Service, scattered among 12 states; and, of course, Washington must have
had at least one copy.

We may assume with a fair amount of certainty that the first (the
unnumbered) cipher book used by the USMTC was merely an elaboration
of the one Stager produced for the communications of the governors of Ohio,
Indiana and Illinois, and of which a copy is given by only one of the
writers who have told us about these ciphers, namely, David H. Bates.
Bailey, in his series of articles entitled "Lincoln in the Telegraph Office"

*The Century Magazine, Vol. LXXIV, Nos. 1-5, May-Sept, 1907* shows a facsimile thereof (p. 292, June 1907 issue), and I have had as good a reproduction made of it as is possible from the rather poor photographic facsimile. The foregoing cipher is the prototype upon which all subsequent cipher books were based, the first of the War Department series being the one shown by Plum, in Appendix to this lecture.

When these ciphers came into use it was not the practice to misspell certain words intentionally; but as the members of the U.S.M.T.C (who, as I've told you, not only served as telegraph operators but also as cipher clerks) developed expertness, the practice of using non-standard orthography was frequently employed to make solution of messages more difficult. Thus, "meet" became "meet" or even "flesh", "wood" is used in place of "would", etc. In an actual case involving a message sent to General Grant at Vicksburg the word "Arkansas" is spelled in three words: "Art" "see" "see," and one finds hundreds of examples of this sort of artifice. Then, further to increase security, more and more "arbitrariness".

The series was then put out in book form under the same title by the D. Appleton-Century Company, New York, 1907, reprinted in 1939.
that is, code equivalents were added to represent such things as ordinal and cardinal numbers, months of the year, days of the week, hours of the day, geographical names of places and rivers, punctuation, etc. As a last additional step, code equivalents for frequently-used words and phrases were introduced. One good example of two typical pages from one of these books will characterize them all.

You will notice that the code equivalents are printed but their meanings are written in by hand. This was usually the case, and the reason is obvious: for economy in printing costs, because the printed code equivalents of plain-text items in cipher books belonging to the same series are identical; only their meanings change from one book to another, and of course, the transposition routes, their indicators, and other variables change from one book to another. As already indicated, I am fortunate in having six of these cipher books in my private collection, so that comparisons among them are readily made. The first feature to be noted is that the code equivalents are all good English dictionary words (or proper nouns), of not less than three nor more than seven (rarely eight) letters. A careful scrutiny shows that in the early editions the code
equivalents are such as are not likely to appear as words in the plain-text messages; but in the later editions, beginning with No. 12, more than 50% of the words used as code equivalents are such as might well appear in the plain-text of messages. For example, words such as AID, ALL, ARMY, ARTILLERY, JUNCTION, CONFEDERATE, etc., baptismal names of persons, and names of cities, rivers, bays, etc., appear as code equivalents. Among names used as code equivalents are SHERMAN, LINCOLN, THOMAS, STANTON, and those of many other prominent officers and officials of the Federal and Confederate Army and Government; and, even more intriguing, such names were employed as indicators for the number of columns and the routes used—the so-called "Commencement Words." It would seem that names and words such as those I've mentioned might occasionally have brought about instances where difficulty in deciphering messages arose from this source of confusion, but the literature doesn't mention them. A bit later we shall see why such commonly-used proper names and words were not excluded. There was, indeed, method in this madness.

But what is indeed astonishing to note is that in the later editions of
these cipher books, in great majority of cases the words used as

"arbitraries," differ from one another by at least two letters (for example, LADY and LAMB, LARK, and LAWN, ALBA and ASIA, LOCK and WICK, MILK and MINT),
or by more than two (for example, MYRTLE and MYSTIC, CARBON and CANCER,
ANDES and ATLAS). One has to search for cases in which two
words differ by only one letter, but they can be found if you search long
each for them, as, for example, QUINCY and QUINCE; FINE and PIKE, ROSE
and ROSE. Often there are words with the same initial trigraph or
tetragraph, but then the rest of the letters are such that errors in
transmission or reception would easily manifest themselves, as, for example, in the cases of
MONSTER and MONARCH, MAGNET and MAGNOLIA. All in all, it is important to
note that the compiler or compilers of cipher books had adopted a principle
known today as the "two-letter differential," a feature found only in
codebooks of a much later date. In brief, the principle involves the use,
in a given codebook, of code groups differing from one another by at
least two letters. This principle is employed by knowledgeable code
compilers to this very day, not only because it enables the recipient of a
message to detect errors in transmission or reception, but also because the permutation tables used in constructing the code words facilitate their correction without calling for a repetition. It is clear, therefore, that the compilers of these cipher books took into consideration the fact that errors are to be expected in Morse telegraphy, and by incorporating, but only to a limited extent, the principle of the two-letter differential, they tried to guard against the possibility that errors might go undetected. Had artificial letter groups been used as code equivalents instead of dictionary words, possibly the cipher books would also have contained the permutation tables. But there is, however, another feature about the words the compilers of these books chose as code equivalents. It is a feature that manifests real perspicacity on their part. A few moments ago I said that I would explain why, in the later and improved editions of these books, words which might well be words in plain-text messages were not excluded from the lists of code equivalents: it involves the fact that the basic nature of the cryptosystem in which these code equivalents were to be used was clearly recognized by those who compiled the books. Since the cryptosystem was based upon word transposition, what could be more confusing to a would-be cryptanalyst, working with messages in such a system, than to find himself unable to decide whether a word in the cipher text is actually in the
original plain-text message and has its normal meaning, or is a code word
with a secret significance—or even a null, a non-significant word, a "blind"
or a "check word," as those elements were called in those days? That, no
doubt, is why there are, in these books, so many code equivalents which might
well be "good" words in the plain-text messages. And in this connection I
have already noted an additional interesting feature: at the top of each
page devoted to indicators for signaling the number of columns in the
are printed the
specific matrix for a message, these appear in several of these books, the
or what we now call "indicators." Now, there are nine such
so-called "commencement words," six words, in sets of three, any one of
which could actually be a real word or "waste in the plain-text message.
Words when used as
Such indicators could be very confusing to enemy cryptanalysts, especially
after the transposition operation. Here are the "commencement words" on
page 5 of Cipher Book No. 9: Army, Anson, Action, Astor, Advance, Artillery,
Anderson, Ambush, Agree; on page 7 of No. 10: Cairo, Curtin, Cavalry,
Congress, Childs, Calhoun, Church, Cobb, etc. Moreover, in Nos. 1, 3, 4
5, and 10 the "line indicators," that is, the words indicating the number
of horizontal rows in the matrix, are also words such as could easily be
words in the plain-text messages. For example, in No. 1, page 3, the line indicators are as follows:

<table>
<thead>
<tr>
<th>Address</th>
<th>1</th>
<th>Faith</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjust</td>
<td>2</td>
<td>Favor</td>
</tr>
<tr>
<td>Answer</td>
<td>3</td>
<td>Confine</td>
</tr>
<tr>
<td>appear</td>
<td>4</td>
<td>Bed</td>
</tr>
<tr>
<td>Appeal</td>
<td>5</td>
<td>Beef</td>
</tr>
<tr>
<td>Assume</td>
<td>6</td>
<td>Bend</td>
</tr>
<tr>
<td>Awake</td>
<td>7</td>
<td>Avail</td>
</tr>
<tr>
<td>Encamp</td>
<td>8</td>
<td>Active</td>
</tr>
<tr>
<td>Enroll</td>
<td>9</td>
<td>Absent</td>
</tr>
<tr>
<td>Enough</td>
<td>10</td>
<td>Accept</td>
</tr>
</tbody>
</table>

Note two things in the foregoing list: first, there are variants—there are two indicators for each case; and second, the indicators are not in strict alphabetic sequence. This departure from strict alphabeticity is even more obvious in the pages devoted to vocabulary, a fact of much importance cryptanalytically. Note this feature, for example, in Fig. 10, showing pages 14 and 15 of Cipher Book No. 12.

In this respect, therefore, these books partake somewhat of the nature of two-part codes, or, in British terminology, "hatted" codes. In the second lecture of this series the physical difference between one-part and two-part codes was explained, and it is therefore unnecessary to repeat that explanation here. But an indication of the technical difference between these two types of codes from the point of view of cryptanalysis may be useful at this point. Two-part codes are much more difficult to
solve than one-part codes, in which both the plain-text elements and their code equivalents progress in parallel sequences. In the latter type of determination of the meaning of one code group quickly and rather easily leads to the determination of the meanings of other code groups above or below the one that has been solved. For example, in the following short but illustrative example, if the code group 1729 has been determined to be "then," the meaning of the code group 1728 could well be "the," that of the code group 1730, "there". But in a two-part code, determining the meaning of the code group 0972 to be, as being the word "then," gives no clue whatever as to the meaning of the groups 7621 or 1548. For ease in decoding messages in such a code there must be a section in which the code groups are listed in numerical and are accompanied by which, of course, will be sequence, their meanings in a random sequence. The compilers of the U.S.M.T/C cipher books must have had a very clear idea of what I have just explained, but in simplicity matters, they made a compromise of a practical nature between a strictly one-part and a strictly two-part
code, because they realized that a code of the latter sort is twice as
besides being much more laborious to compile and check, the contents
bulky as one of the former sort. The arrangement they chose wasn't 
too
bad, so far as crypto-security was concerned. As a matter of fact, and
speaking from personal experience in decoding a rather long message

difficult
addressed to General Grant, I had a trying time in locating many of the
code words in the book, because of the departure from strict alphabeticity.
I came across that message in a work-book in my collection, the work-book
of one of the important members of the U.S.M.T.C.—none other than our friend
Plum, from whose book, *The Military Telegraph during the Civil War*, comes
much of the data I've presented. On the first fly-leaf of
Plum's work-book there appears, presumably in his own handwriting, the
legend "W. R. Plum Chf Opr with Gen. G. H. Thomas". Here's one of the
messages he enciphered in Cipher Book No. 1, the book in which, he says,
more important telegrams were sent than in any other:

Note how many "arbitraries," or words with secret-meanings, appear in
the plain-text message, that is before transposition. After transposition
the melange of plain-text and code words must have been quite mystifying.*

And yet, was the system so very inscrutable after all? I don't think so.

Even in the case of the foregoing message there are enough unencoded words in sequence in the plain-text version so that with a bit of patience, working on the cipher version, I think the transposition could be removed without too much difficulty and the general tenor of the message could be determined. There would remain, of course, the business of finding the specific meanings of the code words. In the case of cipher book No. 1, which, was, according to Plunkett, the one that had the longest and widest use, an accumulation of messages would probably have given enough data for determining the specific meanings of the code words. But it is to be remembered that these messages were transmitted by wire telegraphy, and not by radio, so that opportunities for intercepting the "tapping" telegraph or capturing couriers or headquarters with their files intact. Opportunities for these lines were not frequent, but they did occur from time to time, and in one case a Confederate signalman hid in a swamp for several weeks and tapped a Federal telegraph line, obtaining a good many messages. *What success, if any, did Confederate cryptanalysts have in their attempts to solve such messages?

*In searching for a good example my eye caught the words "Lincoln shot" at the left of the matrix and I immediately thought that the message had to do with Booth's assassination of the President. But after hurriedly translating the message and finding nothing in it having anything to do with the shooting it occurred to me to look up the indicators for a matrix of six rows and eight columns. They turned out to be LINCOLN (message of 8 columns), SHOT (6 rows). The word SMALL beneath the "Lincoln shot" is a variant for SHOT, also meaning "6 rows".
U.S.M.T.C. cryptograms, they did intercept? We shall try to answer this question in due time, but now we must hasten to a consideration of the cryptosystems employed by the Confederate States Army.

As indicated earlier, in the Confederacy there were no competing signal organizations, as there were on the Union side. There was nothing at the center of government in Richmond or in the combat zone comparable to the extensive and tightly-controlled civilian military telegraph organization which Secretary Stanton ruled with an iron hand from Washington. Almost as a concomitant it would seem, there was in the Confederacy, save for two exceptional cases, one and only one cryptosystem to serve the need for protecting tactical as well as strategic communications, and that was the so-called Vigenere Cipher, which apparently was the cipher authorized in an official manual prepared by Capt. Alexander as the partial equivalent of Myer's Manual of Signals. You won't find the name Vigenere in any of the writings of contemporary signal officers of either the North or the South. The signalmen of those days called it the "Court Cipher," this term referring to the system in common use in diplomatic or "court" secret communications about this period in history. It is hardly necessary for me to tell you in detail about that cipher which employs the so-called Vigenere Square with a repeating key.* Here is the square which Plum presents in his which is followed by his description of its manner of employment: A keyword is employed to change the alphabets cyclically, thus making the cipher what is called today a periodic or multiple-alphabet cipher controlled by the individual letters of a key, which may consist of a word, a phrase, or even of a sentence, repeated as many times as necessary.
### Confederate States Cipher Key

| 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| a  | b  | c  | d  | e  | f  | g  | h  | i  | j  | k  | l  | m  | n  | o  | p  | q  | r  | s  | t  | u  | v  | w  | x  | y  | z  |
| 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

To put into cipher the first message, which is put up by using "Manchester Bluff" as the key, and the second by the key term, "Complete Victory," find at the left-hand side of the table the first letter of the first word to be ciphered, and at the top of the table, the first letter of the term. At the junction of the columns in which these letters are so found, will be seen the arbitrary letter which is to be used in lieu of the real one at the left. Continue in this way with each successive letter of the message and key term, repeating on the latter till finished. Thus, "Sherman is victorious," put in cipher by using the first key, would read, as shown by the capitals, c-o-m-p-l-e-t-e-v-i-o-n-a-b-e. Of course, any change in the key word, term or phrase changes the arbitrarians, and if neither the real message nor the key is known, it would be somewhat vexatious working it out, unless there were some such suggestive words as occur in Davis's message above, which indicate the ciphered words very clearly; e.g., "By which you may effect" o t p g k x y a crossing "above that part" h p g k n u c t. This meaning occurred to the author, of the river.

at first sight, and doubtless would be to any one familiar with military affairs in that section. Having guessed real words, it is very easy to work out the letters of the key. The following two important ciphers were transmitted as divided below; i.e., each word was sent separately, not all mixed, as in the Pemberton cipher. This division does not facilitate translation by the key at all, but materially assists without it, and was, therefore, bad practice. We give below, each message, with its translation, because these telegrams were very important. The curious reader may, at his leisure, by using the key board, study out the key terms, one of which will be found entirely new and quite apropos, in the light of what speedily followed.
CONFEDERATE STATES OF AMERICA, MILITARY TELEGRAPH, Dated
Head-quarters, February 25, 1865. Received at Richmond,
Va., 12:25 minutes, A.M.
TO HON. J.C. BRECKENRIDGE, Sec'y of War:—I recommend
that the telegrams in outgoing unfatigued unopened ex-f'vzj and is-
waajru katu are not of immediate necessity, uq kpjiNbbgr
mpo thnil should be leugtsp. (Signed) R.E. LEE

TRANSLATION.—I recommend that the removal of public
property, machinery, stores and archives which are not of
immediate necessity, be commenced. All powder should be
secured.

HEAD-QUARTERS C.S. ARMIES, March 29, 1865.
GEN. R. KINZIE SMITH, comdg. Trans-Miss. Dept., Gen:—
Vtg eciilysps rcog uj lhozines kfc k df vaspb uf tcfFato
abm bxj aszkhmgjelxivbcex gb niel uesu ht kfg adhi egh
opom kfs uavj pf xymocci yu addctpt in 1cjakpat in evjus
mrvr tvhce abm iu soing o ndez en 1ucr ny njtyzme
xvzryb yrq rxpx rzakjph ytax xep ezes racdrxzypt
zmzeb acgg nafqvrf no kfg ambe frtr va nvv kge pyh feun
okfrlnzyrl qx jtbhx rj xftx xvmv f4 acgg avnxvvy
yuag ce mzyat yga scuh.
I am most respectfully your obdt. servt.,
(Signed) R.E. LEE

TRANSLATION.—Gen: The president deems it advisable
that you should be charged with the military operations on
both banks of the Miss., and that you should endeavor as
promptly as possible to cross that river with as large a
force as may be prudently withdrawn from your present Dept.
You will accordingly extend your command to the east bank
of the Miss., and make arrangements to bring to this-side
such of your present force as you may deem best.
I am most respectfully your obedient servant.

There are certain comments to be made on the foregoing, which in all
right as far as it goes, but it just doesn't go far enough, unfortunately, for
the procedure. Please give the two fatal defects.

In the first place, note that in the first message certain words are
left unenciphered; in the second place, in both the first and the second
message, the ciphers retain and clearly show the lengths of the words which
have been enciphered. Both of these faulty practices greatly weaken the security of ciphers
because they leave good clues to the contexts, and can easily result in falsification
of messages, and even possibly solving the messages. We know today that cipher
messages should leave nothing in the clear. Even the address and the signature,
the date, time and place of origin etc., should if possible be hidden; and
the cipher text should be in completely regular groupings so as not to disclose
the lengths of the plain-text words, and hence to promote accuracy in
transmission and reception.

So far as my studies have gone, I have not found a single example of
a Confederate Vigenere cipher which shows neither of these two fatal
weaknesses. And the second of the two 3esuenn examples is the only case
I have found which there are no unenciphered words in the text of the message.
And the only example I have been able to find in which word lengths are not
shown (save for one word) is in the case of the following message:

Vicksburg, Dec. 26, 1862.

GEN. J.E. JOHNSTON, JACKSON:
I preferievesr, it has reference to xhvkjshcfrbselregwmyk
to prevent amuzeyzjwtpjw at that point, maelpghvelviaufultialt
lihfnagtswmlfgoajd.

(Signed) J.C. PEMBERTON,

Even in this case there are unenciphered words which afford a clue which enables
our new friends to solve the message. It took some time; however, and the story is
re-solution.

In the various accounts of these ciphers I have encountered, one and only
write who makes a detailed comment on
one dissenting voice in regard to the two fatal practices to which I refer.

A certain Dr. Charles E. Taylor, a Confederate veteran (in an article entitled
"The Signal and Secret Service of the Confederate States," published in the
Confederate Veteran, Vol. XL, Aug-Sept 1932) after giving an example of
encipherment according to the "court cipher" says:
worth telling.

According to Plum, the foregoing cipher message was the very first one captured by USMTC operators, and it was obtained during the siege of Vicksburg, which surrendered on 4 July 1863. But note the date of the message: 26 December 1862. What was done with the captured message during the months from the end of December 1862 to July 1863? Here is what Plum reports:

What efforts General Grant caused to be made to unravel this message, we know not. It was not until October, 1864, that it and others came into the hands of the telegraph cipherers at New Orleans, for translation...

The New Orleans operators, who worked out this key [Manchester Bluffs], were aided by the Pendleton cipher and the original telegram, which was found among that general's papers after the surrender of Vicksburg; also by the following cipher dispatch, and one other:

Plum gave the messages involved, and their solution, and the keys, the latter being the three cited above. It would seem that General Grant had been brought to General Grant's attention and he did nothing.
about it, he was not highly interested in intelligence.

Secondly, the solution of the message and the others apparently took some time, even though there was one message with its plain text (the Pemberton message) and two messages not only with interspersed plain-text words but also with spaces showing word lengths. But Plum does not indicate how long it took for solution. Note that he merely says that the messages came into the hands of the telegraph operators in October 1864; he does not give when solution was reached.
It hardly needs to be said that the division between the words of the original message as given above was not retained in the cipher. Either the letters were run together continuously or breaks, as if for words, were made at random. Until the folly of the method was revealed by experience, only a few special words in a message were put into cipher, while the rest was sent in plain language. This afforded opportunity for adroit and sometimes successful guessing.

... I think it may be said that it was impossible for well prepared cipher to be correctly read by any one who did not know the key-word. Sometimes, in fact, we could not decipher our own messages when they came over telegraph wires. As the operators had no meaning to guide them, letters easily became changed and portions, at least, of messages rendered meaningless /sic/ thereby.

Frankly, I don't believe Dr. Taylor's comments are to be taken as characterizing the practices that were usually followed. No other ex-
signalman who has written about the ciphers used by the Confederate Signal Corps makes such observations and I think we must simply discount what Dr. Taylor says in this regard.

It would certainly be an unwarranted exaggeration to say that the two weaknesses in the Confederate cryptosystem cost the Confederacy the victory for which it fought so mightily, but I do feel warranted at this moment in saying that further research may well show that certain battles and in saying that further research may well show that certain battles and campaigns were lost because of faulty cryptography leading to communications inaccuracy.

A few moments ago I said that, save for an exception or two, there was in the Confederacy one and only one cryptosystem to serve the needs of secure tactical as well as strategic communications. One of these exceptions concerned the cipher used by General Bessregard after the battle of Shiloh and (8 April 1862). This cipher was purely monoalphabetic in nature, i.e. one example: a reciprocal cipher alphabet was used:

```
  A B C D E F G H I J K L M
  N O P Q R S T U V
  `---`---`---`---`---`---`---
  L O S T P O S T I B T U
```


This simple cipher was discarded as soon as the official cipher was prescribed in Alexander's manual. It was just as well that Deschregard's cipher was discarded because the deciphered message came to the attention of Confederate authorities in Richmond via a northern newspaper! It is curious to note that the Federal War Department had begun using ciphersystems for messages very promptly after the outbreak of war, whereas not until 1862 did the Confederate States War Department prepare an official ciphersystem, and then it adopted the "court cipher".

The other exception involved a system used at least once before the official system was adopted and it should be mentioned. On 26 March 1862, the Confederate States President, Jefferson Davis, sent General Johnston by special messenger a dictionary, with the following accompanying instruction:* I send you a dictionary of which I have the duplicate, so that you may communicate with me by cipher, telegraphic or written, as follows: First give the page by its number; second the column by the letter L, M or R, as it may be, in the left-hand, middle, or right-hand columns; third, the number of the word in the column, counting from the top. Thus, the word junction would be designated by 146, L, 20. This cipherage a you do doubt have already made or, as there were three of the types of ciphers used by both sides during the American Revolutionary Period almost a century before, except that in this case the dictionary had three columns to the page instead of two. I haven't tried to find what dictionary you used—but it shouldn't take long to locate it, since the code equivalent of the word "junction" was given: 146, L, 20. Moreover, there is extant one fairly long message, with its decode, given. How many other messages there may be in National Archives I don't know.

Coming back now to the "court cipher," you will probably find it just as hard to believe, as I find it, that according to all accounts three and three only the four keys were used by the Confederates during these whole years of warfare from 1862 to 1865. It is true that Southern signalmen make mention of frequent changes in key but in all the literature only the following four are specifically cited:

1) **COMPLETE VICTORY**
2) **MANCHESTER BLUFF**
3) **COME DISTRIBUTION**
4) **IN GOD WE TRUST**

It seems that all were used concurrently, but I have seen it only once, and that is in a book explaining the "court cipher" many times, the last—well, I just don't know because only one example has turned up. Note that in the case of the next three, the key consists of exactly 15 letters, but why this should be so is not clear. How the rule been made? No one ever cared to explain. But as has been clearly stated, the length of word lengths was not even contemplated, let alone prescribed, so that there seems to be no advantage in choosing the keys which contain exactly 15 letters. And, by the way, doesn't the key COME DISTRIBUTION sound rather ominous to you these days?

An example of two of authentic Confederate messages which were intercepted and deciphered by members of the [name redacted]... Here...
Perhaps you will wish to decipher them, which should be quite easy in view of the fact that you will merely have to select the proper key from among those given above.

Sooner or later, one of the Confederate signal officers was bound to come up with a device to simplify ciphering operations, and a gadget devised by a Captain William N. Barker seemed to meet the need. In Myer's Manual there is a picture of one form of the device, shown here in Fig. 50. I don't think it necessary to explain how it worked, for it is almost self-evident. Several were captured during the war, one of them being among the items in the NSA Museum. But here's a photograph of the one found in the office of Confederate Secretary of State Judah P. Benjamin after the capture of Richmond.

How many of these devices were in existence or use is unknown, for their construction was an individual matter—it was not an item of regular issue to members of the corps. Here's a picture of one captured at Vicksburg and you can see that it was a do-it-yourself job, a rough piece of work.

In practically every account of the codes and ciphers of the Civil War you will find references, some in much detail, to ciphers used by Confederate secret service agents engaged in espionage in the North as well as in Canada.
In particular much attention is given to a set of letters in cipher which were intercepted by the New York City Postmaster and which were involved in a plot to print Confederate currency and bonds. Much ado was made about the solution of these ciphers by cipher operators of the U.S. Post office in Washington and the consequent breaking up of the plot. But I won't go into these ciphers for two reasons. First, the alphabets were all of the simple monoalphabetic type, a total of six altogether being used. Since they were composed of symbols, a different series for each alphabet, it was possible to compose a cipher word by jumping from one series to another without any external indication of the shift, but good eyesight and a bit of patience were all that was required for solution in this case because of the inept manner in which the system was used: a whole word, sometimes several successive words, were enciphered by the same alphabet. But the second reason for my not going into the story is that my colleague Edwin C. Fishel, whom I've mentioned before, has done some research among the records in our National Archives dealing with this case and he has found something which is of great interest and which I feel bound to leave for him to tell at some future time, as it is his story, not mine.

So very fragmentary was the amount of cryptologic information known to the general public in those days that even on John Wilkes Booth's body and in another except for two
his trunk in the Federal Hotel in Washington there were found copies of what were previously a cipher square. Since the Federal authorities in Washington had copies of a similar square, captured or taken from prisoners at Yorktown...
times during the war, an attempt was made to implicate leaders of the
Confederacy in the plot to assassinate Lincoln. They offered as evidence a
cipher square which had been mounted on the cipher reel found by Union. Asst. Secretary of War, Charles A. Dana
in Confederate Secretary of State Judah P. Benjamin's office in Richmond, the Federal authorities

Then they attempted to prove that this necessarily meant that the Confederate leaders had been giving Booth instructions in cipher. In regard to the word, "a picture of the cipher squares found on Booth's, and also a tin box in his hotel room in Washington, assassination, but the attempt was not successful. The following is quoted from Philip Van Doren Stern's book entitled Secret Missions of the Civil War (Rand McNally and Co., New York, 1959, p. 320):

Everyone in the War Department who was familiar with cryptography knew that the Vigenere was the customary Confederate cipher and that for a Confederate agent (which Booth is known to have been) to possess a copy of a variation of it meant no more than if a telegraph operator was captured with a copy of the Morse Code. Hundreds and perhaps thousands of people were using the Vigenere. But the Government was desperately seeking evidence against the Confederate leaders so they took advantage of the atmosphere of mystery which has always surrounded cryptography and used it to confuse the public and the press. This shabby trick gained nothing, for the leaders of the Confederacy eventually had to be let go for lack of evidence.

It is only fitting that what was probably the last official cipher message of the Confederacy was written in the Vigenere. This was a brief note from Jefferson Davis dated April 26, 1865, at Charlotte, North Carolina, and sent to his secretary, Burton E. Harrell, at Chester, South Carolina. It read: "The hostile government reject the proposed settlement, and order active operations resumed in forty-eight hours from now today." By a curious coincidence, the key words needed to decipher this communication were "One Retribution."

To the foregoing I will comment that I doubt very much whether "everyone in the War Department who was familiar with cryptography knew that the Vigenere was the customary Confederate cipher." From what not one of them had even heard the name Vigenere or had even seen a copy of the table, except where cases were captured in operations. I doubt whether anyone on either side even knew that the cipher used by the Confederacy had a name, or...
least of all, that a German Army reservist named Kasiski, in a book published
in 1863, showed how the Vigenere cipher could be solved by a straightforward
mathematical method. Moreover, I believe that ignorance of cryptography
and of its history was so abyssmal that the Union authorities sincerely
believed that the cipher square used by the Confederates was actually invented
by them and that possession of such a square was prima facie evidence of
membership in or association with Confederate conspiracies.

I have devoted a good deal more attention to the methods and means for
crypto-communications in the Civil War than they deserve, because professional
cryptologists of 1961 can hardly be impressed either by their efficacy from
the point of view of ease and rapidity in the cryptographic processing, or
by the degree of the technical security they imparted to the messages they
were intended to protect. Not much can be said for the security of the visual
signaling systems used in the combat zone by the Federal Signal Corps for tactical
purposes, because they were practically all based upon simple monalphabetic
ciphers, or variations thereof, as for instance, when whole words were
enciphered by the same alphabet. There is plenty of evidence that
Confederate signalmen were more or less regularly reading and solving those
signals. What can be said about the security of the route ciphers used by
the U/S/H/T/C for strategic or highcommand communications in the zone of the
interior? It has already been indicated that, according to accounts by ex-
such ciphers
U/S/H/T/C men, apparently they were beyond the cryptanalytic capabilities
of Confederate cryptanalysts; but can we really believe that this was true?
Considering the simplicity of these route ciphers and the undoubted intellectual capacities of Confederate officers and soldiers, why should messages in these systems have resisted cryptanalytic attack? In many cases the general subject matter of a message and perhaps a number of specific items of information could be detected by quick inspection of the message. Certainly, if it were not for the so-called "arbitraries" ex-cadet-words the general sense of the message could be found by a few minutes work, since the basic system must have been known through the capture of cipher books, a fact mentioned several times in the literature. It seems almost-certain that capture of but one book (they were all generally alike) would have told Confederate signalmen exactly how the system worked and this would naturally give away the basic secret of the superseding book. So we must see that whatever degree of security these route ciphers had depended almost entirely upon the number of "arbitraries" ex-cadet-words actually used in practice. A review of such messages as are available shows wide divergencies in the use of the arbitraries. In any event the number actually present in these books must have fallen far short of the number needed to give the real protection that a well-constructed code can give, so that it seems to me that the application of native intelligence, should, with some patience, be sufficient to solve them—or so it would be quite logical to assume. That such an assumption is well warranted is readily demonstrable.

During the course of preparing this lecture, my friend and colleague,
It was curiously enough, at this point in preparing
his lecture that my friend and colleague of my NSA days,
Mr. Edwin C. Fishel, a long-time member of NSA, gave me just the right
material for such a demonstration. In June of 1960, Mr. Fishel had given
Mr. Phillip Bridges, who is also a member of NSA and who knew nothing about
the route ciphers of the U.S. Army, the following authentic message sent
on 1 July 1863 from General George C. Meade, at Harrisburg, Pennsylvania,
to General Couch at Washington:

(MESSAGE TO BE FURNISHED) \Fig. 17

It took Mr. Bridges only a few hours, five or six, to solve the
cryptogram, and he handed the following plain-text to Mr. Fishel:

Thomas been it \------"Nulls"
For Parson. I shall try and get to you by tomorrow morning a
reliable gentleman and some scouts who are acquainted with a
country you wish to know of. Rebels this way have all concentrated
in direction of Gettysburg and Chambersburg. I occupy Carlisle.
Signed Optic. Great battle very soon. tree much deal \------"Nulls"

The foregoing solution is correct, save for one pardonable error:

"Thomas" is not a "null" but an indicator for the dimensions of the matrix
and the route. "Parson" and "Optic" are code names and I imagine that
Mr. Bridges recognized them as such but, of course, he had no way of
interpreting them, except perhaps by making a careful study of the events
and commanders involved in the impending action, a study he wasn't called
upon to undertake.

The foregoing message was enciphered by Cipher Book No. 12, in which
the indicator THOMAS specifies a "Message of 10 lines and 5 columns". The route
was quite simple and straightforward: "Down the 1st (column), up the 3rd; down
the 2nd; up the 5th, down the 4th."
It is obvious that in this example the absence of many "arbitraries," that is, code words with specific plain-text meanings as assigned in the codebook, made solution a relatively easy matter. What Mr. Bridges would have been able to do with the cryptogram had there been many of them is questionable. Judging by the worksheets Mr. Bridges submitted, it seems that when he was solving the message he did not realize that a transposition matrix was involved; and on questioning him as to whether he knew or suspected this when he commenced work, his answer was in the negative. He realized this only later.

A minor drama in the fortunes of Major General D. C. Buell, one of the high commanders of the Federal Army, is quietly and tersely outlined in two cipher telegrams. The first one, sent on 29 Sept. 1862, from Louisville, Kentucky, was in a cipher book where I wasn't called upon, and was externally addressed to Colonel Anson Stager, head of the Military-Telegraph-Corps, in Washington, but the internal addressee was Major General H. W. Halleck, "General-in-Chief" in our present day "Chief of Staff" role. This message was externally signed by William H. Drake, Buell's cipher operator, but the name of the sender was indicated internally. For some years, most messages for Washington were externally addressed to Stager. On receipt they were deciphered by clerks of the Military-Telegraph-Corps and the plain-text forwarded to the addresses whose names were enciphered. Here's the telegram:

COLONEL ANSON STAGER, Washington:

Austria awaits I am over to requiring orders capture blissful for your instant command turned and instructions and rough looking further shall further the Camden as of ocean September poker twenty I the to I command obedience repair orders quickly pretty. Indianapolis your him accordingly my fourth received 1862 wounded nine have twenty turn have to to to alvord hasty.

WILLIAM H. DRAKE
Rather than give you the plain-text of this message, perhaps you
would like to work it out for yourselves, for with the information you've
already received the solution should not be difficult. The message contains
one error, which was made in its original preparation: one word was omitted.

The second telegram, only one day later, was also from Major General Buell,
to Major General Halleck, but it was in another cipher book--apparently the two
books involved were used concurrently. Here it is:

GEORGE C. MAYNARD, Washington:

Regulars ordered of my to public out suspending received 1862
spoiled thirty I dispatch command of continue of best otherwise worst
Arabia my command discharge duty of my last for Lincoln September
period your from sense shall duties the until Seward ability to the
I a removal evening Adam herald tribune.*

PHILIP BRINNER

As before, I will give you the opportunity to solve this message for
yourselves. (At the beginning of the next lecture I shall present the plain-
text of both messages.)

To return to J. W. Brown, whom I've mentioned before and who gives us most

of what little sound information there is about the cryptanalytic successes of both sides,
first, let's see what the Union signal men could do with rebel ciphers. Here are
the Federals, here are some which he presents:

some statements he makes [p. 214]:

The first deciphering of a rebel signal code of which I
find any record was that made by Capt. J. S. Hall and Capt. P. A.
Taylor, reported Nov. 25, 1862. Four days later, Maj. Myer wrote
to Capt. Cushing, Chief Signal Officer, Army of the Potomac,
not to permit it to become public "that we translate the signal
messages of the rebel army".

April 9, 1863, Capt. Fisher, near Falmouth, reported that one
of his officers had read a rebel message which proved that the
rebels were in possession of our code. The next day he was
informed that the rebel code taken (from) a rebel signal officer
was identical with one taken previously at Yorktown.

He received from Maj. Myer the following orders:

*A curious coincidence--or was it a fortuitous foreshadowing of an event far in
the future?--can be seen in the sequence of the last two words of the cipher
text. The message is dated September 30, 1862; the New York Herald and the
New York Tribune combined to make the New York Herald-Tribune on March 19, 1924--
62 years later!
Next you see a photograph of an important message which you may wish to solve yourself. It was sent by President Jefferson Davis to General Johnston, on a very significant date, 11 April 1865. For ease in working on it I give also a transcription, since the photograph is very old and in poor state. I believe that this message does not appear in any of the accounts I've read.

[Fig 15]
"Send over your lines, from time to time, messages which, if it is in the power of the enemy to decipher them, will lead them to believe that we cannot get any clue to their signals."

"Send also occasionally messages untrue, in reference to imaginary military movements, as for instance, --'The Sixth Corps is ordered to reinforce Keyes at Yorktown'."

Undoubtedly, what we have here are references to the general cipher system used by the Confederates in their electric-telegraph communications, for

Note the expression "Send over your lines". This could hardly refer to visual communications. Here we also have very early instances, in telegraphic communications, of what we call cover and deception, i.e., employing certain ruses to try to hide the fact that enemy signals could be read, and to try to deceive him by sending messages for him to read, and matched by undetected

Brown's account continues [p. 215]:

In October, 1863, Capt. Merrill's party deciphered a code, and in November of the same year Capt. Thickstun and Capt. Marston deciphered another in Virginia.

Lieut. Howgate and Lieut. Flock, in March, 1864, deciphered a code in the Western Army, and at the same time Lieut. Benner found one at Alexandria, Virginia.

Capt. Paul Babcock, Jr., then Chief Signal Officer, Department of the Cumberland, in a letter dated Chattanooga, Tennessee, April 26, 1864, transmitting a copy of the rebel signal code, says:

Capt. Cole and Lieut. Howgate, acting Signal Officers, occupy a station of communication and observation on White Oak Ridge at Ringgold, Ga... On the 22nd inst. the rebels changed their code to the one enclosed, and on the same day the above-mentioned officers by untiring zeal and energy succeeded in translating the new code, and these officers have been ever since reading every message sent over the rebel lines. Many of these messages have furnished valuable information to the general commanding department.

With regard to Confederate reading of Union visual signals, Brown makes the following observations of considerable interest [p. 274].

The absolute necessity of using a cipher when signalling in the presence of the enemy was demonstrated during these autumn months by the ease with which the rebels read our messages. This led to the issuing of an order that all important messages should be sent in cipher. Among the multitude of messages intercepted by the enemy, the following were some of the more important: [p. 276]

Brown thereupon cites 25 such messages but he gives no indication whatever as to the source from which he obtained these examples or how he knew they had been intercepted. They all appear to be tactical messages sent by visual signals.

The following is also from Brown [p. 279]:

About the first of June (1864), Sergt. Colvin was stationed at Fort Strong, on Morris Island, with the several codes heretofore
The following is also from Brown [p. 279]:

About the first of June (1864), Sergt. Colvin was stationed at Fort Strong on Morris Island, until the second series of ciphers used by the rebels, for the purpose of reading the enemy's signals if possible. For nearly two weeks nothing could be made out of their signals, but by persevering he finally succeeded in learning their codes. Messages were read by him from Beach Inlet, Battery Bee, and Fort Johnson. Gen. J. G. Foster, who had assumed command of the Department of the South, May 26th, was so much pleased with Sergt. Colvin's work, that in a letter addressed to Gen. Halleck, he recommended "that he be rewarded by promotion to Lieutenant in the Signal Corps, or by a brevet or medal of honor." This recommendation was subsequently acted upon, but, through congressional and official wrangling over appointments in the Corps, he was not commissioned until May 13, 1865, his commission dating from Feb. 14, 1865.

(p-281) During the month, Sergt. Colvin added additional laurels to the fame he had earned as a successful interpreter of rebel signals. The enemy had adopted a new cipher for the transmission of important messages; and the labor of deciphering it devolved upon the sergeant. Continued watchfulness at last secured the desired result, and he was again able to translate the important dispatches of the enemy for the benefit of our commandants. The information thus gained was frequently of special value in our operations, and the peculiar ability exhibited by the sergeant led Gen. Foster once more to recommend his promotion.

(p-286) About the same time an expedition under Gen. Potter was organized to act in conjunction with the navy in the vicinity of Bull's Bay. Lieut. Fisher was with this command, and by maintaining communications between the land and naval forces facilitated greatly the conjoined action of the command. Meanwhile every means was employed to intercept rebel messages. Sergt. Colvin, assigned to this particular duty, read all the messages within sight, and when the evacuation of Charleston was determined upon by the enemy, the first notification of the fact came in this way before the retreat had actually commenced. As a reward for conspicuous services rendered in this capacity, Capt. Merrill recommended that the sergeant be allowed a medal, his zeal, energy and labors fully warranting the honor.

After the occupation of Charleston, communications was established by signals with Fort Strong, on Morris Island, Fort Johnson and James Island, Mount Pleasant, and Steymeyer's Mills. A line was also opened with the position occupied by the troops on the south side of the Ashley river.

In many of the cases cited by Brown it is difficult to tell whether wig-wag or electric telegraph messages were involved. But in one case, [evacuation of Charleston] it is perfectly clear that visual messages were involved, when Brown says that Sgt. Colvin "read all the messages within sight."

Once before in this lecture it was mentioned that the visual signalmen of each side were reading the visual signals of the other side. This led to the use, by both sides, of ciphers to protect the signals transmitted by the visual method. But in addition, discovery that Confederates operators were
Further with regard to rebel cryptanalytic success with Union messages, Brown has this to say [p.215]:

The reports of Lieut. Frank Markoe, Signal Officer at Charleston, show that during the siege thousands of messages were sent from one post to another, and from outposts to headquarters, most of which could have been sent in no other way, and many were of great importance to the Confederate authorities.

Lieut. Markoe says that he read nearly every message we sent. He was forewarned of our attack on the 18th of July, 1863. He adds regretfully, however, that through carelessness of the staff officers at headquarters it leaked out that he was reading our messages. Our officers then began to use the cipher desk. In August he intercepted the following message: "Send me a copy of rebel code immediately, if you have one in your possession." He therefore changed his code. A little later our officers used a cipher which Lieut. Markoe says he was utterly unable to unravel.

It is unfortunate that neither Lieut. Markoe, the Confederate cryptanalyst, nor Brown, the Union signalman, tells us what part of cipher this was that couldn't be unravelled. I assume that it was the Myers method with a key phrase of some length and with
successive letters, not whole words, being enciphered by successive letters of the key. But this is only an assumption and may be entirely erroneous.

In the foregoing citations of cryptanalytic successes to note first, it is significant that visual messages were intercepted and read by both sides; that Confederate telegraphic messages protected by the Vigenère cipher were read by Union personnel whenever such messages were intercepted, and that USMTC telegraph messages protected by the Route cipher were apparently intercepted occasionally but never solved.

Later I shall make some comments on this last statement, but at the moment let us note that technically the Vigenère cipher is theoretically much stronger than the Route cipher, so that we have here an interesting situation: the users of a technically inferior cryptosystem were able to read enemy messages protected by a technically superior one, but the users of a technically superior cryptosystem were not able to read enemy messages protected by a technically inferior one — a curious situation indeed.
N° 6
1st draft
INTRODUCTION TO CRYPTOLOGY-VI

Confidential
This lecture, the sixth and last in this series, deals with cryptology in the period from the end of World War I to the end of World War II (unclassified material only). The emphasis in this lecture is upon communications security (COMSEC) because most of the information given in the four preceding lectures the emphasis was largely upon communications intelligence (COMINT) but also because COMSEC in the final analysis is really more vital than COMINT.

You will perhaps recall that in the very first lecture in this series reference was made to the role that COMINT (or "Magic") played in the Japanese attack on Pearl Harbor but in the military and naval and air operations which followed that attack. This is not the place nor is there time to go into the complex problems involved in an attempt to fix responsibility for the blame for being caught off guard. Millions of words have been published on this subject and I do not propose to add to that voluminous literature whatever thoughts I may have therein.
This, the sixth and final lecture in this series on the history of cryptography, will be devoted to a presentation of events and developments of significance or importance in that history from the end of World War I to the end of World War II.

It would be entirely too ambitious a project even to attempt to compress all that should or could be told in that segment of our history of cryptography. In a nutshell, however, it can be said that the most significant and important events and developments during that quarter of a century were directly concerned or connected with the advances made in the production of more complex mechanical, electrical and electronic cryptographic apparatus and with the concomitant advances in the production of more sophisticated mechanically electrical and electronic apparatus for the solution of the messages produced by these increasingly complex cryptographic machines.

These two phases are inter-related because, for a sort of simple analogy, cryptography and cryptanalysis represent the two faces of a single coin.

It would be nice if I could go
bit into detail in regard to these increasingly complex matters but security considerations prevent my doing so because the classification of these lectures, viz., CONFIDENTIAL, is the lowest one now possible. As to the advances in the development and use of more sophisticated cryptographic apparatus I will only note at this point a comment which General Omar Bradley makes in his quiet but interesting book entitled A Soldier's Story: Signal Corps officers like to remind us that "although Congress can make a general, it takes communications to make him a commander." It is immodest for me to try to amend General Bradley's remark but this is how I wish he had worded it:

Signal Corps officers like to remind us that "although Congress can make a general, it takes rapid and secure communications to make him a good commander."

This will in fact be the keynote of this lecture. In other words, communications security or COMSEC will be its main theme and the one Dutch

But before coming to that part of our history, perhaps a bit more attention must be devoted to events and developments of cryptanalytic significance or importance during the period 1935 to 1941. By far the most spectacular and interesting of these are the ones which were so fully and drastically disclosed by the various investigations conducted by the Army and Navy very secretly while World War II was still in progress and depth secretly and openly after the close of hostilities. The investigations were intended to ascertain why we were caught by surprise by the sneak attack on Pearl Harbor by the Japanese on the morning of 7 December 1941. They were also intended to fix the blame on whoever was responsible for the debacle. I don't think I should even attempt to give you my personal opinion on these complex questions, which were studied by seven different boards within the Services and finally by the Joint Congressional Committee on the Investigation of the Pearl Harbor Attack. I mentioned the latter investigation in my first lecture and now I must add to what I then said. The Committee published its findings...
conclusions and recommendations in 1946. It began its work in September 1945 with secret hearings but on 70 days subsequent to 15 November 1945 up to and including 31 May 1945 open hearings were conducted in the course of which some 15,000 pages of testimony were taken and a total of 183 exhibits received incident to an examination of 43 witnesses. The Committee put out a final Report of 580 pages to accompany a set of 39 volumes of testimony and exhibits. In the Report there were one by the Majority (signed by six Democratic members and two Republican members) and one by the Minority (signed by two Republican members). The Minority Report was not nearly as long as that of the Majority but it brought into focus certain troublesome points which still from the subject of acrimonious discussions and writings who believes the attack was "engineered" by President Roosevelt for this history the interesting fact is that both the Majority and Minority Reports contain glowing tributes to the role played by COMINT before and during our participation in World War II. In my first lecture I present a brief sketch in this regard taken from the Majorit
Report, but here is what the Minority Report says on the subject:

6. Through the Army and Navy intelligence services extensive information was secured respecting Japanese war plans and designs, by intercepted and decoded Japanese secret messages, which indicated the growing danger of war and in-creasingly after November 26. The imminent of a Japanese attack.

With extraordinary skill, zeal, and watchfulness the intelligence services of the Army Signal Corps and Navy Office of Naval Censorship broke Japanese codes and intercepted messages between the Japanese Government and its spies and agents and ambassadors in all parts of the world and supplied the high authorities in Washington reliable secret information regarding Japanese designs, decisions, and operations at Rome, in the United States, and in other countries.

Although there were delays in the translation of many intercepts, the intelligence service had furnished reports which indicated a large number of Japanese messages which clearly indicated the growing desire of the Japanese Government on or before December 7, 1941.

The Majority Report made five main recommendations, of which the second is of special interest:

That there be a complete integration of Army and Navy intelligence agencies in order to avoid the pitfalls of divided responsibility which experience has made so abundantly apparent; that upon effecting a unified intelligence office be selected for intelligence work who possess the background, penchant, and capacity for such work, and that they be maintained in the work for an extended period of time in order that they may become steeped in the ramifications and refinements of their field and employ their reservoir of knowledge in evaluating material received. The assignment of an officer having an aptitude for such work should not impede his progress nor affect his promotions. Efficient intelligence services are just as essential in time of peace as in war and this branch of our armed services must always be accorded the important role which it deserves.

\[\text{P. 253 of Report of the Majority}\]
I assume that the gist of this has been confirmed, in that the recommendation has been carried out. It will be seen that the recommendation has been carried out. In this connection I think it will be of interest to cite what the distinguished commander whom I have already mentioned, General Omar Bradley, has to say on this point.

In these intelligence activities at Allied Forces Headquarters, the British easily outstripped their American colleagues. The tenacious years of prewar studies the British had devoted to areas throughout the world gave them a vast advantage which we have never overcome. The American army's long neglect of intelligence training was soon reflected by the inexperience of our initial undertakings. For too many years in the preparation of officers for command assignments, we had overlooked the need for specialization in such activities as intelligence. It is unrealistic to assume that every officer has the capacity and the inclination for field command. Many are uniquely qualified for staff intelligence duties and instead would prefer to devote their careers to those tasks. Yet instead of grooming qualified officers for intelligence assignments,
Person is called a "general" or "specialist." But their operating family is called a "central office." In the beginning, "intelligence" was used to mean knowledge gained through personal experience or general knowledge. It was not considered important enough to be a formal part of training. As the importance of intelligence grew, so did the need for trained personnel. Training programs were developed for officers, and new career paths opened up for those interested in intelligence. We developed a new appreciation for the importance of intelligence in our own careers, and we pitched our enthusiasm and energy towards its advancement.
and operations such as are involved in modern engineering, electrical communications, guided missiles, rockets, etc. etc.? How much can be learned without first-hand experience in the tricky business of ordinary military intelligence operations let alone the much more complicated business of cryptography as applied in modern military operations?

But let us leave these speculations, interesting as they may be, and continue with our history. Let us first dispose of the COMINT area of their history.
However, there is one small but extremely significant piece of information involved in this matter and I will say a few words about it. You will recall that in the first lecture I called to your attention an article which appeared in the 17 December 1945 issue of TIME magazine and which was based upon a letter from General George C. Marshall, then Chief of Staff of the U.S. Army, from Germany, written to Governor Thomas E. Dewey, Republican candidate for President in the 1944 election campaign. In that letter, General Marshall practically begged Governor Dewey to say nothing during the campaign about a certain piece of information which General Marshall had reason to believe had been "peeked" to him by persons not authorized to disclose it. The information dealt with the fact that the U.S. had been reading Japanese codes and ciphers even before the attack on Pearl Harbor. The vital point which General Marshall wanted to convey to Governor Dewey was that not only was that piece of information which had surreptitiously been given to Governor Dewey true...
but more important were the facts that (1) the war was still in progress, (2) the Japanese were still using certain of the pre-Pearl Harbor cryptosystems, and (3) the U.S. was still reading these systems as well as certain other enemy communications. Therefore, it was vital that Governor Dewey ask me the information which had come into his possession as to our reading secret Japanese communications prior to the attack on Pearl Harbor. I said in that first lecture that I might later give further extracts from TIME’s account and, here they are. I continuing the extracts printed on pages 3, 4, and 5 of the first lecture, here they are:

The Marshall-Dewey correspondence is so important in cryptologic history that I feel that the whole of it should be included in this brief history. When the letter was written it was
Not more importantly the letter was still unknown.

The letter came into the possession of the Joint Congressional Committee on the Investigation of the Attack on Pearl Harbor. It was published, by authority of the Committee, put on sale by the Superintendent of Documents of the Government Printing Office. The Marshall-Daney

were indeed such a sensation that LIFE magazine

printed the whole of it in its issue of 17 December 1945, with the following introduction:

So far as I am aware, it has never disclosed who gave Governor Daney the information. But it is a fact that Governor Daney as a patriotic citizen, responded to General Marshall's request —
made no use of the secret information during the campaign, no other it you force I am aware.
TIME's account specifically states that Dawes "held his tongue. The War Department's most valuable secret was kept out of the campaign."

Whatever
Except for a change in the first two paragraphs this letter is identical with the first letter. The
chain letter was published in newspapers and
the second letter year reported substantially
the rest of the first letter except for the first two
paragraphs.

The last
life failed to note that two sentences in
the penultimate paragraph of the "First Letter" were
omitted from that paragraph in the "Second letter." But
there is no explanation for the omission. Perhaps it was
simply for the sake of brevity, but this seems improbable.

There is no explanation for the omission:
perhaps it was simply for the sake of brevity.

In my first lecture (p. 4 of NSA Technical
Journal No. 7, 1944) I called attention to the fact that the
account given in the TIME article gives credit to the Army
Cryptanalysts for providing the secret communications
Intelligence "which enabled the Navy to win such
spectacular battles as those of the Coral Sea and Midway,
and to waylay Japanese convoys," whereas the credit
for the communications intelligence which enabled our Navy to win these battles was produced by Navy cryptanalysts. One cannot blame him for making such a bad error because the letter which General Marshall's letter itself, several years ago, I asked General Marshall's letter to Governor Dewey and who was at the time a high 
level officer in 21-2 who had prepared the General Marshall's letter and I was told that the letter which 
was prepared for General Marshall's signature did not meet with the General's whole-hearted approval 
and that the General himself had modified it perhaps that is how the error to which I have 
referred crept into the letter. One could hardly 
expect General Marshall to be entirely familiar with 
the technical cryptanalytic details involved except in the very busy days preceding the pressure of events, the differences between the enemy 
cryptanalytic organizations and our own. 

Since the disclosures made at the front 
Congressional investigation as far as concerns the important accomplishments of the two services accomplished before and after the
It is possible, though it may be probable, that certain
COMINT regarding the Battles of the Coral Sea and
Midway came from messages read by Army
Cryptanalysts, and this is what confused General
Pearl Harbor attack in the field of communications intelligence, much has been written and is now in the public domain regarding those accomplishments. Fortunately, but no technical details of significance have been developed. Hints have and there are in abundance in the many books and articles that have been published by U.S. writers since the end of World War II, but more than hints of the great lamented COMINT work in U.S. military and naval processes are to be found in books and articles published by officers of the beaten Japanese and German and Italian armed forces. Time does not permit any citing of these hints or definite statements, but the following are of particular interest, because they concern the battle of Midway, which is considered, the one which turned the war in the Pacific from victory to one of conspicuous defeat:

The first extract above is the part that most interested us at the moment, and in particular, the portion which refers to the negatively bad and ineffective functioning of Japanese intelligence. The Japanese author is a bit too severe on the Japanese intelligence organization.
If Admiral Yamamoto and his staff were vaguely disturbed by the persistent bad weather and by lack of information concerning the location of the enemy, they would have been truly dismayed had they known the actual enemy situation. Post-war American accounts make it clear that the United States Pacific Fleet knew of the Japanese plan to invade Midway even before our forces had sortied from home waters.

As a result of some amazing achievements by American intelligence, the enemy had succeeded in breaking the principal code used in use by the Japanese Navy. In this way the enemy was able to learn of our intentions almost as quickly as we had determined them ourselves.

The distinguished American naval historian, Professor Samuel E. Morison, characterizes the victory of United States forces at Midway as "a victory of intelligence." In this judgment the author fully concurs, for it is beyond the slightest possibility of doubt that the advance discovery of the Japanese plan to attack was the foremost single and immediate cause of Japan's defeat. Viewed from the Japanese side, this success of the enemy's intelligence translates itself into an

This because their cryptanalysts were up against much more sophisticated cryptosystems than they were qualified to solve. In fact, even if they had been extremely adept in cryptanalysis, it would have been of no avail — U.S. high-level communications were protected by cryptosystems of very great security.

This brings us to a subject which is of highest importance — the phase which deals with communications security, or COMSEC, and I shall confine myself largely to its historical background in the U.S. Armed Forces. The background is a very broad one because it should include the background of the developments of each of the three components of COMSEC: cryptosecurity, transmission security, and physical security of cryptomaterials. But since time is limited and because I think you would be more interested in the phases pertaining to cryptosecurity, I will omit references to the history of the other two components. And even in limiting the data to cryptosecurity, I will have opportunity only to give some of the highlights of the development of the items that comprise our cryptomaterials, making our comments on the history of the development and im-
provenance of our techniques, procedures and practices, all of which are extremely important.

Coming directly to the history of the development of both cryptomaterials themselves, I hardly need reiterate what was pointed out in previous lectures as to the profound effect of the advances in the science and art of electrical communications in the 20th century. These advances had a direct effect upon military communications and an indirect effect upon military cryptology. Hand-operated ciphers and, of course, codebooks became almost obsolete with the need for greater and greater speed of cryptographic operations to match as much as possible the very great increase in the speed of communication thought about by inventors and improvements in electric telegraphy. The need for cryptographic apparatus and machines became quite obvious.

I shall begin the story with a definition which you will find in any good English dictionary, a definition of the word "accident." You will get the point of what may seem to you to be merely another of my frequent digressions from the main theme, but if it be a digression I think you will...
nevertheless find it of interest. The word "accident" in Webster's Unabridged Dictionary is defined as follows:

1. Literally, a befalling.
   a. An event that takes place without one's forethought or expectation; an undesigned, sudden, and unexpected event.
   b. Hence, often, an undesigned and unforeseen occurrence of an afflictive or unfortunate character; a mishap resulting in injury to a person or damage to a thing; a casualty; as, to die by an accident.

There are further definitions of the word "accident" but what I've given is sufficient for our purposes. But why define the word; what has it to do with COMSEC?

During our participation in World War II, the President of the United States, accompanied by many of his highest level assistants, journeyed several times halfway around the world. He journeyed in safety—by land with no accident.

On the other hand, Admiral Isoroku Yamamoto, Commander-in-Chief of the Japanese Navy, started out on an official enterprise, Navy conference figure stating that the Admiral...

[Continued over]
had met a glorious end while directing operations in a naval engagement against superior enemy forces. But we know that this was simply not true; Admiral Yamamoto "met with an accident." But some bright person, it was the late Jimmy Walker, when mayor of New York City, I think, who said that "accidents don't just happen — they are brought about." No, Admiral Yamamoto didn't die simply by accident; he died because our Navy just took the schedule of his trip down to the last detail so that it was possible to set up an ambush with high degree of possible success.
REF ID:A62831

~~ ~D-4. ~~a-~----;

e:

-}o ..


assigned to make the interception over Bula, 35 miles short of Belleau, Yamamoto's plane, a Betty, accompanied by another Betty, and covered by six Zekes, took in sight exactly on schedule, and hit Col. Thomas J. Lapham's very plane. He dove on it and shot it down in flames. The other Betty was also shot down for good measure, plus one of the Zekes. ... We bottled up the story, of course. One obvious reason was that we didn't want the Japs to know that we had broken their code. ... Unfortunately, somebody took the story to Australia, whence it leaked into the papers, and no doubt eventually into Japan. ... But the Japs evidently did not realize the implication any more than did the hattately we continued to break their codes.

Admiral Nolten's story contains a good many more instances of cryptographic significance, part of the Japanese's well as excellent control on the part of their Navy. Other authors, both American and Japanese, cite similar instances. One Japanese author states, categorical language that Japan was defeated because of poor COMSEC on the part
of the Japanese Navy and good combat on the part of the American Navy.

But lest you get the impression that enemy intelligence agencies had no success at all with the inner communications of U.S. Armed Forces, let me tell you that they did have some success and in certain instances very significant success. There is not time to go into this disappointingly disheartening statement but I can say that as a general rule the successes were attributable not to technical weaknesses in U.S. cryptosystems but to improper use in the case by unskilled or insufficiently trained cryptographic clerks. I say it as well. All you right now is that this has been true for a great many years in a form almost out of help from human error.

In direct conflict with Spinoza and his ideas on mathematics and physical science are what we call matters of fact. Because as Francis Bacon said in The Advancement of Learning: This Art of Cyphering is both a useful Art of Decyphering; by supporting unprofitable

But as things are, of great use for suppose that Cyphers were well managed, there be
Multitudes of them which exclude the Discipline.

But in regards of the rawness and unskillfulness of the handers, through which they passe, the greatest Matters, are many times carried in the weakest Cyphers.

When electrical and particularly radio transmission entered into the picture, electrical regards to communications security had to be taken into account, but many commanders have failed to realize how much intelligence can be gained from a study of the procedures used in transmission, the direction and flow of communications, the call signs of the transmitting and receiving stations, direction etc., all without solving the slightest communications even if they are in cryptic form. Following are a couple extracts from a document entitled "German Operational Intelligence," published in April 1945 by the German Military Document Section, Combined British, Canadian, and U.S. Staff:

(P.8) "Signal intelligence, etc., as per card..."

(P.8) "Most of their signal intercept success..."
(P.22) "Importance of Signal Intelligence during the Normandy Invasion. During the invasion etc"

A great many examples of intercepted messages of tactical content are cited in the above-mentioned document, which is replete with information of deep interest although the document was originally issued with the lowest security classification than in use (U.S. "Restricted", British-Canadian "For official use only"). I wish there were time to quote or greater length from this useful brochure.

Here is part matter on p. 8 of this.
Until the advent of electronic cryptography, most cryptographic apparatus and devices were built upon or around circular mechanisms or cipher wheels, cipher disks, etc. The very earliest such disks appear in a treatise by an Italian cryptologist named Alberti whose Trattato in cifra was written in Rome about 1470. It is the oldest treatise on cryptography known to exist. The modern counterpart is the Enigma machine, which was used extensively during World War II. The Enigma machine was more complex than any other cryptographic device of its time. It was invented by the German Navy and later used by the military forces of other countries, including the Soviet Union and Japan.

The Enigma machine used a series of three or more rotors, each of which could be set to any one of 26 positions, corresponding to the 26 letters of the alphabet. The rotors were turned by hand or by motor, and each rotation changed the code. This made it very difficult for the enemy to decipher the messages.

The Allies were able to crack the Enigma code during World War II, which significantly contributed to their victory. However, the Enigma machine was not the only cryptographic device used during the war. Other devices, such as the Lorenz machine, were also employed by various countries.

Despite the advances in cryptography, the principles of cryptography have remained the same for centuries. The study of cryptography continues to evolve, with new techniques and technologies being developed to ensure secure communication in an increasingly digital world.
Here's a picture of the vernacular cipher disk (Fig. 8) and the explanation.

And you will remember that the Signal Officer of the Confederate Signal Corps mechanized the Vigenère cipher and put it out in the form of a cylinder (see Figs. 13, 14, and 15) of Lecture No. 14). The cipher disk used by the Signal Corps of the U.S. Army during the period from 1910 to 1920, that is, during the period of World War I (Fig. 13), was nothing but a white celluloid variation of the original disk of the vintage of 1870 except that it was even simpler than its progenitor because in the latter the cipher alphabet produced were mixed alphabets whereas in the Signal Corps disk the cipher alphabets are fixed several standard sequences.
was patented in 1924 (Fig. 11). Here you have an even greater improvement over the Signal Corps version—a blank is added to both sequences so that the space between words could be emphasized. This is a fatal weakness if seen in the cipher text, in the Huntington device, the spaces between words would be emphasized, but the cipher text would have space signs, although they would not correspond to the actual spaces in the plain text.

It is interesting to note that during the days when the German National Socialists were banned as an organization Hitler and his cohorts used this variation of the old desk—it had the 10 digits on both the outer and the inner sequence (Fig. 13).

The first significant improvement on the old cipher desk was that made by Sir Charles Wheatstone who, sometime before 1874, invented and described his cipher device which he called a cryptograph in a volume entitled The Scientific Papers of Sir Charles Wheatstone, published by the Physical Society of London. Here is a picture of Wheatstone's device (Fig. 13). What Sir
Charles did was to make the outer circle 1 letters (for the plain text) comprise the 26 letters of the alphabet plus one additional character to represent "space." The inner circle, for cipher equivalents, contained only the 25 letters of the alphabet and these could be disarranged in a mixed sequence. Two hands, like the hour and minute hands of a clock, were provided, under control of a differential gear mechanism, so that as the long hand is advanced a complete circuit of the face of the cryptograph the short or "hour" hand advances one space or segment or letter. As the inner circle of letters on the face of the cryptograph, in Fig. 13, for example, the plain-text letter C is represented by the cipher letter A. If the long hand is now advanced clockwise direction for one revolution, it will be represented no longer by A but by G.

In encipherment the long hand is always moved in the same direction (clockwise, for example) and is placed over the successive letters of the plain-text message, the cipher equivalents being recorded by hand to correspond with the letters to which the short hand points at each encipherment.
In this way, successive identical letters of the plain text will be represented by different letters in the cipher text, depending upon how many revolutions of the long hand intervene between the first and subsequent appearances of the same plain text letter. Correspondents must naturally agree upon the mixed alphabet used in the inner circle and the initial position of the two hands at the beginning of the encipherment of a message. In decipherment, the operator, having noted the cipher letter in the inner circle and noting the plain text letter to which the long hand points in the outer circle.

During World War I, some time in 1917, the British Army resuscitated Wheatstone's cryptograph and improved it both mechanically and cryptographically. Here is a picture of the device (Fig. 14) in which it will be seen that the inner circle is juxtaposed in an essential manner against the outer circle of fragments
The property are made of a substance which letters may be written in pencil or in ink. In this, Wheatstone device both sequences of letters are now mixed sequences. Making the inner circle also a mixed sequence, considerable degree of security to the cipher. When it was proposed that all the allied armies use this device for field communication, and its security had been approved by British, French, and American cryptologists (both at GNA-AEF and at Washington) an opportunity to agree or disagree with the assessment of these cryptologists was given me while I was able to show that the modified Wheatstone cryptograph was still insufficiently secure for serious purposes and the devices, thousands of which had been issued, were withdrawn. If you are interested in the method of solution, you will find it in Reader's Digest Publication No. 20, entitled "Several Machine Ciphers and Methods for Their Solution." A better method of solution was devised by me some years later.
museum requesting that he lend the device for a short period to me as principal cryptanalyst of the War Department. Imagine my surprise and pleasure when I unpacked the box sent to me, and found a device, beautifully made and encased in a fine mahogany case, with its inventor's name and date engraved on the face of the machine, which was nothing but another version of the Wheatstone Cryptograph. Technically, it was similar to the British modification except that the outer sequence had 33 characters instead of 26, so that the differential gear method of operating on the plates 27 to 26 was now on the plates 33 to 31. Journal Thomas Davis Ward was an American army colonel, first Chief of Ordnance, and an associate of Eli Whitney, had anticipated Sir Charles Wheatstone by over 60 years in this invention. He also anticipated the British in their modification of Wheatstone's cipher because in the Wardsworth device both alphabets could be made mixed sequences. This is shown in Fig. 16 as regards the outer sequence and below the inner one. Could also be rearranged but I am now not sure as to its point. But returned the device.
a good many years ago and it is now on display in the Eli Whitney Room of the New Haven Historical Society's Museum.

The next device I will bring to your attention is shown in Fig. 17, invented by a French Army reservist, Commandant Bagerias, who tried to get the French Army to adopt it. He was not successful and included a description of his device in a book published in 1781 in Paris. He had, however, described his device in an article entitled "Cryptographe à 20 rondelles—alphabets (25 letters per alphabet," published in 1891. In this device there is a central numbered shaft on which can be mounted 20 disks on the periphery of each of which can be mixed alphabets of 25 letters each. The disks are assembled on the shaft in some prearranged or key sequence. The first 20 letters of the plain text of a message are aligned, as seen in Fig. 17 (JE SUIS INDECHIFFRABLE "I am indecipherable") and as cipher text one may select any one of the other 24 lines of letters, then the next set of 20 plain-text letters is aligned, etc. To decipher a...
indication that the letters on the order sequence are wider changeable, so that of Fig. 16 seems to indicate that those on the inner sequence are not, this may be an illusion.
message, one takes the first 20 cipher letters, aligns them on the device (the disks having been assembled on the shaft in accordance with the prearranged key sequence) and then one turns the whole cylinder, searching for a line of plaintext letters which form intelligible text. Then will be only one such row, and the letters are recorded. Then the next 20 letters of cipher are aligned, etc.

In 1893 another French cryptologist, the Marquis de Viaire, showed how messages prepared by means of the Bagieric's cylindrical cipher could be solved. Maybe that is why Bagieric wasn't too successful in his attempts to get the French Army to adopt his device. But in the U.S. there were apparently none who encountered either what Bagieric or de Viaire's wrote on the subject. Capt. Parker, when I have mentioned in a previous lecture, Hitt, U.S. Army, in 1915 invented a device based upon the Bagieric principle but not in the form of disks mounted upon a central shaft. Instead of disks, Hitt's device used sliding strips and there is a picture of his first model which he presented to me some time in 1923 or 1924 (Fig. 18). But I learned about his

L'Art de chiffrer et de déchiffrer les dépêches secrètes. Paris, 1893, p. 100
while still at Riverbank,
sometime

during 1937 I solved one challenge message put
up by Mrs. Hitt. I didn't immediately learn from de Vries
in accomplishing the solution (which brought a box
of chocolates to Mrs. Friedman) because at that
time I hadn't come across the de Vries book. I
solved the message by guessing the key. Mrs. Hitt
employed to arrange her strip alphabets. She wasn't
wise to the quirks of inexperienced cryptographic
clerks; she used RIVERBANK LABORATORIES as
the key, just as I suspected she would. The
device she brought with her was an improved model:
the alphabets were glued to strips of wood,
as seen in Fig. 19.

Capt. Hitt brought his device to the
attention of the then Major Maudsley, whom I have
also mentioned in a previous lecture and who was
then on duty in the Office of the Chief Signal Officer
in Washington. There is some question as to whether
it was Hitt who brought his device to Maudsley's
attention; Maudsley later told me that he had
independently conceived the invention and, moreover,
had made a model using 36 disks instead of
ships. I have that model, a present from General
Maunderone many years later. It is made of brass, very heavy, on the peripheries of the disks of which he had engraved the letters of his own specially-derived alphabet. In 1919, after my return to Riverbank from my service in the AEF, Maunderone sent Riverbank the first 25 letters of a set of some 25 or more beginnings of messages ciphered by his device and alphabet. He also sent the same data to Major Yardley, in G2. Nobody ever solved the messages, even after a good deal of work and even after Maunderone told in two consecutive words in one of the test challenge messages, "many years later I found the reason for our complete lack of success, when I came across the plain texts of those messages in a dusty old file in the OS SigO. Here is a picture of the beginnings of the first six messages (Fig. 20). Maunderone, when I chided him on the unfairness of his challenge messages, told me that he had not prepared them himself—he had an underling (Major Fowler was his name; I still remember it!) prepare them. In our struggles to solve the challenge messages, assumed that they would contain the usual sorts of words found as
the initial words of

military messages. It was the complete failure by

Enigma and G-2 to solve the challenge messages

that induced Maudsley to go ahead with the
development of his device. It culminated in what

became known as Cipher Device Type M-94. Here is

a picture of it (Fig. 21). That device was used for

at least 10 years in the Army and Navy.

In 1922, a wartime colleague, the late

Capt. John M. Manley (Prof. and Head of the Department of

English at the University of Chicago) brought to my

attention a photocopy of a holographic manuscript

in the collection of Jefferson Papers in the library

of Congress. It consisted of two pages, and there is a

picture of the second page (Fig. 22) showing Jefferson's

basic for calculating the number of permutations the set of

36 wheels of his device. He didn't attempt to make

the multiplication; he didn't have an electronic

computer—for the total number is astronomical

in size. Jefferson anticipated Babbage by over

100 years.

It soon became apparent to both the

Army and the Navy cryptologists that a great amount

in cryptography would be obtained if the alphabet

-15-
of the M-94 device could be made variable instead of being fixed. There began efforts to develop a practical instrument based upon this principle. I won't take time to show these developments but will show the final form of the Army Ship Cipher Device Type M-138-A (Fig. 23). This form used our aluminum base into which channels were cut to hold paper cardboard strips of alphabet which could be slid easily within the channels. It may be interesting to you to learn that after I had given up in my attempts to find a firm which would or could make such a ground device in quantity, Mrs. Friedman succeeded on behalf of her own group in the U.S. Coast Guard. The aluminum Ship Cipher Device Type M-138-A was used from 1935 to 1940 or 1942 by the Army, the Coast Guard, and the State Department. It was used as a back-up system even after the two services as well as the Department of State began employing devices of the so-called "hand-operated" type. They can really be considered as being "machines," just of the employing mechanically driven type. However,
alphabetic sequences can be mounted so that a constantly-changing series of cipher alphabets are produced. We come now to a type of apparatus which can be called a machine, such as the one shown in Fig. 24, called the Kryha, the name of its German inventor, who unfortunately committed suicide a few years ago, perhaps because he failed to make a success of his invention. The Kryha has a fixed, outer circle against which is juxtaposed a rotatable circle of letters. Both sequences of letters can be made mixed alphabets (the segments are removable and interchangeable on each sequence). The handle at the right serves to wind a rather powerful steel spring which drives the notching mechanism on which the letters of the inner circle are mounted. In Fig. 25, can be seen something of the inner works mechanism. The large wheel at the right is seen has segments some of which are open or closed, depending upon the "pathing" or key. This wheel controls the angular displacement or "stepping" of the circular rotating platform upon which the cipher
The negative is mounted in a plastic holder, and an initial imprint is made on it. The composition of these alphabets is governed by some key or process, but other prearrangement of the cipher alphabets must be recorded by hand. After each enunciation, the button you saw in the center of the panel in the proceeding Fig. 24 is pushed down, the inner wheel 1, 2, 3, 4... etc. up to 7 steps and the next letter is enunciated, etc. The picture I've shown you applies to the latest model of the Kyrpa, as regards the first model, which came on the market sometime in the 1920's, a German mathematician produced an impressive brochure showing how many different permutations and combinations the machine afforded. Here's a picture of a couple of pages of his dissertation (Fig. 26), but even in those days, cryptanalysts were not too impressed by calculations of this sort. With modern electronic computers, calculations have become of even less significance.

Let us now proceed to some more...
complex and more secure machines. In this next machine which represents a slide (Fig. 27) you see a rather marked improvement by a Swedish cryptographic firm. It is mechanical - a machine designated as Cryptographa Ball. Here for the first time you see a cryptographic machine - a keyboard similar to that of an ordinary typewriter. Depressing a key on this causes a lamp to light under one of the letters on the indicating bank above the keyboard. At the back of this machine can be seen four wheels in front of two rear wheels. The four are the rotating elements which drive the two rear wheels, the latter are electrical commutators that change the circuits between the keys of the keyboard and the lamps of the indicating board.

I must show you the internal works of this machine which control the rotating elements and explain how the wheels themselves change the machine, but I must show you the next step in cryptographic machines, which made it possible to eliminate the tedious job of recording by hand on paper the results of decipherment desipherment, by a printing mechanism which was associated with the cryptographic machine.

Here is a slide (Fig. 28) which shows the assembly - the B-211 connected to a Remington typewriter modified to be actuated by impulses from the crypto-
graphic machine. Of course, the next step would be to make the recording mechanism an integral part of the cryptographic machine. Thus you can see in the next slide (Fig. 30), in which the four rotating members referred to in connection with Fig. 27 and which control the two commutators also mentioned in connection with Fig. 27 are clearly seen. The mechanism at the right controls the printing wheel in front of the slide-box mechanism and causes the proper letter to be printed upon the tape seen at the front of the machine.

Now we come to the next and very important development, one first conceived by an European inventor. This was followed soon by an American inventor. In this advance the circuits between the keys of the keyboard and the lamps of the indicating board are varied by rotating electrical members called rotors, interposed between fixed electrical members called stators. In Europe the first of such machines put upon the market for purchase by anyone desiring one is shown in the next slide (Fig. 31). The machine was appropriately named the ENIGMA — for solution of messages encompassed by its means was believed to be impossible in nearly 20.
In Fig. 1 at the left is seen the machine with the top cover plate removed. At the front is the keyboard; above it the indicator board, consisting of lamps underneath glass disks upon which letters have been inscribed. Above the metal indicator board are seen the panes of glass matched wheels. At the right in Fig. 1 the top cover plate has been removed, exposing the internal machinery. Three rotors or connection rings in cascade can be seen attached to notched rings. The rotors are rotatable and change the circuits between the keys of the keyboard to the lamps of the indicator board. In such a rotor there is a circle of contacts on the left face and a similar circle on the right face; wires passing through the rotor connect the contacts on the right face to those on the right face. The letters on these panes of glass are the letters of the alphabet which letters can be seen through small windows in the cover plate so that the rotors can be aligned to an initial setting. Used the expression "in cascade" a moment ago which simply means that the current passes through all three rotors before reaching
and the contacts are connected to switches operated by means of the 26 keys of the keyboard. The connections between the 26 contacts and those switches of the keyboard are fixed.

equally spaced. These are also has a circle of 26 contacts, but only on its right face. But the stator is also rotatable and its position can also be seen through a window (labeled 3 in Fig. 1(1)), so that the initial setting of the stator and the rotor can be seen through the four windows. The initial settings of these four elements constitute the key for the starting point in exploring operations.
a lamp of the indicator board. In the ENIGMA, the current exits from the last rotor at the right and enters into another rotor having 26 contacts, but only on its left face. This rotor is fixed or non-rotatable, and 13 of its contacts are connected to internal wires, connected to the inner rotor by wires passing through the stator. This stator serves to return the current from one of the 26 contacts on the right face of the right rotor to the rotor contact on the right face of the left rotor. Then the circuitry in this machine insures that if \( A_p = K \), then \( K_p = A_r \). That is, the cipher process is reciprocal in nature. It also has as a consequence that no letter can ever be itself shifted by \( A_p \), for example, can never be represented by \( A \), no matter what \( A \) happens to the two-letter rotor and the left-hand rotor at the same time. Of all the other 25 letters of the alphabet, the three rotors are interchangeable, or that six permutations arrangements of these rotors is the maximum. Since in this construction the rotors cannot be inserted in an "upside-down" position. This renders such machines useless, for the letters are made so that they can be inserted in either an
"rightside-up" or "upside-down" position. This makes possible a maximum of $6 \times 4 \times 2 = 48$ permutations of the three rotatable rotors. The right-hand stator can be moved only by hand, the reflector at the right is fixed in this model of the ENIGMA. Depressing the keys of the keyboard causes the first rotor to advance one step, thus changing the circuit from the left-hand stator through the rotors to the reflector, then back through the rotors to the left-hand stator, thus causing a second depression of the same key to produce a different cipher equivalent. It won't take the time to tell you about how the rotors are caused to advance, so that every thousand rotors can be enciphered before the windlass settings of stator and rotors return to their initial alignment (the total number is not in this case 26 or 17576 but $26 \times 25 \times 26$ or 11,900, for technical reasons of which there isn't time to explain.) Power for the electrical circuits is provided by small dry cells in the box at the upper right in Fig. 31 (II).
I process in sales, but it was by no means spectacular. When Hitler came into power, further sales were prohibited, for reasons that must be omitted in this lecture. Suffice it to say that the Enigma became the basis for machines used by the German Armed Forces in World War II.

In the U.S., a California inventor named Kelner independently conceived a machine similar to the Enigma but with some important differences: the cipher alphabet produced by it were not reciprocal, and moreover, a letter could represent itself in the cipher text. Kelner managed to avoid these two weaknesses by an intricate plate which could be set for enciphering and deciphering. Here is a plate (Fig. 33) which shows Kelner's very first model, which he constructed for communications of the Ku Klux Klan. You will note that in this model there was but one rotor, also, the cipher machine was connected to an electric typewriter so that hand recording was no longer necessary. Kelner interested one Navy in his machine, and built the 5-rotor model which you see in this slide (Fig. 34). These rotors are interchangeable and can be inserted "right side up" or "upside down." The writing could be readily changed. But this was not a printing
The virtue of the Navier machine was that the
wiring in the rotor were variable, a feature not
incorporated in the ENIGMA rotor.
Army developed at the Signal Corps Laboratories at Ft. Monmouth a machine known as Converter M-134, and became a side (Fig. 35) showing what it looked like.

At first thought, the Navy dropped magnetic communication as a Navy problem, but then built several naval models for Navy and Army.

Navy was not competent to build what Navy wanted and wanted what Army was not competent to build. Therefore, Navy dropped magnetic communication.

Navy then decided to go into the method used by Major Van Norden. The Navy gave me the necessary documents, which I did not think worthwhile, and the Navy was unable to study the method of the Office of Naval Intelligence. After some research, the Navy gave me a challenge, which we solved.

Navy Office of Naval Intelligence asked me to study the method of the Office of Naval Intelligence. After some research, the Navy gave me a challenge, which we solved.

I worked with the upper left, the Office of Naval Intelligence, and sent a number of documents to the Office of Naval Intelligence, which would be available to the Office of Naval Intelligence.
machine which was developed and produced by the Teleprinter Corporation in Chicago. This machine was very successfully used by all our armed forces from 1940 to the end of World War II and for some years thereafter. This was a rather large and expensive machine that was used for very last minute in field operations. The Army became interested in a small mechanical machine invented by a Swedish engineer, named Hagelin. Modifications designed by the Army were incorporated in the machine, and over 100,000 of them were manufactured by the Smith-Corona Typewriter Co. at Sharon, New York. Here's a slide (Fig. 36) showing the converter M-209, which was used by all our armed forces in World War II. When properly used, it gave a high degree of security, even in improperly used, as was often the case, its security was rather illusory. This machine operates on what is termed the key-generator principle, and when two or more messages are enciphered by the same key stream or portions thereof, detection is relatively simple matter but I can't go into that now.

With the world wide use of teleprinter equipment, the need for a reliable and practical, or integrated cryptographic mechanism to be associated with the teleprinter arose. The first development of this sort in the U.S. is shown in this slide (Fig. 38), was that by the American
and Telephone Co. in 1918, as a more or less simple but ingenious modification of its ordinary printing telegraph.

First, a few explanatory words about the letter may be useful. It is based upon the use of two elements of two different kinds to represent characters of the alphabet. These elements may be positive and negative currents, instantaneous in the presence and absence of current.

Here is a slide (Fig. 39) which depicts the Baudot code, which is transmitted to the printer by perforations in the paper tape in which there are holes...
designated as the ECM Mark II, ECM standing for "electric cipher machine" in the Army, it was designated as the SIGABA, in accordance with a nomenclature in which cryptographic materials are given short titles beginning with the initial nomenclature SIG.

The ECM - SIGABA is a rather large machine requiring a considerable amount of electric power and much too heavy to be carried by a single operator performing field service. It was safeguarded with extreme care and under strictest security regulations during the whole period of World War II operations. None of our Allied were permitted to have even to see the key alone even in order to facilitate inter-communication between the British. An adaptor was developed so that, by the use of the latter in connection with the ECM - SIGABA, messages could be exchanged in the British cipher possessed with a British machine called TYPEx, which an adaptor cryptographically equivalent to the American one had been developed. This system of inter-communication worked satisfactorily securely.
Certain improvements in the method of usage and certain new components to be associated with the ECM - SIGABA for automatic decipherment by perforated tapes were introduced during the wartime employment of these machines. But the SIGABA - ECM as originally developed and produced became obsolete some years after the close of hostilities, because newer machines developed by NSA engineers, replaced them, not because fast messages enciphered on the machine had been deciphered by the enemy. As a matter of historical fact it may be stated that all efforts to solve such messages were fruitless and it is also a fact that no machines were ever captured by the enemy, nor were a machine exposed to enemy inspection at any time. Once and only once were there any apprehensions in this regard, when, through a careless disposal of specific instructions and trailers in which this machine and associated materials were housed, were stolen from during the night when parked on the street in front of the Headquarters of the 28th Division during the Battle of the Bulge. A great search was instituted during the course of this, and the trailer with all its contents intact was found resting on the bank of the diverted stream. The episode terminated in court martial proceeding.
years before the SIGABA was put into service. The Army's small

About 1920 the need for a cipher machine for

field use became obvious. The strip cipher system

for this purpose was the M-134, but it was not suitable for

reasons already indicated. The

sum $2,000 was allotted by the Chief Signal

Officer for the development of a suitable machine for field

usage. Unfortunately, the funds were turned over to the

Signal Corps laboratories at Fort Monmouth, New

Jersey, for the development of a machine

by the military director of the laboratories

with the technical guidance of the Signal

Intelligence Service, outside assistance developed a

machine which required no electricity, being all-mechanical.

The machine was sent to the Signal Intelligence

Service for tests. Two short messages were cabled

by the Chief of the SIS. Obtained the machines and the

model over the telegraph director,

who directed, and I turned them over to two of my assistants

for the reason for turning over the model into the machine was that it must be

remembered that under field conditions machines will be captured. One of the

two tests messages was signed in about 20 minutes, the

other took longer — 35 minutes. This was a

significant SCA development. Roughly about by the

failure to recognize that cryptographic invention

must be guided by technically qualified cryptographic personnel. Unfortunately all the available funds had

been expended; no work was left for a fresh start.
new development referred to as mechanical guidance from
the SIS. It was about this time that the
development of small mechanical machines was
and proceeded in quantity in Stockholm
by a Swedish engineer named Nagel, brought to the
attention of the Chief by a representative of the Nagel
firm. The SIS was asked to look into it and as technical
expert, I turned in an unfavorable report on the machine
although its practicality and cryptoanalysis was considered quite good.
It had a low degree of cryptographic security which in itself
practical
of improperly used and experienced. And taught me
that improper use could be expected without
sufficient frequency to jeopardizing the security
all messages enciphered by the same setting. The
machine was whether correctly enciphered or not. One had to
assure the CSO that my opinion was not motivated by the "N11 faction" that
was overruled by my military superior, and properly
request the SIS not to SC by the SIS.

The SIS, to its credit, developed something that was better
than the Nagel machine, as even as good as it was with
all its flaws, deficiencies and cryptographic weaknesses taken
into consideration. Accepting its qualities as possible for
the well-considered direction of the CSO, the point out where
improvements could be made and the modifications were
incorporated in the same machines which became known as Coltenet M-209. Over
years after they were manufactured in 1942-1944 by the Smith-Corona Typewriter
Company at Asbury, New York - Note a slide (Fig. 5) showing the machine which
was extensively used by all armed forces during World War II and even
another (Fig. 6) showing the internal mechanism. It turned out that under
field conditions the German field staff based on personal
rejection of the Nagel machine was fully justified - a
great deal of traffic, as it was sold by the German
Italians and Japanese. It seemed difficult to succeed any
further when declassified following successful attacks. The
traffic, those feelings were generated by my personal belief to
think up something better than the Nagel despite the
This was because the Hagelin machine operates on what is termed the key-generator principle so that when two or more messages are enciphered by the same key stream or portions thereof, solution of those messages is a relatively simple matter. Such solution permits discovery of the settings of the keying elements so that the whole stream can be produced and used to solve messages.
Excerpt from: 
**The Pickwick Papers**, Chapter XI: "Involving another journey and an antipathetic discovery."

This paragraph in *Mr. Dedlett's* shorthand typewritten script of episode dealing with a fraudulent inscription.
large machine requiring considerable amounts of electric power and hence unsuited for use by small units in field operations. In the late 1930's the Army became interested in a small mechanical machine invented by a Swedish engineer named Hagelin.

Modifications desired by Army were incorporated in the machine, which was called Converter M-209 and over 100,000 of them were manufactured in the years 1942-1944 by the Smith-Corona Typewriter Co. at Grafton, New York. Here's a slide (Fig. 35) showing Converter M-209, which was used by all our Armed Forces in World War II, and here is another (Fig. 36). When properly used it gave a high degree of security; when improperly used, as was often the case, its security was rather illusory. This machine operates on what is termed the key-generator principle and when two or more messages are enciphered by the same key stream or portions thereof, solution is relatively a simple matter but I cannot go into that now.

With the wide-scale adoption of automatic printing telegraph or teleprinter machines for electrical communications the need became pressing for a reliable and practical cryptographic mechanism to be associated or integrated with the teleprinter. The first apparatus of this sort in the U.S., shown in this slide (Fig. 38), was that developed by the American and Telephone Co., in 1918, as a more or less simple but ingenious modification of its ordinary printing telegraph. The basic principles of modern teleprinter may be useful. It is based upon what is called the "Baudot Code", that is, a system in which two different elements taken in groups of five are employed in which there are two elements of two different kinds to represent characters of the usual alphabet. These two elements may be positive and negative currents of electricity, or the letter system being often referred to as being composed of "marking" and "spacing". Here is a slide (Fig. 39) which depicts the Baudot or 5-unit code in the form of a paper tape in which there are holes in certain positions transversely to the length of the tape. The holes are produced by a perforating mechanism; the small holes running the length of the tape are "feed-holes" by means of which the tape is advanced step by step. You will note that there are
five levels on which the holes and spaces or blanks appear. The letter A, for example,
is represented by *holes* on the 1st and 2nd levels; the 3rd, 4th, and 5th levels remaining
unperforated is represented by no holes on the other three levels. Thus the
English alphabet uses 26 of the 32 permutations; the remaining 6 permutations
end of the tape are two permutations labeled "letters" and "figures", respectively.

These are equivalent to the "shift" and "unshift" keys on a typewriter keyboard, for
"lower" and "upper" case. When the "letters" key is depressed, the characters
Printed are the letters of the alphabet (all capital letters); when the "figure" key is depressed, the character represented are similar to those printed on a typewriter; when the "shift" key is depressed, the printed characters may represent "line feed," "space," and "carriage return," and they perform electrically in a teleprinter, which is done by hand on a typewriter.

I advance the paper on which the message is printed to advance to the next line; the character "space," does exactly what depressing the space bar on a typewriter does, etc. When there are no holes anywhere across the tape, the character is called a "blank," or "blanking," character—nothing. Rappos; printing, not functioning; by the printer, but the tape merely advances.

In modifying the printing telegraph machine, to make it a printing telegraph alphabet machine, or, to put the matter in a slightly different way, in developing the printing telegraph alphabet machine, the American Telegraph and Telegraph Company made good stock was fortunate in having at its disposal the services of a remarkable and original individual, named G. F. Vernam, who had a brilliant and novel principle, that principle turned out to be so useful and valuable that it has come to bear his name and always referred to as the "Vernam rule." Vernam saw that of its two general brute invariant rule
the marking and spacing elements of a 5-unit code group were combined with those of another code group, which would serve as a keying group, so that a system in accordance with the same general rule could be used and the resultant 5-unit group transmitted over a circuit and combined at the receiver with the same keying group in accordance with the same general rule. The final resultant would be the original.

Vernam extended this idea to make it applicable to the encryption of any character. An application in Vernam's name was filed in the U.S. Patent Office on 13 September 1918, and Patent No. 1,310,719 was granted on the invention entitled a "Secret Signaling System" on 22 July 1919.

The following more detailed description is taken from Vernam's patent on the foregoing extracted from a paper written by one of the AT&T Company's engineers, who was associated with Mr. Vernam at the time, after his invention was conceived and after his retirement from that company, became one of NSA's consultants:

Here is an extract from a paper prepared by Vernam himself which in simple language explains this system which only uses two different symbols or elements, the so-called "binary code". The combinatory rule is its own inverse.
how his invention worked in a system developed during World War I for use of the Signal Corps, U.S. Army.

**CIPHER MACHINE - METHOD OF OPERATION**

The messages are first punched on a paper tape by means of the keyboard perforator (Fig. 28 of this lecture). ... 

The cipher "key" may take the form of another tape [etc. as indicated on attached sheets labeled p.17-21-].

Materials attached.

This invention and exactly how the system works.

[Signature]

Copy matter attached p. 17
duty and

Secretary of writing a congratulatory letter to Colonel

Faygum, dated 24 March 1926, the following paragraph:

Your very brilliant scientific achievement

reflects great credit upon you and your whole

personnel. It would be impossible to exaggerate in paying you and Riverbank the deserved
tribute for this very scholarly accomplishment.

The A.T.

The A.T. and T. Company (writing Teleprinter Code) were

ever after Riverbank printed the whole key-tape system,
drawn some insecure; the machine went into storage, where

in due course most of them were dismantled. But after

left Riverbank at the end of 1920 and had

in charge by Chief Signal Officer's staff in Washington, en-

trusted the Chief Signal Officer to reconstruct two of the

equipments. Have I employed, believe it or not, in

preparing the manuscripts for several editions of new

codes for field use, called Division Field Codes

for use in training or an emergency. I had undertaken

to explain how this stunt for it was a stunt, but it

worked very successfully until there was no longer any

need for codes of this type.

Cipher printing telegraphy was placed

upon the shelf and more or less forgotten by the Signal

Communications Engineers

Corps from 1925 until, soon after Pearl Harbor, through

early 1938, Mr. Frank B. Rourke,

one of my associates and I kept urging that there was
If the paper by Mr. Parker (see footnote 21) closes with the following sentence final paragraph:

Perhaps some day Mr. Friedman will tell

of the part that he and the Riverbank Laboratories played in the cryptanalytic phase of this develop-

ment.

Mr. Parker was not aware of the fact that what he suggested had not only been done once (with the copies of the write-up mentioned in p. 83 which had been sent to Washington) but they had

laid on paper, that often happens to documents of limited interest — complete and final萃. The disappearance of the voluminous files of bureaucracy. The peculiar thing was that after a certain outfit found the name was using the double-step paging system for its teleprinter communications, I scrutinized through my own files and uncovered the handwritten manuscript of what I had written at the close of the successful operation of that system while at Riverbank. It is a classified docu-

ment dated 15 July 1944, a tithe of which is an encryption

history report itself. It is possible that this write-up would make

available to those of you who are interested in reading it if proper authority grants permission. [Footnote continues on attachment]
Mr. Parker's paper devotes a good deal of space to the contention that the only reason why the double-tape ending method was adopted was that the Signal Corps and specifically its representative, Colonel Maulding, "complained about the difficulties that might be experienced in the preparation and distribution of one-time random key tapes, and seemed inclined to disapprove of the proposed system because of these difficulties. Since, the system, when properly used, seemed obviously to be one which gave absolute secrecy, a discussion arose ... on the value of the system and on methods which might be desired for the production and distribution of long one-time key tapes having characters arranged at random," Parker and his associates were of the opinion that they had put in their paper that the original method of use sped up the use of long tapes of this nature and that he and his associates felt that the production and distributing of long tapes "while presenting a challenge, was not impractical." I am glad to admit that they were right, because during World War II and throughout the war, by special machinery tapes of this nature were produced (in some cases as many as five copies being performed on a single operation). Distribution and accounting for the tapes...
proved practical too and saved from occasional error involving the re-use of a once-used tape.

The system of absolutely secure inter-communication was devised and was used between and by radio printing telegraphy, among large headquarters where the volume of traffic justified the use of this equipment. The principal advantage was the simplicity of operation—no rotors to be set, no settings of rotors to be deciphered, no checking of decipherment by deciphering the message before transmission, etc.
leading members of the
cryptanalytic

...Made, the S.S.S. maintained a theoretical interest in such
there came an
equipment and in 1937 an opportunity to test such theories
as were developed by them when a machine produced
by the International Telephone and Telegraph Company
was built; interest of the Department of State was a possible
answer to the needs of that Department for rapid and
secure cryptocommunications by radio. The Secretary of
State requested the Secretary of War to investigate the
machine from the point of view of Security Communications
and periodic inspection of the Department of State were provided. It is a

...I must tell you who invented and developed the
machine. It was none other than my old friend Colonel

Frank, it is embarrassing to talk about the results. Your test

...He was too much inclined to listen to what he had to say
about the inadequacies of his brainchild. As is so often the case, when a competent technician has to give up
his technical studies because of the pressure of admin-
istrative duties, he finds it very difficult to keep abreast of new developments and progress in
the field of his technical competence. The I.T.T. Com-
pany having about a great deal of money on a develop-
ment which hardly presented any room for improvement,

...because the principles underlying it were so fully understood,
dropped the further work on it. Colonel Frank, I am glad to say, had

...The opportunity and was well enough in 1944 to be able t...
or would be real need for improved machines for protecting teleprinter communications, there was a great interest in such apparatus but what was perhaps a more important fact was the lack of funds for research and development for such work.

Ref ID: A62831

...in the failure to continue with the SIGABA project. Funds for research and development for such work was the lack of funds for research and development for such work.

immediate thought of need for cipher printing telegraphy, especially for communication, but there was no apparatus for it—not a single one of those machines of 1918–1920 was in existence.

But they have drawings and the development of the machines under contract was being done by the Teletype Corporation because well, that firm had proved that it had the necessary know-how when it produced the SIGABA—ECM's for us. Navy had less need for cipher printing telegraphy because the use of radio printing telegraphy by radio was not practicable for ships at sea. However, Navy did have a need for such apparatus for its land communications and joined Army in the development thereof. The machine produced with remarkable speed by Teletype Corporation most of them were allotted to Army a few to Navy. The Army called the machine the SIGUM, the Navy called it CSP-885. Under heavy...
regard to mechanical and electrical features and in regard to methods of keying, the use of indicator, etc. But I must tell you that before these machines became available in quantity there was only one recourse: we went back to the use of the double-keying, using standard key apparatus. The writer was key-tape method of sight-reading practically the times it was in 1920 but we had safer methods of key-tape production and indicators for their use. The S.I.S. and the equivalent unit in Navy were not happy because operators' errors left messages open to editing, so that when the new cipher machines were ready they were placed into service as soon as possible, priority being given to pursuits with heavy traffic.

Other types of cryptographic apparatus were developed during World War II. Sometimes called C.I.F.A.X. machines, for protecting friendly transmission.

C.I.F.A.X. machines cannot refrain from adding that in every case the apparatus produced by research and development firms that without direct guidance from the cryptologists of the Army and the Navy, the one exception is I believe, in the case of the extremely high-security cipher system developed and built
by the A.T.& T. Company. It was called SIGSALY.

These were pipe terminals, each of which cost over
$1,000,000. But NSA cryptologists and engineers
have produced smaller and better SIGSALY principles.
And such equipments are bound to play extremely
important roles in any future wars in the future.

So much for cryptographic apparatus. Next this
point, I shall return to that phase of cryptographic
history before the close of this lecture. Right now I
shall say a few words about cryptanalytic
apparatus.

The solution of modern crypto-communication
problems has been facilitated—and in some
cases, made possible—by the invention, development, and
application of cryptanalytic machinery including apparatus
for interception and decipherment of communications between
participants. One must understand
the basic nature of the problem which confronts the
cryptanalyst when he attempts to solve one of these
modern very complex cryptosystems. First of all he
must be given the crypto-communications in a form
which has been prepared for study. Usually they are
characters in the case of literal communications or they are
signals of a recordable type, in the case of facsimile or aphony communications. Next he must have available to him instrumentalties that will assist him in his analytical work, such as machinery for making frequency counts, comparisons of sequences, etc., and this, in the case of complex systems, must be done at high speed. Cryptanalysis of modern cryptosystems requires testing a very great number of assumptions and hypotheses, because of the astronomical number of permutations and combinations that must be tested until the correct answer is found. Since the advent of high-speed machinery for such purposes, including electronic digital computers about which so much is being heard and read nowadays, the cryptanalyst does not defeat astronomically great numbers of possibilities.

Perhaps long before my time cryptanalysts in Europe discovered that the use of slidding strips of paper could sometimes facilitate reaching a solution to a cryptanalytic problem, but so far as I am aware the very first cryptanalytic aid, in the U.S. is the one shown in Fig. , which is a picture of what made
at Riverbanks and which I called the Polyalphabetic. It was useful in solving ciphers which today are regarded as being if the very simplest types. When I came to Washington after leaving Riverbanks, I wasn't troubled by a plethora of ideas for cryptanalytic aids — I was preoccupied with devising and inventing cryptographic aids and machines. But I did now and then develop and try out certain ideas for cryptanalytic aids, frequency counters, comparison or coincidence machinery and the like. Why didn't I think of IBM machines? I did, but what good did that do? Did the Signal Office have any such machines — or even one dollar for their rental? You know the answer is that without my spelling it out. There wasn't any use even in suggesting that IBM machines could be of assistance to me — remember, that is I'm telling about the years 1921 to 1933, and in the last-named year we were in the depths of a great economic depression. But one day in 1934 (Army and Navy were not then sharing money) learned by a democratic route that the Navy Coast and Signal sections had two or three IBM machines and my chagrin was almost unbearable. Not long afterwards I learned that a certain division of the Office of the
Quartermaster General in the Munitions Building had an IBM installation which had been used for accounting purposes in connection with the C.C.—the Civilian Conservation Corps established to provide work and maintenance subsistence for young men who could find no jobs in the depression. I also learned that a new officer had just been assigned to head that particular division— and that he just had no use for these newfangled ideas of his predecessors and wanted to get rid of these nasty IBM machines. But the contract with IBM still had some months to go run before the lease expired and after the machines would sit idle or the Government would lose money by canceling the contract before the due date of expiration. This annoyed me, but it also gave me an idea. I wrote a memorandum and here's a picture of it (Fig.). I'll read you what it says:

Attached

Attached to the memo was a brief explanation of what I'd told you about their installation in the Office of the Quarter-master General. Note that I placed

1/3 M
Major Akin: In many years service here I have never once "set my heart on" getting something I felt desirable. But in this case I have set my heart on the matter because of the tremendous load it would lift off all our backs.

The basic idea of using machinery for code compilation is mine and is of several year's standing. The details of the proposed system were developed in collaboration with Mr. Case, of the Int. Bus. Machines Corp.

I regard this as one of my most valuable contributions to the promotion of the work for which we are responsible.

Please do your utmost to put this across for me. If you do, we can really begin to do worthwhile cryptanalytic work.

F.
The emphasis upon the burden that would be lifted from cryptographic work by using the IBM machinery, thus leaving more time for cryptanalytic work. This was because the responsibilities of the S. I. S. for cryptanalytic operations were at that time restricted purely to theoretical studies. Studies on cryptanalytic work on foreign cryptosystems were a responsibility of the Signal Corps during peace-time. 21-2 of the General Staff, but they had been transferred to the Chief Signal Officer and the Signal Corps in the year 1918. But the Chief Signal Officer had very little money to use for that purpose, and besides, the Army regulation applicable thereto specifically restricted cryptanalytic operations on foreign communications to war-time. And, more to the point, was the fact that there was no material to work on even of funds were available, because there had at that time no intercept stations whatever, anywhere in or outside the U.S. But that's another story and I will proceed to the next point, which is that my memo to Major Atkins produced results. Just a
Half month after I wrote and put it in his "In" basket I got the machines moved from the Office of the Quartermaster General to my own in the Office of the Chief Signal Officer. That move must have been potenti-

Once having proved demonstrated their utility to the Chief Signal Officer the almost prematurely terminated contract with IBM was renewed—and soon expanded. I don't know how we could have managed without such machines during World War II. Here's a picture of one of two whole wings in one of our buildings at Arlington Hall filled with IBM machines—

the biggest installation in the world at that time.

We built or had built for us by IBM and other concerns adapters to work with standard IBM machines; we constructed or had constructed for us by commercial firms highly specialized cryptanalytic apparatus, machines, and complex assemblies of components. Under war-time pressures fantastic things were ac-
completed and many were the thrills of gratifying achievements when things that couldn't be done were done—and were of high importance in military, naval and air operations against the enemy.

Even were time available I couldn't show you pictures of some of the high-class gadgets we used, neither is it permissible to say more than I have already said about them, even though it is no longer a deep secret that electronic computers are highly useful in cryptologic work. For example, here is a paragraph taken from a Russian book entitled and below it is what it says in English.

To the layman—the exploits of professional cryptanalysts, when these exploits come to light—as, for example, in the various investigations of the attack on Pearl Harbor—are much more fascinating than those of cryptographers, whose achievements in their field appear to be dull or tedious to the layman. But long consideration of the military importance of communication security as against...
that of cryptanalysis and communication intelligence has induced me to formulate what I shall modestly call Friedman's Law: it is quite simply stated. If you keep the cryptanalyst or CCIN front of your cryptologue, from bright and shining, he has a good chance of remaining a battle winner. If he is in front of an enemy, but if the cryptographic or CONSEC front of him that coin becomes dull from neglect, indifference, or carelessness, he will almost certainly lose as battle of this forces openly comparing in size and ability compared with those of this enemy. 

While the foregoing statement of war cryptanalyst opinion grounded upon a half century's devotion to cryptology as a profession, I bring this sense of lectures to an undramatic close. 

56 26
From: Tokyo
To: Washington
19 November 1941
(J19)

Circular #2353

Office Chief's Code.

I do not know but what, as a result of the terrible strain in our operations, we have at length come to stand amid the ultimate evil circumstances, and if this be so, our communications with the country (ies) we are dealing with will be cut. And in the event that our foreign relations fringe on catastrophe, then in the middle and at the end of our universal broadcasts, the form of weather predictions, we will repeat and broadcast twice each the following:

(1) In the case of Japanese-American relations (HIGASHI NO KAZEAME).

(2) In the case of Japanese-Soviet relations (KITA NO KAZE KUMORI).

(3) In the case of Japanese-British relations (including their implications in Thai along with Malaya and the Netherlands East Indies), (NISHI NO KAZE HARE).

Hence you will know that you are suitably to destroy codes, documents, etc.

You will please guard this in strictest secrecy.

This for Voice Broadcast:
"Twice in middle and twice at end"

There is good evidence that "Nishi no kazehare" was really transmitted in this way, see Doc No 4 of FCC Statement.
From: Tokyo
To: Washington
19 November 1941
(J19)

Circular #2353

Office Chief's Code.

I do not know but what, as a result of the terrible strain in our operations, we have at length come to stand amid the ultimate evil circumstances, and if this be so, our communications with the country (ies) we are dealing with will be cut. And in the event that our foreign relations fringe on catastrophe, then in the middle and at the end of our universal broadcasts, the form of weather predictions, we will repeat and broadcast twice each the following:

(1) In the case of Japanese-American relations (HIGASHI NO KAZEAME).
    East wind, rain

(2) In the case of Japanese-Soviet relations (KITA NO KAZEKUMORI).
    North wind, cloudy

(3) In the case of Japanese-British relations (including their implications in Thai along with Malaya and the Netherlands East Indies), (NISHI NO KAZEHARE).
    West wind, clear

Hence you will know that you are suitably to destroy codes, documents, etc.

You will please guard this in strictest secrecy.

[Handwritten note: This for Voice broadcasts of weather forecasts in middle and end of broadcast.
There is good evidence that "Nishi no kazehare" was really transmitted in this way. See Doc. 114 of FCC statement.]
As discussed, as requested, comments and return information and files.

See note on reverse.

Recommendation:

Signature if approved.

Your action.

As classified and approved for release by

NSA on 11-08-2013, pursuant to E.O.

3526

NSA SC Form No. 96 (Rev) 16 Nov 44

SECRET

TODAY'S DATE

TO

FOM

SECRET

15-3-64100
I desire a fresh translation of these two messages. Please get your most competent man on it. In case any of the groups are garbled or in case of slightest doubt about any of the deciphered groups, please let me know.

I would appreciate having these back as soon as possible.

These messages have been translated by Mr. Jerrard and Mr. Ford Joint in collaboration. I am sure translation can be depended upon as accurate.
Circ # 235h

Secret

Please note that in case our foreign relations are on the verge of a break the following words are to be inserted at the beginning and end of general information broadcasts, five times each.

1. In the event of tension in Japanese-American relations: "East."
2. In the event of [tension in] Japanese-Soviet relations: "North."
3. In the event of [tension in] Japanese-British relations (including occupation of THAILAND and invasion of Netherlands East Indies and Malaya):

"West."
Circ # 2353

Handle in office chief's code.

As a result of the tension in the international situation matters may come to the worst. Since in this event communications between us and the opposing countries will at once be suspended it has been decided that, in case our foreign diplomatic relations come to a crisis, the following is to be broadcasted as a weather forecast in the Japanese language overseas news broadcast to all areas, repeated twice at the middle and at the end.

1. In the event of [a crisis in] Japanese-American relations:
   "East wind, rain."

2. In the event of [a crisis in] Japanese-Soviet relations:
   "North wind, cloudy."

3. In the event of [a crisis in] Japanese-British relations (including occupation of THAILAND and invasion of Netherlands East Indies and Malaya):
   "West wind, fair."

In accordance with the above please make suitable disposition of your codes, documents, etc.

This is to be treated with strictest secrecy.
FROM: TOKYO (TOGO)  
TO: WASHINGTON (KOSHI)  

19 NOVEMBER, 1941  
J-19  
CIRC #2353 (COMPLETE)  

MWZHU BUWTJ
Office Chief's Code:

I do not know but what, as a result of the terrible strain in our operations, we have at length come to stand and the unfortunate circumstances, and if this be so on other communications with the countries we are dealing with will be cast.

And in the event that our foreign relations finance on catastrophe then in the Middle East there will be a form of weather. In all relations we will repeat and broadcast twice each the following:

1. In the case of Japanese American relations (Higashi no Kaze-tai).
2. In the case of Japanese-Soviet relations (Kito no Kaze-tai).
3. In the case of Japanese-British relations (including their implications in that along with Malaya and the Netherlands East Indies) (Nishi no Kaze-tai).

Hence you will know that you are to absolutely destroy these documents. If you will please guard this in

Strict Secrecy.
I do not know but what we have arrived at the very worst as a result of the terrible strain of war. If such be the case immediately communications between us and the nations we are dealing with will be broken. If our diplomatic relations should reach the point of rupture, the broadcasting of Japanese news to various areas of the world should be stopped, as a last resort in the form of weather forecasts.

1) In the case of Japanese-American relations: Higashi No Kaze
2) In the case of Japanese-Soviet relations: Kita No Kaze Kumori

In accordance each we will have those broadcasts repeated, thereby you will know when to turn up codes and pertinent documents. You are ordered to keep the forgoing in the strictest secrecy.
UNITED STATES CIVIL SERVICE COMMISSION

POSITION DESCRIPTION

CLASSIFICATION ACTION

Classification 1949

ALLOCATION BY

CLASS TITLE OF POSITION

CLASS

Service  Series  Grade  INITIALS  DATE

a  Civil Service Commission

CRYSTALLOGRAPHIC RESEARCH ADVISOR

b  Department, agency, or establishment

c  Bureau

d  Field office

e  Recommended by initiating office

CLASS TITLE OF POSITION

CLASS

Service  Series  Grade  INITIALS  DATE

Modernization of Civil Service

b  Department, agency, or establishment

c  Bureau

d  Field office

e  Recommended by initiating office

CLASS TITLE OF POSITION

CLASS

Service  Series  Grade  INITIALS  DATE

Special Assistant to the Director

b  Department, agency, or establishment

c  Bureau

d  Field office

e  Recommended by initiating office

CLASS TITLE OF POSITION

CLASS

Service  Series  Grade  INITIALS  DATE

13 This is a complete and accurate description of the duties and responsibilities of this position

signature of employee

(signature of immediate superior)  (Date)

Title

Director, National Security Agency

Signature

(signature)  (Date)

Title

Description of duties and responsibilities (See Guide to Position Classifiers, Employees and Supervisors for the Preparation of Position Descriptions Standard Form No. 78A)

December 31, 1969

Declassified and approved for release by NSA on 05-31-2013 pursuant to E.O. 13526

If more space is required use the other side and additional pages same size 8 x 11".
SPECIAL ASSISTANT TO THE DIRECTOR

DUTIES AND RESPONSIBILITIES:

As the Cryptologic Research Advisor is the principal consultant to the Director, National Security Agency concerning the technical and exploitational aspects of all cryptologic activities. These activities encompass two very broad fields of endeavor, communications intelligence and communications security, and involve several unrelated technical, professional and scientific fields and programs which demand continued "pioneering" effort to keep abreast of advancements in the fields. Renders technical advice and assistance to the Director, staff divisions and operating offices in the formulation and execution of the broad over-all plans and programs of the National Security Agency and in the technical control and coordination of all activities. Is responsible for studying and evaluating the overall programs in terms of current and new technical tactical and strategic information for the purpose of recommending to the Director changes in programs which may be justified by any changes in trends or by the results of advances in the communications electronic field brought about by the research being carried on by various government agencies, universities and industrial laboratories. Investigates new discoveries with a view towards applying such discoveries or modifications thereof to the accomplishment of communications security and communications intelligence production programs.

HELP PROVIDED BY GUIDES:

Follows broad agency policy directives and regulations and is guided by past and current technical successes and accomplishments, but the present and advancing sophistication of the science of communications security and communications intelligence on a world-wide basis is such as to require cognizance of advances in these very broad fields and the ability to consider and apply this knowledge as guidelines in the solution of specific problems as well as in the continuing advancement of the art.

HELP PROVIDED BY SUPERVISOR:

Works under general administrative direction of the Director of the Agency acting independently on all scientific and technical matters. Receives no technical direction from higher echelons within the Agency.

ORIGINAL THINKING DONE:

Is responsible for initiating ideas and investigating and advancing techniques and programs in hitherto unexplored lines in a variety of scientific fields, especially the very broad field of communications-electronics, in order to advance the work of the Agency and to insure that the communications of the United States Armed Forces are the most secure in the world and the maximum production of communications intelligence.
PERSONAL WORK CONTACTS:

Participates in high-level committee and conference work for coordinating communications intelligence and communications security activities within the Agency and with the requirements of cooperating groups outside the Agency; initiates and maintains relationships with professional, technical and scientific personnel of highest professional reputation and standing to secure information and assistance needed in solving cryptologic problems; maintains close technical liaison with Service Cryptologic Agencies and with other Agencies and governments and is recognized as an outstanding authority in the field of cryptology.

THE EXTENT TO WHICH DECISIONS AND JUDGMENTS MADE ARE CHECKED OR REVIEWED:

Advice, decisions and opinions are accepted as technically sound and valid and have considerable influence on national and international policies and agreements as well as on programs of the National Security Agency. Any review is in terms of administrative policies, budgetary and manpower considerations.

THE IMPORTANCE AND EFFECTS OF WORK DONE:

The functions and programs of the Agency are of vital importance to and are an integral part of the National Defense programs.

SUPERVISORY RESPONSIBILITIES:

Exercises no direct supervision, but recommendations, policies, plans and programs originated by the Research Advisor affect and control the efforts of several thousand personnel through the Agency.
National Security Agency

Cryptologic Research Advisor GS-1540-13
Vacancy

BACKGROUND:

The scientific advancements in the broad field of communications, and the importance of this field to world security, place increasingly complex demands upon the National Security Agency in the accomplishment of its missions in the Communications Intelligence, Communications Security, and Research and Development fields. These rapid advancements and the greater importance of this mission were recognized by the recent Presidential Executive Directive abolishing the Armed Forces Security Agency and reconstituting the organization as the National Security Agency. To efficiently and effectively accomplish the expanded mission, it is essential to attract and retain recognized authorities in the professional and scientific fields and to equitably compensate these authorities for their services. The present compression within the Agency at the GS-15 level does not meet this requirement. The attached position description generally outlines the scope of this highly technical mission but does not disclose some of the highly classified programs which are undertaken by this Agency.

QUALIFICATIONS REQUIREMENTS:

The incumbent of this position must possess outstanding qualifications in the field of cryptology. He must possess outstanding ability to conceive and initiate programs which will insure that the Agency not only keeps abreast of the advancing sophistication of the science of cryptology on a world-wide basis, but also continues the advancement of the art. He must also possess top recognition in this field to obtain technical assistance and cooperation in the various fields of endeavor.

EVALUATION:

The incumbent of this position will be the top cryptologic advisor in this highly technical and specialized field, supporting the security measures of the nation and the world. In addition to the importance of this position, the extremely complex and unprecedented nature of the work appears to warrant allocation to the proposed grade of GS-15. It is recommended, therefore, that the Civil Service Commission concur in this recommendation and submit the position to The President for final action.

WILMA FLYNN
Chief, Civilian Position Classification Section
National Security Agency

CONFIDENTIAL
**Civilian Supergrade Positions**

<table>
<thead>
<tr>
<th>Position</th>
<th>Organization</th>
<th>Proposed Grade</th>
<th>Authorized Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chief Communications Scientist.</strong> Serves as the Deputy Director for Research and Development in the exercise of management and operational and technical control of cryptologic research and development vested in the Director of the National Security Agency.</td>
<td>N/D</td>
<td>GS-18</td>
<td>GS-18</td>
</tr>
<tr>
<td><strong>Cryptologic Research Advisor.</strong> Serves as Special Assistant to the Director of the Agency and is responsible for advising the Director and Deputy Directors (Military - rotating between the services) concerning the technical and exploitative aspects of cryptologic activities of the Agency. Studies and evaluates the overall program for the purpose of recommending changes justified by any changes in trends or by results in advances in the cryptologic field.</td>
<td>Spec. Asst. to Director</td>
<td>GS-18</td>
<td>GS-18</td>
</tr>
<tr>
<td><strong>Chief Cryptanalyst.</strong> Serves as Technical Director of a large organization responsible for all specialized classified communication activities of the Armed Forces.</td>
<td>PROD</td>
<td>GS-18</td>
<td>GS-16</td>
</tr>
<tr>
<td><strong>Communications Scientist.</strong> Responsible for the performance of communication security functions under the cognizance of the National Security Agency. This includes the establishment and promulgation of the communications security doctrine, policy, techniques and instructional material of the Armed Forces.</td>
<td>COMSEC</td>
<td>GS-17</td>
<td>0</td>
</tr>
<tr>
<td><strong>Chief Physical Science Administrator.</strong> Assistant Director, Research and Development, directs the research and development activities, the purpose of which is to augment the ability of the National Security Agency to perform its mission rapidly, thoroughly and economically. This involves work in several professional fields, including electronics, physics, mechanical and electrical engineering, mathematics, cryptology, and a variety of related fields, encompassing basic research, applied research, and pioneer development.</td>
<td>N/D</td>
<td>GS-17</td>
<td>GS-16</td>
</tr>
<tr>
<td>Position</td>
<td>Organization</td>
<td>Grade</td>
<td>Authorized</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------</td>
<td>-------</td>
<td>------------</td>
</tr>
<tr>
<td>Communications Specialist. Responsible for providing the technical continuity in the current and long-range planning of the cryptologic activities of the Agency.</td>
<td>P/P</td>
<td>GS-17</td>
<td>0</td>
</tr>
<tr>
<td>Cryptanalyst. Serves as one of two Agency cryptanalytic authorities in a large organization, with responsibility for planning, coordinating and directing the Agency specialized cryptanalytic program, and for the suspension and termination of various phases of work.</td>
<td>PROD</td>
<td>GS-17</td>
<td>GS-16</td>
</tr>
<tr>
<td>Physical Science Administrator (Research). Serves as Chief of Office for Research, exercising technical control and guidance over the activities of a research group composed of an Engineering Research Division, Mathematical Research Division, and Physical Research Division, investigating areas having actual or potential value in meeting the special requirements of cryptologic equipment and techniques.</td>
<td>R/D</td>
<td>GS-16</td>
<td>0</td>
</tr>
<tr>
<td>Physical Science Administrator (Development). Serves as Chief of Office for Development, exercising technical control and guidance over development activities, including the conduct and control of projects for development of cryptologic equipment and methods, and involves work in several scientific and technical subject matter fields.</td>
<td>R/D</td>
<td>GS-16</td>
<td>0</td>
</tr>
<tr>
<td>Comptroller. Responsible for analyzing and evaluating command programs to facilitate the accomplishment of objectives within available resources in the performance of accounting, budgeting, auditing, management analysis, and reporting functions to aid in the most effective utilization of personnel, equipment, and funds.</td>
<td>COMP</td>
<td>GS-16</td>
<td>0</td>
</tr>
<tr>
<td>Cryptanalyst (Security). As the Chief Security Analyst, recommends new cryptosecurity and physical security policies, and directs the implementation in the services of established policies in these fields.</td>
<td>CONSEC</td>
<td>GS-16</td>
<td>0</td>
</tr>
<tr>
<td>Cryptologic Statistician. Is responsible for determining the feasibility of applying analytical machine processing equipment and techniques in the solution of problems, advising on such application, and devising and developing appropriate methods for the use of the equipment.</td>
<td>PROD</td>
<td>GS-16</td>
<td>0</td>
</tr>
<tr>
<td>Position</td>
<td>Organization</td>
<td>Proposed Grade</td>
<td>Authorized</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Cryptanalyst. Makes recommendations on matters dealing with specialized activities, anticipating new cryptologic developments and conducting original research in cryptanalytic techniques, new systems, and new devices, from the viewpoint of the specialized interest.</td>
<td>PROD</td>
<td>GS-16</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>14</td>
<td>5</td>
</tr>
</tbody>
</table>
Lecture 2

Final Version
As I said at the close of the preceding lecture, a bit of history is always useful in introducing a subject belonging to a special and not too well known field; therefore, I'll proceed with some historical information about cryptology, which, as you learned before, comprises two closely related sciences, namely, cryptography and cryptanalysis. I will repeat and emphasize that they are but opposite faces of the same valuable coin; progress in one inevitably leads to progress in the other, and to be efficient in cryptology you must know something about each of them.

Cryptography and cryptanalysis probably go back to the dawn of the invention and development of the art of writing itself. In fact, there is reason for speculating as to which came first—the invention of writing or the invention of cryptography; it's somewhat like the question as to which came first—the hen or the egg. It is possible that some phases of cryptography came before the art of writing had advanced very far.

I've mentioned the art of writing. As in the case of other seemingly simple questions, such as, "why is grass green?", when we are asked to define writing we can't find a very simple answer, just because the answer isn't at all simple. Yet, Breasted, the famous University of Chicago historian and Orientalist, once said: "The invention of writing and of a convenient system of records on paper has had a greater influence in uplifting the human race than any other intellectual achievement in the
career of man." There has been, in my humble opinion, no greater invention in all history. The invention of writing formed the real beginning of civilization. As language distinguishes man from other animals, so writing distinguishes civilized man from barbarian. To put the matter briefly, writing exists only in a civilization and a civilization cannot exist without writing. Let me remind you that animals and insects do communicate—there's no question about that; but writing is a thing peculiar to and found only as a phenomenon in which man and no animal or insect engages, and let's never forget this fact. Mankind lived and functioned for an enormous number of centuries before writing was discovered and there is no doubt that writing was preceded by articulate speech for eons—but civilization began only when men got the idea of and invented the art of writing. So far as concerns Western or Occidental civilization, writing in essence is a means of representing the sounds of what we call speech or spoken language. Other systems of writing were and some still are handicapped by trying to represent things and ideas by pictures. I'm being a bit solemn about this great invention because I want to impress upon you what our studies in cryptology are really intended to do, namely, to defeat the basic or intended purpose of that great invention: instead of recording things and ideas for the dissemination of knowledge, we want and strive our utmost to prevent this aim from being realized, except among our own brethren and under certain special circumstances, for the purpose of our mutual security, our self-preservation. And that's important.
Writing is a comparatively new thing in the history of mankind. No complete system of writing was used before about 3500 B.C.

Ordinary writing, the sort of writing you and I use, is perhaps an outgrowth or development of picture writing or rebus writing, which I'm sure most of you enjoyed as children. A rebus contains features of both ordinary and cryptographic writing; you have to "decrypt" the significance of some of the symbols, combine single letters with syllables, pronounce the word that is represented by pictures, and so on. Here's an example which I have through the courtesy of the Bell Telephone Laboratories. Let's see how much of it you can make out in half a minute.

From rebus writing there came in due course alphabetic writing and let me say right now that the invention of the alphabet, which apparently happened only once in the history of mankind, in some Middle East Semitic region, in or near the Palestine-Syria area, then spread throughout the whole of the European continent, and finally throughout most of the world, is perhaps man's greatest, most important, and most far-reaching invention because it forms the foundation of practically all our written and printed knowledge, except that in Chinese. The great achievement of the invention of the alphabet was certainly not the creation of the signs or symbols. It involved two brilliant ideas. The first was the idea of representing merely the sounds of speech by symbols, that is, the idea of what we may call phoneticization; the second was the idea of adopting a system in which,
roughly speaking, each speech sound is denoted or represented by one and only one symbol. Simple as these two ideas seem to us now, the invention was apparently made, as I've said, only once and the inventor or inventors of the alphabet deserve to be ranked among the greatest benefactors of mankind. It made possible the recording of the memory of mankind in our libraries, and from that single invention have come all past and present alphabets. Some of the greatest of men's achievements we are now apt to take for granted; we seldom give them any thought. The invention of the art of writing and the invention of the alphabet are two such achievements and they are worth pondering upon. Where would we be without them? Note that among living languages Chinese presents special problems not only for the cryptologist but also for the Chinese themselves. No Sinologist knows all the 85,000 or so Chinese symbols, and it is also far from easy to master merely the 9,000 or so symbols actually employed by Chinese scholars. How far more simple it is to use only 28 to 26 symbols! Being a monosyllabic language, it seems almost hopeless to try to write Chinese by the sort of mechanism used in an alphabetic polysyllabic language; attempts along these lines have been unsuccessful and the difficulties in memorizing a great many Chinese characters accounts for the fact that even now only about 10% of the Chinese people can read or write to any significant degree. The spread of knowledge in China is thereby much hampered.
Probably the earliest reliable information on the use of cryptography in connection with an alphabetic language dates from about 900 B.C., Plutarch mentioning that from the time of Lycurgus there was in use among the Lacedemonians, or ancient Greeks, a device called the scytale. This device, which I'll explain in a moment, was definitely known to have been used in the time of Lysander, which would place it about 400 B.C. This is about the time that Aeneas Tacticus wrote his large treatise on the defense of fortification, in which there is a chapter devoted specifically to cryptography. In addition to mentioning ways of physically concealing messages, a peculiar sort of cipher disk is described. Also a method of replacing words and letters by dots is mentioned.

We find instances of ciphers in the Bible. In Jeremiah Chapter 25, Verse 26 occurs this expression: "And the King of Sheshakh shall drink after them." Also, again in Jeremiah 51:41: "How is Sheshakh taken!"

Well, for perhaps many years that name "Sheshakh" remained a mystery, because no such place was known to geographers or historians. But then it was discovered that if you write the twenty-two letters of the Hebrew alphabet in two rows, eleven in one row and eleven in the other, like this, you set up a substitution alphabet whereby you can replace letters by those standing opposite them. For example, "Shin", is represented by "Beth" or vice versa, so that "Sheshakh" translates "Babel", which is the old name of "Babylon."

Hebrew then did not have and still doesn't have vowels; they must be supplied.
This is an example of what is called ATHBASH writing, that is, where Aleph, the first letter is replaced by Teth, the last letter; Beth, the second letter, by Shin, the next-to-the-last, etc. By sliding the second row of letters one letter each time there are eleven different cipher alphabets available for use. The old Talmudists went in for cryptography to a considerable extent. Incidentally, in mentioning the Bible, I will add that Daniel, who, after Joseph in Genesis, was an early interpreter of dreams and therefore one of the first psychoanalysts, was also the first cryptanalyst. I say that he was an early psychoanalyst, because you will remember that he interpreted Nebuchadnezzar’s dreams. In the Bible’s own words, “Nebuchadnezzar dreamed dreams, wherewith his spirit was troubled, and sleep brake from him.” But, unfortunately, when he woke up he just couldn’t remember those troublesome dreams. One morning he called for his wise men, magicians, astrologers, and Chaldean sorcerers and asked them to interpret the dream he’d had during the preceding night. “Well, now, tell us the dream and we’ll try to interpret it”, they said. To which King Nebuchadnezzar exclaimed, “The thing is gone from me. I don’t remember it. But it’s part of your job to find that out, too, and interpret it. And if you can’t tell me what the dream was, and interpret it, things will happen to you.” What the king asked was a pretty stiff assignment, of course and it’s no wonder they failed to make good, which irked Nebuchadnezzar no end. Kings had a nasty habit of chopping your head off in those days if you failed or made a mistake, just as certain arbitrary
and cruel despots are apt to do even in modern times for more minor infractions, such as not following the Party Line. So in this case it comes as no surprise to learn that Nebuchadnezzar passed the word along to destroy all the wise men of Babylon, among whom was one of the wise men of Israel, named Daniel. Well, when the King's guard came to fetch him, Daniel begged that he be given just a bit more time. Then, by some act of divination, --the Bible simply says that the secret was revealed to Daniel in a night vision--Daniel was able to reconstruct the dream and then to interpret it. Daniel's reputation was made. Some years later, Nebuchadnezzar's son Belshazzar was giving a feast, and, during the course of the feast, in the words of the Bible, "came forth fingers of a man's hand and wrote over against the candlestick upon the plaster of the wall." The hand wrote a secret message. You can imagine the spine-chilling scene. Belshazzar was very much upset, and just as his father did, he called for his wise men, soothsayers, Chaldean sorcerers, magicians and so on, but they couldn't read the message. Apparently they couldn't even read the cipher characters! Well, Belshazzar's Queen fortunately remembered what that Israelite Daniel had done years before and suggested that Daniel be called in as a consultant. Daniel was called in by Belshazzar and he succeeded in doing two things. He succeeded not only in reading the writing on the wall: "MENE, MENE, TEKEL, UPHARSIN", but also he was successful in deciphering the meaning of those strange words. His interpretation: "Mene" -- "God hath numbered thy kingdom and finished
it." "Tekel" -- "Thou are weighed in the balances and found wanting."

"Upharsin" -- "Thy kingdom shall be divided and given to the Medes and
Persians." Apparently the chap who did the handwriting on the wall knew
a thing or two about cryptography, because he used what we call "varianta",
or different values, for in one case the last word in the secret writing on
the wall is "Upharsin" and in the other it is "Peres"; the commentators are
a bit vague as to why there are these two versions of the word in the Bible.
At any rate, Babylon was finished, just as the inscription prophesized; it
died with Belshazzar.

I think this curious biblical case of the use of cryptography is
interesting because I don't think anybody has really found the true meaning
of the sentence in secret writing, or explained why the writing on the wall
was unintelligible to all of Belshazzar's wise men. Here's a slide which
is supposed to give the best explanation of the enigmatical sentence that
has always been considered one of the most obscure of the many difficult
scriptual passages which have awakened the interest and baffled the ingenuity
of scholars. You see that this savant thinks that the cuneiform ideograms
were written without any division between the individual words, so that the
sentence "would be just as hard to read as a rebus and would puzzle the
most skillful decipherer." He goes on to say: "The difficulty would have
been still more increased if the ideograms had been grouped in some unusual
way, severing the natural connection of the component elements. If the
signs had been written in this manner it would have been almost impossible to arrive at their true meaning." But why could Daniel read and interpret the writing when his competitors couldn't? This our savant doesn't explain. Another savant offers as his explanation of the mystery the following hypothesis: That the words were written in columns, as shown in this slide, and that Daniel in solving the mystery read downwards or rather down, up, down. This explanation doesn't satisfy me any more than the other one.

The next slide I show you is the scytale, which I've already mentioned as one of the earliest cipher devices history records. The scytale was a wooden cylinder of specific dimensions around which they wrapped spirally a piece of parchment or leather; they then wrote the message on the parchment, unwound it, and sent it to its destination by a safe courier, who handed it over to the commander for whom it was intended and who, having been provided with an identically-dimensioned cylinder, would wind the strip of leather or parchment around his cylinder and thus bring together properly the letters representing the message. This diagram may not be accurate. I don't think anyone really understands the scheme. The writing was done across the edges of the parchment, according to some accounts, and not between the edges, as shown in this slide. Incidentally, you may be interested to learn that the baton which the European field marshal still carries as one of the insignia of his high office derives from this very instrument.
We don't know much about the use of cryptography by the Romans, but it is well known that Caesar used an obviously simple method; all he did was to replace each letter by the one that was fourth from it in the alphabet. For example, A would be represented by D, B by E, and so on. Augustus Caesar is said to have used the same sort of thing, only even more simple: each letter was replaced by the one that followed it in the alphabet.

Cicero was one of the inventors of what is now called shorthand. He had a slave by the name of Tyro, who wrote Cicero's records in what are called Tyronian notes. Modern shorthand is a development of Tyro's notation system.

The next slide shows some cipher alphabets of olden times, alphabets used by certain historical figures you'll all remember. The first cipher alphabet on the slide was employed by Charlemagne, who lived from 768 to 814 A.D. The second one was used in England during the reign of Alfred the Great, 871 to 899. The third alphabet is called **ogan writing** and was used in ancient Ireland. The alphabets below that were used much later in England: the fourth one by Charles the First, in 1646; the fifth, the so-called "clock cipher", was used by the Marquis of Worcester in the 17th Century; finally, the last one was used by Cardinal Wolsey in about 1524.

In the Middle Ages cryptography appears first as a method of concealing proper names, usually by the simple substitution of each letter by the next one in the alphabet, just about as Augustus Caesar did hundreds of years
before. At other times the vowels were replaced by dots, without changing
the consonants—a method that was used throughout Europe to about 1000 A.D.,
when letters began to be replaced by various signs, by other letters, by
letters from another language, by runes which are found in abundance in
Scandinavia, and by arbitrary symbols. Here's an example of a runic inscrip-
tion on a stone that stands before Gripsholm Castle near Stockholm, Sweden.
The word rune means "secret".

Within a couple hundred years the outlines of modern cryptography
began to be formed by the secret correspondence systems employed by the
small Papal States in Italy. In fact, the real beginnings of systematic,
modern cryptography can be traced back to the days of the early years of the
13th Century, when the science began to be extensively employed by the
princes and chanceries of the Papal States in their diplomatic relations
amongst themselves and with other countries in Europe. The necessity for
secret communication was first met by attempts inspired by or derived from
ancient cryptography, as I’ve outlined so far. There was a special pre-
dilection for vowel substitution but there appeared about this time one of
the elements which was later to play a very prominent role in all cipher
systems, an element we now call a syllabary, or a repertory. These were
lists of letters, syllables, frequently-used parts of speech and words, with
additions of arbitrary equivalents for the names of persons and places.
There is still in existence one such syllabary and list of arbitrary
equivalents which was used about 1236 A.D. and there are other examples
that were used in Venice in 1350.

Among examples of ciphers in medieval cryptography is a collection of
letters of the Archbishop of Naples, written between 1363 and 1365, in which
he begins merely with symbol substitutions for the vowels and uses the letters
that are actually vowels to serve as nulls or non-significant letters to throw
the would-be-cryptanalyst off the right track. As a final development, the
high-frequency consonants L, M, N, R, and S, and all the vowels, are replaced
not only by arbitrary symbols but also by other letters.

About 1378 an experienced cryptologist named Gabriele Lavinde of Parma
was employed as a professional by Clement VII and in the Vatican Library
there is a collection of ciphers devised and used by Lavinde about 1379. It
consists of repertories in which every letter is replaced by an arbitrary
symbol. Some of these ciphers also have nulls and arbitrary equivalents or
signs for the names of persons and places. There is a court cipher of Mantua
dated 1395 that used this system.

At the beginning of the 15th Century the necessity of having variants
for the high-frequency letters, especially the vowels, became obvious. Here
is an alphabet of that period which is interesting because it shows that even
in those early days of cryptography there was already a recognition of the basic
weakness of what we call single or nonalphabetic substitution, that is, where
every letter in the plain-text message is represented by another and always
the same letter. Solution of this type of cipher, as many of you may know,
is accomplished by taking advantage of the fact that the letters of an
alphabetic language are used with greatly differing frequencies. I don't
have to go into that now because many of you, at some time or other, have
read Edgar Allan Poe's "Gold Bug", and understand the principles of that
sort of analysis. This slide clearly shows that the early Italian crypto-
graphers understood the fact of varying frequencies and introduced stumbling
blocks to quick and easy solution by having the high-frequency letters
represented by more than a single character, or by several characters, as
you see in this slide. I will add that the earliest tract that the world
possesses on the subject of cryptography, or for that matter, cryptanalysis,
is that which was written in 1476 by a Neapolitan, whose name was Sicco
Simonetta. He set forth the basic principles and methods of solving ciphers,
simple ciphers no doubt, but he describes them and their solution in a very
clear and concise form.

Cipher systems of the type I've described continued to be improved. In
this slide is shown what we may call the first complete cipher system of this
sort. There are substitution symbols for each letter; the vowels have
several equivalents; there are nulls; and there is a small list of arbitrary
symbols, such as those for "the Pope", the word "and", the conjunction "with", and so on. This cipher, dated 1471, was used in Venice, and is typical of the
ciphers used by the Papal chanceries of those days.

-13-
The step remaining to be taken in the development of these ciphers was to expand the "vocabulary", that is, the list of equivalents for frequently-used words, and syllables, the names of persons and places, parts of speech, and so on. This step was reached in Italy during the first half of the 15th Century and became the prototype of diplomatic ciphers used in practically all the states of Europe for several centuries. Here is one of 78 ciphers collected in a Vatican codex and used from about 1440 to 1469. Note that the equivalents of the plain-text items in this slide are Latin words and combinations of two and three letters, and that they are listed in an order that is somewhat alphabetical but not strictly so. I suppose that by constant use the cipher clerk would learn the equivalents almost by heart, so that an adherence to a strict alphabetic sequence either for the plain-text items or for their cipher equivalents didn't hamper their operations too much. In this next slide there is much the same sort of arrangement, except that now the cipher equivalents seem to be digraphs and these are arranged in a rather systematic order, for ease in enciphering and deciphering. Now we have the real beginnings of what we call a one-part code, that is, the same list will serve both for encoding and decoding. These systems, as I've said, remained the prototypes of the cryptography employed throughout the whole of Europe for some centuries. The Papal States used them and as late as 1793 we find them used in France. I wish here to mention specifically the so-called King's General Cipher used in 1572 by the Spanish Court, and I show here a picture of it.
But there were two exceptional cases which show that the rigidity of cryptographic thought was now and then broken during the four centuries we have been talking about in this brief historical survey. Some of the Papal ciphers of the 16th Century and those of the French Court under Kings Louis XIII and XIV exemplify these exceptions. In the case of these French Court ciphers we find that a French cryptologist named Antonio Rossignol, who was employed by Cardinal Richelieu, understood quite well the weaknesses of the one-part codes and syllabaries. It was he who, in about 1649, introduced a new and important improvement, the idea of the two-part code or syllabary, in which for encoding a message the items in the vocabulary are listed in some systematic order, nearly always alphabetical; the code equivalents, whatever they may be, are assigned to the alphabetically-listed items in random order. This means that there must be another arrangement or book for ease in decoding, in which the code equivalents are listed in systematic order, numerically or alphabetically as the case may be, and alongside each appears its meaning in the encoding arrangement, or book. The significance of this improvement you'll find out sooner or later. Codes of this sort also had variants—Rossignol was clever, indeed. One such code, found in the 1691 correspondence of Louis XIV had about 690 items, with code groups of two and three digits. Not at all bad, for those days!

Now this sort of system would appear to be quite secure, and I suppose it was indeed so, for those early days of cryptographic development—but it
wasn't proof against the cleverness of British brains, for the eminent mathematician John Wallis solved messages in it in 1689. Never underestimate the British in this science—as we'll have reason to note in another lecture in this series.

French cryptography under Kings Louis XV and XVI declined, reaching perhaps its lowest level under Napoleon the Great. It is a fact that in Napoleon's Russian enterprise the whole of his army used by a single code book of only 299 groups, practically without variants, even for the high-frequency letters. Furthermore, not all the words in a message were encoded—only those which the code clerk or the writer of the message thought were important. It's pretty clear that the Russians intercepted and read many of Napoleon's messages—this comes from categorical statements to this effect by Czar Alexander I himself. We won't be far wrong in believing that the weaknesses of Napoleon's crypto-communications formed an important factor in Napoleon's disaster. A hundred and twenty-five years later, Russian ineptitude in cryptographic communications lost them the Battle of Tannenberg and knocked them out of World War I.

The other 16th Century Papal ciphers that constituted the second exception to the general similarity of cryptographic systems of those days were quite different from those I've shown you. In this exception the ciphers were monalphabetic, but some letters had the same equivalent, so that on decipherment the context had to be used to decide which of two or more
possible plain-text values was the one meant by each cipher letter. Here's
a slide which shows one such cipher used by the Maltese Inquisitor in 1585.
You'll note that the digit 0 has two values, A and T; the digit 2 has three
values, U, V, and B, and so on. There were two digits used as nulls, 1 and 8;
digits with dots above them stood for words such as Qua, Que, Qui, and so on.

Here's a slide which shows how a message would be enciphered, and also
how one would be deciphered. A bit tricky, isn't it? Many, many years later
Edgar Allan Poe describes a cipher of this same general type, where the
decipherer must choose between two or more possible plain-text equivalents
in building up his plain text, the latter guiding the choice of the right
equivalent. The trouble with this sort of cipher is that you have to have
pretty smart cipher clerks to operate it and even then I imagine that in many
places there would be doubtful decipherments of words. It wasn't really a
practical system even in those days but it could, if used skillfully and with
only a small amount of text, give a cryptanalyst plenty of headaches. But
such systems didn't last very long because of the practical difficulties in
using them.

The first regular or official cipher bureau in the Vatican was established
in about 1546, and in Venice at about the same time, about one hundred years
before a regular cipher bureau was established in France by Cardinal Richelieu.
It is interesting to observe that no new or remarkable ideas for cryptosystems
were developed for a couple of hundred years after the complex ones I've
described as having been developed by the various Papal cryptologists. One-part and two-part syllabaries and simple or complex ones with variants were in use for many decades, but later on, in a few cases, the code equivalents were superenciphered, that is, the code groups formed the text for the application of a cipher, generally by rather simple systems of additives. Governmental codes were of the two-part type and were superenciphered by the more sophisticated countries.

The first book or extensive treatise on cryptography is that by a German abbot named Trithemius, who published in 1531 the first volume of a planned 4-volume monumental work. I said that he planned to publish four volumes; but he gave up after the third one, because he wrote so obscurely and made such fantastic claims that he was charged with being in league with the Devil, which was a rather dangerous association in those or even in these days. They didn't burn Trithemius but they did burn his books. This may be a good place to present a slide which shows that the necessity for secrecy in this business was recognized from the very earliest days of cryptology, and certainly by Trithemius. Here is the sort of oath that Trithemius recommended be administered to students in the science of cryptology. All of you have subscribed to a somewhat similar oath, but we now go further and back up the oath with a rather strict law. You've all read it, I'm sure.

We come now to some examples from more recent history. This slide shows a cipher alphabet used by Mary, Queen of Scots, who reigned from 1542 to 1567.
and was beheaded in 1587. In this connection it may interest you to learn
that question has been raised as to whether the Queen was "framed" by means
of this forged postscript in a cipher that was known to have been used by
her.

The Spanish Court under Phillip II, in the years 1555-1596, used a great
many ciphers and here's one of them. You see that it is quite complex for
those early days and yet ciphers of this sort were solved by an eminent
French mathematician named Vieta, the father of modern algebra. In 1589
he became a Councilor of Parliament at Tours and then Privy Counselor.
While in that job he solved a Spanish cipher system using more than 500
characters, so that all the Spanish dispatches falling into French hands
were easily read. Phillip was so convinced of the security of his ciphers
that when the found the French were aware of the contents of his cipher
dispatches to the Netherlands, he complained to the Pope that the French
were using sorcery against him. Vieta was called on the carpet and forced
to explain how he'd solved the ciphers in order to avoid being charged with
sorcery, a serious offense.

The next cryptologist I want you to know something about is another
Italian savant who wrote a book, published in 1563, in which he showed
certain types of cipher alphabets that have come down in history and are
famous as Porta's Alphabets. Here's an example of the Porta Table, showing
one alphabet with key letters A or B, another alphabet with key letters C
or D, and so on. I don't want to go into exactly how the key letters are used; it is sufficient to say that even to this day cryptograms using the Porta alphabets are occasionally encountered.

That Porta's table was actually used in official correspondence is shown by this slide, which is a picture of a table found among the state papers of Queen Elizabeth's time; it was used for communicating with the English Ambassador to Spain. Porta was, in my opinion, the greatest of the old writers on cryptology. I also think he was one of the early but by no means the first cryptanalyst able to solve a system of keyed substitution, that is, where the key is changing consistently as the message undergoes encipherment. Incidentally, Porta also was the inventor of the photographic camera, the progenitor of which was known as the _camera obscura_.

The next slide shows a picture of what cryptographers usually call the Vigenere Square, the Vigenere Table, or the Vigenere Tableau. It consists of a set of twenty-six alphabets successively displaced one letter per row, with the plain-text letters at the top of the square, the key-letters at the side, and the cipher letters inside. The method of using the table is to agree upon a key word, which causes the equivalents of the plain-text letters to change as the key changes. Vigenere is commonly credited with having invented that square and cipher but he really didn't and, what's more, never said he did. Here's a picture of his table as it appears in his book, the first edition of which was published in 1586. It is more complicated than as described in ordinary books on cryptology.
Here is one more example of another old official cipher. Here are the alphabets on a card which could be slid up and down, as a means of changing the key. Here is another, called the "two-square cipher", or "two-alphabet cipher". It is a facsimile of a State Cipher used in Charles the First's time, in 1627, for communicating with France and Flanders. It involves coordinates and I want you to notice that there are two complete alphabets inside it, intended to smooth out frequencies. The letters of the keywords OPTIMUS and DOMINUS serve as the coordinates used to represent the letters inside the square. Here's part of a cipher used by George III dated the 1st of September 1799.

One writer deserving special attention as a knowledgeable cryptologist in the 17th Century, and the one with whose cipher I'll close this lecture, is Sir Francis Bacon, who invented a very useful cipher and mentioned it for the first time in his *Advancement of Learning*, published in 1605, in London. The description is so brief that I doubt whether many persons understood what he was driving at. But Bacon described it in full detail, with examples, in his great book *De Augmentis Scientiarum*, which was published almost 26 years later, in 1623, and which first appeared in an English translation by Gilbert Wats in 1649 under the title *The Advancement of Learning*. Bacon called his invention the *Biliteral Cipher* and it is so ingenious that I think you should be told about it so that you will all fully understand it.

In his *De Augmentis* Bacon writes briefly about ciphers in general and
says that the virtues required in them are three: "that they be easy and not laborious to write; that they be safe, and impossible to be deciphered without the key; and lastly, that they be, if possible, such as not to raise suspicion or to elude inquiry." He then goes on to say: "But for avoiding suspicion altogether, I will add another contrivance, which I devised myself when I was at Paris in my early youth, and which I still think worthy of preservation." Mind you, this was 43 years later! Let's consult Bacon for further details. Here is a slide showing a couple of pages of the Gilbert Wats' translation of Bacon's *De Augmentis Scientiarum*. Bacon shows what he calls "An Example of a Bi-literarie Alphabet", that is, one composed of two elements, which, taken in groupings of fives, yields 32 permutations. You can use these permutations to represent the letters of the alphabet, says Bacon, but you need only 24 of them, because I and J, U and V, were then used interchangeably. These permutations of two different things--they may be "a's" and "b's", "1's" and "2's", pluses and minuses, apples and oranges, anything you please--can be used to express or signify messages. Bacon was, in fact, the inventor of the binary code which forms the basis of modern electronic digital computers. Bacon gives a brief example in the word "TUGE" --the Latin equivalent for our modern "SCRAM".

Here it is, as you see. Here's another example, which quite obviously isn't what it appears to be--a crude picture of a castle, in which there are shaded and unshaded stones. It was drawn by a friend who was a physician and the
message conveyed by it is:

My business is to write prescriptions
And then to see my doses taken;
But now I find I spend my time
Endeavoring to out-Bacon Bacon.

And here's another example, not quite so obvious. The message conveyed is:

KNOWLEDGE IS POWER.

So far all this is simple enough—to much so, Bacon says, for the example he used in the case of the word FUDGE is patently cryptic and would not avoid suspicion under examination. So Bacon goes on to describe the next step, which is to have at hand a "Bi-formed Alphabet", that is, one in which all the letters of the alphabet, both capital and small, are represented by two slightly different forms of letters. Having these two different forms at hand, when you want to encipher your secret message you write another external and innocuous message five times as long as your secret message, using the appropriate two forms of letters to correspond to the "a's" and "b's" representing your secret message. Here's FUDGE, enciphered within an external message saying "Manere te volo denece venero", meaning "Stay where you are until I come." In other words, whereas the real message says "SCRAM", the phoney one says "Stick around awhile; wait for me." Bacon gives a much longer example, the SPARTAN DISPATCH; here it is, and here's the secret message which it contains.

Bacon's biliteral cipher is an extremely ingenious contrivance. There can be no question whatsoever about its authenticity and utility as a valid
cipher. Thousands of people have checked his long example and they all find 
the same answer—the one that Bacon gives.

Here's a modern example which uses two slightly different fonts of type 
called Garamond and Imprint, and which are so nearly alike that it takes 
good eyes to differentiate them.

The fact that Bacon invented this cipher and described it in such 
detail lends plausibility to a theory entertained by many persons that 
Bacon wrote the Shakespeare Plays and that he inserted secret messages 
in those plays by using his cipher. If you'd like to learn more about this 
theory I suggest with some diffidence that you read a book entitled The 
Shakespearean Ciphers Examined. I use the word diffidence because my wife 
and I wrote the book which was published in late 1957 by the Cambridge 
University Press.

In the next lecture we'll take up cryptology as used during the period 
of the American Revolution by both the Colonial and the British Forces in 
America.
Th on 3 as revised
Insert for p. 1

Information regarding the taxes and cushans employed during that period has been rather sparse until quite recently, when a book entitled "Turicasts, Traitors and Heroes" by Col. John Bakeless, AUS, was published in 1959 by Hippocott. After a good many years of research, Col. Bakeless brought together for the first time a good deal of authentic information on the subject and some of it is incorporated in this lecture.
According to Col. Braddock—and believe it or not—I in part derive this information from the British commander-in-chief in America, General Burgoyne. He had no code or cipher at all, nor even a staff officer who knew how to compile one; he had to appeal to the commanding general in Canada, from whom he probably obtained the single substitution cipher which was used in 1776 by a British secret agent who—again, believe it or not—was
General Washington's own director-general of hospitals, Dr. Benjamin Church.

General Washington had means for secret communication from the very beginning of hostilities, probably even before the fighting began at Lexington and Concord. Of the British under General Gage, warily provided in this respect, by the time Sir Henry Clinton took over from General Howe, who succeeded Gage, they were much
better off—they had adequate or apparently adequate means for secret communication.
Summary

The third lecture in this series deals with the crypto-systems employed by the British Regulars and the Colonials during the period of the American Revolution. This is followed by a brief explanation of the cryptanalytic nature of the initial breaks in the solution of the age-old mystery presented by the ancient Egyptian hieroglyphic writing.
LECTURE 3

Continuing our survey of cryptologic history, the period of the American Revolution, in U.S. history, is naturally of considerable interest to us and warrants more than cursory treatment. Are you astonished to learn that the systems used by the American colonial forces and by the British regulars were almost identical? You shouldn't be, because the language and backgrounds of both were identical. In one case, in fact, they used the same dictionary as a code book; something which was almost inevitable because there were so few English dictionaries available. Here's a list of the systems they used:

- Simple, monalphabetic substitution—easy to use and to change.
- Monoalphabetic substitution with variants, by the use of a long key sentence. I'll show you presently an interesting example in Benjamin Franklin's system of correspondence with the elder Dumas.
- The Vigenère cipher with repeating key.
- Transposition ciphers of simple sorts.
- Dictionaries employed as codebooks, with and without added encipherment. Two were specially favored, one, Entick's *New Spelling Dictionary*; the other, Bailey's *Dictionary*. Here are a couple of pages from
The way of more complex nonalphabetic substitution ciphers, the British under Clinton's command used a system described by Bafeless in the following terms: "... a substitution cipher in which the alphabet was reversed, 'A' becoming 'a' and 'a' becoming 'A'. To destroy frequency clues, the cipher changed in each line of the message, using 'A' for 'a' in the second line, 'b' for 'b' in the third, and so on. When the cipher clerk reached 'z' in the middle of the alphabet, he started..."
over again. A spy using this cipher did not have to carry with him anything more than paper, since the system was so easy to remember." The alphabets of this scheme are simple reversed standard sequences:

\[
\begin{align*}
A &\rightarrow F & B &\rightarrow G & E &\rightarrow H & D &\rightarrow I \\
C &\rightarrow F & D &\rightarrow E & C &\rightarrow H & B &\rightarrow G \\
O &\rightarrow N & M &\rightarrow L & K &\rightarrow J & I &\rightarrow H \\
W &\rightarrow T & S &\rightarrow R & Q &\rightarrow P & O &\rightarrow N \\
U &\rightarrow T & S &\rightarrow R & Q &\rightarrow P & O &\rightarrow N \\
X &\rightarrow W & T &\rightarrow S & R &\rightarrow P & O &\rightarrow N \\
Y &\rightarrow Z &\rightarrow X &\rightarrow W & T &\rightarrow S & R &\rightarrow P \\
Z &\rightarrow Y &\rightarrow Z &\rightarrow Y &\rightarrow Z &\rightarrow Y &\rightarrow Z &\rightarrow Y
\end{align*}
\]

Bakeless does not explain why these cipher sequences are only 12 in number—not does the source from which he obtained the
information, a note found among the
Chilton Papers. [Ref. Id. A6285.2] at the Library at
the University of Michigan.

Babbage continues:

"Clinton also used another sub-
stitution cipher, with different alphabets
for the first, second and third paragraphs.
Even if an American cryptanalyst should
break the cipher in one paragraph, he
would have to start all over in the
next. As late as 1781, however Sir Henry
was using one extremely clumsy sub-
stitution cipher, in which a 'w' was 51,
I was 54, 'g' 55. Finding that 'd' was 51 and 'r' was 52, I guess 'c' 53. Some-what more complex was his 'proper' cipher, in which twenty-five letters of the alphabet were placed in squares, then an angle alone would represent a letter, the same angle with a dot another letter, the same angle with two dots still another. In some cases, cryptography was used only for a few crucial words in an otherwise clear message, a method also favored by certain American officials.
Of the first cipher mentioned in the preceding extract, there is much more to be said. Perhaps the cipher was limited by space considerations. In any case, I will leave that story for another time and place. As for the second cipher, Daceless mentions in the extract I can give you the whole alphabet, for it exists among the Clinton Papers:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

There is no explanation why the
Sequence beginning with 50 stops with E=55 and then, started with F=66, goes straight on without any break to Z=98. (Remember that in those days I and J were used interchangeably, as were U and V).

Finally, as to what Bakeless (and others) call the "pegpen" cipher, this is nothing but the Rosary old so-called "Masonic" cipher based upon the 4 cross figure: 

\[
\begin{align*}
a & : \mathbb{I}, \\
b & : \mathbb{I}, \\
c & : \mathbb{I}
\end{align*}
\]

which can accommodate 27 characters, not 25 as Bakeless indicates. Letters can be inserted in the scheme in many different arrangements.
are shown in Fig. 1.

The former. To represent a word by code equivalent you simply indicated the page number, then whether Column 1 or Column 2 contained the word you wanted, and then the number of the word in the column. Thus: The word "jacket" would be represented by 178-2-2.

f. Small, specially-compiled, alphabetical 1-part codes of 600-700 items and code names; our old friend the syllabary or repertory, of hoary old age but with new dress.

g. Ordinary books, such as Blackstone's *Commentaries*, giving the page number, the line number and the letter number in the line, to build up, letter-by-letter, the word to be represented. Thus: 125-12-17 would indicate the 17th letter in the 12th line on page 125; it might be the letter T.

h. Secret inks.

i. Special designs or geometric figures, such as one I'll show you presently.

j. Various concealment methods, such as using hollow quills of hollowing out a bullet, and inserting messages written on very thin paper. Strictly speaking, however, this sort of strategy doesn't belong to the field of cryptology. But it's a good dodge, to be used in special cases.

I've mentioned that code or conventional names were used to represent the names of important persons...
and places in these American colonial and British
cryptograms of the Revolution. Here are some examples
taken from a system of code names prepared by Major Andre,
of the sort of names the British used as code names.
The British spy, Chief of Intelligence under General Clinton:
For American Generals - The names of the
Apostles, for instance:

General Washington was "James"
General Sullivan was "Matthew"

Names of Cities: Philadelphia - Jerusalem
                  Detroit - Alexandria

Names of Rivers and Bays: Susquehanna - Jordan
                            Delaware - Red Sea

Miscellaneous: Indians - Pharisees
                Congress - Synagogue

On Fig. 7, we see
Here's a very interesting slide, a British cipher
message of the vintage 1781. It was deciphered before
finding the key, always a neat trick when or if you
can do it. Here's the key-the title page of the then
current British Army Lists-is shown in Fig. 8.

I'm sure you've learned as school children all
about the treasonable conduct of Benedict Arnold when
he was in command of the American Forces at West Point;
but you probably don't know that practically all his
exchanges of communications with Sir Henry Clinton,
Commander of the British Forces in America, were in
cipher, or in invisible inks. Here's an interesting
slide-showing one of Arnold's cipher messages, in
Fig. 26, the plain text. Arnold left a blank space in the chair, the rest he considered unimportant. For the important ones he used a dictionary as a codebook, indicating the page number, column number, and line number corresponding to the position in the dictionary of the plain-text word which the code group represents. Arnold added 7 to these numbers, which accounts for the fact that first number in a code group is never less than 8. The central number is always either 8 or 9, and the third number is never less than 8 or more than 36. The significant sentence appears near the middle of the
message: If I 198.9.34.1858.31 at 197.8.8 ...

Yields the plain text: If I point out a plan of cooperation by which H.S.I. [Sir Henry Clinton] shall possess himself of West Point, the Garrison etc., etc., etc. If forty thousand pounds Sterling I think still be a cheap purchase for an object of so much importance.

The signature, 1729.19 probably stands for the word "Moore", Arnold's code name in these communications was "A Moore". He had also another name, "Gustave".
Fig. 3 at the top shows the code message; at the bottom is the plain text. Arnold used the same additive as in the preceding example.

Insert #2 for p. 4.
In Fig. 14 the left-hand portion shows the "phony" message, the right-hand one, the real message. To make it easy for the reader I have below in typed form both the "phony" and the secret text, the latter being underlined. Marks leaving small rectangular apertures etc.
Explain Courage in Crisis
which he offers to give up West Point for $20,000,

is shown in Fig. 2. A Figure 3 is a message

however, in which he gave the British

information which might have led to the capture of

his commander-in-chief, General Washington.

Washington was too smart to be ambushed—he went by

a route other than the one he said he'd take.

You may find the next slide interesting as

an example of the special sort of mask or grille used

by Arnold and by the British in their negotiations

with him. The real or significant text is written

in lines outlined by an hour-glass figure and then dummy

words are supplied to fill up the lines so that the

entire letter apparently makes good sense. To read

the secret message you're supposed to have the same

size hour-glass figure that was used to conceal the

message. The significant text in this example is

underlined:

"You will have heard, Dr. Sir, I doubt not only

before you can have reached you that Sir W. Howe

is gone from hence. The rebels imagine that

he is gone to the Delaware by this time;

however he has filled Chesapeake Bay with

surprise and terror... etc."

Arnold even used the trick, mentioned above in

method j, that was quite similar to one used recently
Insect for p.5 transferred matter from p.3.

The numbers in the first series obviously refer to line numbers and letter numbers in the line of a key text, the first series of numbers, viz., 22. 6.7. 39. 5.9. 17, indicating line number 22, letter numbers 6.7.39.5.9.

In that line, because of the many repetitions the plain text was obtained by straightforward analysis by an officer present on duty in NSA, Capt. Edward W. Knapp, to whom I am indebted for this interesting example.
The plain text, once obtained, gave him clues to what the key text might be, simply by replacing the plain text letters in the numerical-equivalent order in the putative key text. This done, Capt. Knapp was quick to realize what the key text was. An army list! The date of the message enabled him to find the list without much difficulty in the Library of Congress.
An interesting episode involving concert of this sort is recorded in the Daily Bazaar, in his recently published book "Confessions."

An urgent message of Sir Henry Clinton, dated 8th October 1777, was concealed in an oval box about the size of a rifle bullet, which was handed to Daniel Taylor, a young officer who had been promised promotion if he got through alive. The bullet was made of silver, so that the spy could swallow it without injury from corrosion.

Almost as soon as the pistol, Taylor
was captured... Realizing his peril too late, the spy fell into a fit of horror and, crying, "I am lost!" swallowed the silver bullet. Administration of a strong emetic soon produced the bullet with fatal results, for Taylor was executed. "A rather heartless American joke went round," adds Baker, "that Taylor had been condemned 'out of his own mouth.'"
by the Russian spy, Colonel Abel, who was arrested in New York in June 1957, tried and convicted, and is still languishing in a Federal prison. Here's a picture of the gentleman. How would you like to meet with him suddenly some dark night at a secret rendezvous? We need see (Fig. 5) one Benedict Arnold message that never was deciphered. Only one example is extant; certain words have purely arbitrary meanings, as prearranged.

There was an American who seems to have been the Revolution's one-man National Security Agency, for he was the one and only cryptologic expert Congress had, and, it is claimed, he managed to decipher nearly all, if not all, of the British code messages obtained in one way or another by the Americans. Of course, the chief way in which enemy messages could be obtained in those days was to capture couriers, knock them out or knock them off, and take the messages from them. This was very rough stuff, compared to getting the material by radio intercept, as we do nowadays.

I think you'll be interested to hear a bit more about that one-man NSA. His name was James Lovell and besides being a self-trained cryptologist, he was also a member of the Continental Congress. There's on record a very interesting letter which he wrote to General Nathaniel Greene, with a copy to General Washington. Here it is.
Philadephia, Sept. 21, 1789

Sir:

You once sent some papers to Congress which no one about you could decipher. Should such be the case with some you have lately forwarded I presume that the result of my pains, herewith sent, will be useful to you. I took the papers out of Congress, and I do not think it necessary to let it be known here what my success has been in the attempt. For it appears to me that the Enemy make only such changes in their Cypher, when they meet with misfortune, as makes a difference of position only to the same alphabet, and therefore if no talk of Discovery is made here or by your Family, you may be in chance to draw Benefit this campaign from my last Night's watching.

I am Sir with much respect.

Your Friend,

Maj. Genl. Greene

JAMES LOVELL

In telling you about Lovell I should add to my account of that interesting era in cryptologic history an episode I learned about only recently. When a certain message of one of the generals in command of a rather large force of Colonials came into Clinton's possession he sent it off post haste to London for
solution. Of course, Clinton knew it was going to take a lot of time for the message to get to London, be solved and returned to America—and he was naturally a bit impatient. He felt he couldn't afford to wait that long. Now it happened that in his command there were a couple of officers who fancied themselves to be cryptologists and they undertook to solve the message, a copy of which had been made before sending the original off to London. Well, they gave Sir Henry their solution and he acted upon it. The operation turned out to be a dismal failure, because the solution of the would-be-cryptanalysts happened to be quite wrong! The record doesn't say what Clinton did to those two unfortunate cryptologists when the correct solution arrived from London some weeks later. By the way, you may be interested in learning that the British operated a regularly-established cryptanalytic bureau as early as in the year 1630 and it continued to operate until the end of July 1844. Then there was no such establishment until World War I. I wish there were time to tell you some of the details of that fascinating and little known bit of British history.

There's also an episode I learned about only very recently, which is so amusing I ought to share it with you. It seems that a certain British secret
agent in America was sent a message in plain English, giving him instructions from his superior. But the poor fellow was illiterate and there wasn't anything to do but call upon the good offices of a friend to read it to him. He found such a friend, who read him his instructions. What he didn't know, however, was that the friend who'd helped him was one of General Washington's secret agents!

The next slide shows a picture of one of several syllabaries used by Thomas Jefferson. It is constructed on the so-called two-part principle which was explained in the preceding lecture. This is a portion of the encoding section, and here's a portion of the decoding section, in which the code equivalents are in numerical order accompanied by their meanings as assigned them in the encoding section. This sort of system, which, as I've already explained, was quite popular in Colonial times as in the early days of Italian cryptography, is still in extensive use in some parts of the world. Jefferson was an all-around genius, and I shall have something to say about him and cryptography in a subsequent lecture.

A few minutes ago I mentioned Benjamin Franklin's cipher system, which, if used today, would be difficult to solve, especially if there were only a small amount of traffic in it. Let me show you what it was.
Franklin took a rather lengthy passage from some book in French and numbered the letters successively. These numbers then became equivalents for the same letters in a message to be sent. Because the key passage was in good French, naturally there were many variants for the letter E—in fact, there were as many as one would expect in normal plain-text French; the same applied to the other high-frequency letters such as R, N, S, I, etc. What this means, of course, is that the high-frequency letters in the plain text of any message to be enciphered could be represented by many different numbers and a solution on the basis of frequency repetitions would be very much hampered by the presence of many variant values for the same plain-text letter. Here you can see this very clearly.

I know of but one case in all our U.S. history in which a resolution of Congress was put out in cryptographic form. Here's a slide which shows it—a resolution of the Revolutionary Congress dated 8 February 1782. I have in my collection not only a copy of the resolution but also a copy of the ciphering which it can be deciphered. Interest in cryptology in America seems to have died with the passing of Jefferson and Franklin. But if interest in cryptology in America wasn't very great, if it existed at all after the Revolution, this was not the case in Europe. Books on the subject were written, not by professionals, perhaps, but by learned
amateurs, and I think you will find some of them in the NSA library if you’re interested in the history of the science. Here’s the frontispiece of a French book the title of which I translate as “Counter-espionage, or keys for all secret correspondence.” It was published in Paris in 1793. Here’s Dr. Gryppy himself, and this is perhaps a breadboard model of a G-2 intelligence analyst, or maybe an early model of a WAC.

I am going to take a bit of time now to tell you something about Egyptian hieroglyphics, not only because I think that that represents the next and a great landmark in the history of cryptology, but also because the story is of general interest to any aspiring cryptologist. About 1821 a Frenchman, Champollion, startled the unenlightened world by beginning to publish translations of Egyptian hieroglyphics, although in the budding new field of Egyptology much had already transpired and been published. In Fig. 13 we see a picture of the gentlemen and in Fig. 14 a picture of the great Napoleonic find that certainly facilitated and perhaps made possible the solution of the Egyptian hieroglyphic writing—the Rosetta Stone, which was found in 1799 at Rashid, or, as the Europeans call it, Rosetta, a town in northern Egypt on the west bank of the Rosetta branch of the Nile. Rosetta was in the vicinity of Napoleon’s operations which ended in disaster and when the peace treaty was written...
Article XII of it required that the Rosetta Stone, the significance of which was quickly understood by both the conquered French and victorious British commanders, be shipped to London, together with certain other large antiquities. The Rosetta Stone still occupies a prominent place in the important exhibits at the British Museum. The Rosetta Stone is a bi-lingual inscription, because it is in Egyptian and also Greek. The Egyptian portion consists of two parts, the upper one in hieroglyphic form, the lower one in a sort of cursive script, also in Egyptian but called "Demotic."

It was soon realized that all three texts were supposed to say the same thing, of course, and since the Greek could easily be read it served as what in cryptanalysis we call a "crib." Any time you are lucky enough to find a crib it saves you hours of work. It was by means of this bi-lingual inscription that the Egyptian hieroglyphic writing was finally solved, a feat which represented the successful solution to a problem the major part of which was linguistic in character. The cryptanalytic part of the task was relatively simple. Nevertheless, I think that anyone who aspires to become a professional cryptologist should have some idea as to what that cryptanalytic feat was, a feat which some professor--but not of cryptologic science, I think it was Professor Norbert Wiener, of
the Massachusetts Institute of Technology—said was the greatest cryptanalytic feat in history. We shall see how wrong the good professor was, because I'm going to demonstrate just what the feat really amounted to by showing you some simple pictures.

First, let me remind you that the Greek text served as an excellent crib for the solution of both Egyptian texts, the hieroglyphic and the Demotic, the latter merely being the conventional abbreviated and modified form of the Hieratic character or cursive form of hieroglyphic writing that was in use in the Ptolemaic Period.

The initial step was taken by a Reverend Stephen Weston who made a translation of the Greek inscription which he read in a paper delivered before the London Society of Antiquaries in April 1802.

In 1818 Dr. Thomas Young, the physicist who first proposed the wave theory of light, compiled for the 4th volume of *Encyclopædia Britannica*, published in 1819, the results of his studies on the Rosetta Stone and among them there was a list of several alphabetic Egyptian characters to which, in most cases, he had assigned correct values. He was the first to grasp the idea of a phonetic principle in the Egyptian hieroglyphs: and he was the first to apply it to their
decipherment. He also proved something which others
had only suspected, namely, that the hieroglyphs in
ovals or cartouches were royal names. But Young's
name is not associated in public mind with the decipherment
of Egyptian hieroglyphics— that of Champollion is
very much so. Yet much of what Champollion did was
based upon Young's work. Perhaps the greatest credit
should go to Champollion for recognizing the major
importance of an ancient language known as Coptic as
a bridge that could lead to the decipherment of the
Egyptian hieroglyphics. As a lad of seven he'd made
up his mind that he'd solve the hieroglyphic writing
and in the early years of the 19th century he began
to study Coptic. In his studies of the Rosetta Stone
his knowledge of Coptic, a language the knowledge
of which had never been lost, enabled him to deduce
the phonetic value of many syllabic signs, and to
assign correct readings to many pictorial characters,
the meanings of which became known to him from the
Greek text on the Stone.

The following step-by-step account of the solution
is taken from a little brochure entitled The Rosetta
Stone, published by the Trustees of the British Museum.
It was written in 1922 by E. A. Wallis Budge and was
revised in 1950. I quote:
"The method by which the greater part of the Egyptian alphabet was recovered is this: It was assumed correctly that the oval, or "cartouche" as it is called, always contained a royal name. There is only one cartouche (repeated six times with slight modifications) on the Rosetta Stone, and this was assumed to contain the name of Ptolemy, because it was certain from the Greek text that the inscription concerned a Ptolemy. It was also assumed that if the cartouche did contain the name of Ptolemy, the characters in it would have the sounds of the Greek letters, and that all together they would represent the Greek form of the name of Ptolemy. Now on the obelisk which a certain Mr. Bankes had brought from Philae there was also an inscription in two languages, Egyptian and Greek. In the Greek portion of it two royal names are mentioned, that is to say, Ptolemy and Cleopatra, and on the second face of the obelisk there are two cartouches, which occur close together, and are filled with hieroglyphs which, it was assumed, formed the Egyptian equivalents of these names. When these cartouches were compared with the cartouche on the Rosetta Stone it was found that one of them contained hieroglyphic characters that were almost identical with those which filled the cartouche on the Rosetta Stone. Thus there was good reason to believe that the cartouche on the Rosetta Stone contained the name of Ptolemy.
written in hieroglyphic characters. The forms of the cartouches are as follows:

On the Rosetta Stone

On the Obelisk from Philae

In the second of these cartouches this single sign (point-it-out) takes the place of these three signs (point-the-out) at the end of the first cartouche.

Now it has already been said that the name of Cleopatra was found in Greek on the Philae Obelisk, and the cartouche which was assumed to contain the Egyptian equivalent to this name appears in this form:

Taking the Cartouches which were supposed to contain the names of Ptolemy and Cleopatra from the Philae Obelisk, and numbering the signs we have:

Ptolemy, A.

Cleopatra, B.

Now we see at a glance that No. 1 in A and No. 5 are identical, and judging by their position only in the names they must represent the letter P. No. 4 in A and No. 2 in B are identical, and arguing as before from their position they must represent the letter L. As L is the second letter in the name of Cleopatra, the sign No. 1 (point) must represent K.

Now in the cartouche of Cleopatra we know the values of Signs Nos. 1, 2 and 5, so we may write them down thus:
In the Greek form of the name of Cleopatra there are two vowels between the L and the P, and in the hieroglyphic form there are two hieroglyphs, this (point) and this (circle), so we may assume that the first is E and the one is O. In some forms of the cartouche of Cleopatra, No. 7 (the hand) is replaced by a half circle, which is identical with No. 2 in A and No. 10 in B. As T follows P in the name Ptolemy, and as there is a T in the Greek form of the name of Cleopatra, we may assume that the half circle and the hand have substantially the same sound, and that that sound is T. In the Greek form of the name Cleopatra there are two a's, the positions of which agree with No. 6 and No. 9, and we may assume that the bird has the value of A. Substituting these values for the hieroglyphs in B we may write it thus:

Thomas Young noticed that these two signs always followed the name of a goddess, or queen, or princess, so the other early decipherers regarded the two signs as a mere feminine termination. The only sign for which we have no phonetic equivalent is No. 8, the lens, and it is obvious that this must represent R. Inserting this value in the cartouche we have the name of Cleopatra deciphered. Applying now the values which we have learned from the cartouche of Cleopatra
to the cartouche of Ptolemy, we may write it thus:

We now see that the cartouche must be that of Ptolemy, but it is also clear that there must be contained in it many other hieroglyphs which do not form part of his name. Other forms of the cartouche of Ptolemy are found, even on the stone, the simplest of them written thus:

\[ (\text{point out on slide}) \]

It was therefore evident that these other signs were royal titles corresponding to those found in the Greek text on the Rosetta Stone meaning "ever-living, beloved of Ptah." Now the Greek form of the name Ptolemy, i.e. Ptolemaios, ends with S. We may assume therefore that the last sign in the simplest form of the cartouche given above has the phonetic value of S. The only hieroglyphs now doubtful are \( \text{(\text{m})} \) and \( \text{(\text{n})} \), and their position in the name of Ptolemy suggests that their phonetic values must be M and some vowel sound in which the I sound predominates.

These values, which were arrived at by guessing and deduction, were applied by the early decipherers to other cartouches, e.g.:

Now, in No. 1, we can at once write down the values of all the signs, viz., P. I. L. A. T. R. A, which
is obviously the Greek name Philoctera. In No. 2 we know only some of the hieroglyphs, and we write the cartouche thus:

\[ (\text{???)} \]

It was known that the running-water sign occurs in the name Berenice, and that it represents the last word of the transcript of the Greek title Εἰκασσαρος," and therefore represents some S sound. Some of the forms of the cartouche of Cleopatra begin with (this=sag), and it is clear that its phonetic value must be K. Inserting these values in the above cartouche we have:

\[ (\text{???)} \]

which is clearly meant to represent the name "Alexandros," or Alexander. The position of this sign (point) shows that it represented some sound of E or A.

Well, I've showed you enough to make fairly clear what the problem was and how it was solved.

That's the way in which the initial break was made in the decipherment of Egyptian hieroglyphics, and, as you may already have gathered, the cryptanalysis was of a very simple variety. It was very fortunate that the first attacks on Egyptian hieroglyphics didn't have to deal with enciphered writing. Yes, the Egyptians also used cryptography; there are "cryptographic hieroglyphics!" Here, for instance, is an example of
The following is a long article by Étienne Duleston in "Revue d'Égyptologie", Paris, 1933. It is entitled "Essay sur la cryptographie privée de la fin de la XVIIIe dynastie" and I quote from page 14 thereof:

"Finally, the playful tendency, already pointed out in the Construction of the alphabet, appears in the orthography. Certain groups offer, when
read so clear, a fallacious meaning: they are intentions, motives, and am I phrasing the enigmatic character of this cryptography:

Fig. 17
substitution. That-character-in-place-of-this-one
means—'to-speak.'

Before leaving the story of Champollion's mastery
of Egyptian hieroglyphic writing I think I should
re-enact for you as best I can in words what he did
when he felt he'd really reached the solution to the
mystery. I'll preface it by recalling to you what
Archimedes is alleged to have done when he solved a
problem he'd been struggling with for some time.
Archimedes was enjoying the pleasures of his bath
and was just stepping out of the pool when the solution
of the problem came to him like a flash. He was so
overjoyed that he ran, naked through the streets
shouting "Eureka! I've found it, I've found it."[1]

Well, likewise, when young Champollion one day had
concluded he'd solved the mystery of the Egyptian
hieroglyphics, he set out on a quick mile run to
the building where his lawyer brother worked, stumbled
into his brother's office, shouted: "Eugene, I've
got it!", and flopped down to the floor in a trance
where he is said to have remained immobile and
completely out for five days. Don't let that sort of
thing happen to you around here when and if you find
the answer to a complex problem. The char force will
probably sweep you up and throw you into the secret
trash bin for disposition by burning.
I shouldn't leave this brief story of the cryptanalytic phases of the solution of the Egyptian hieroglyphic writing without telling you that there remain plenty of other sorts of writings which some of you may want to try your hand at deciphering when you've learned some of the principles and procedures of the science of cryptology. A list of thus-far undeciphered writings was drawn up for me by Professor Alan C. Ross of London University in 1945 and had 19 of them. Since 1945 only two have been deciphered, Minoan Linear A and Linear B writing. The Easter Island writing is said to have very recently been solved, but I'm not sure of that. There are some, maybe just a very few, who think the hieroglyphic writing of the Ancient Maya Indians of Central America may fall soon, but don't be too sanguine about that.

Should any of you be persuaded to tackle any of the still undeciphered writings in the list drawn up by Professor Ross, be sure you have an authentic case of an undeciphered language before you. Here's one that was written on a parchment, known as the Michigan Papyrus. It had baffled certain savants who had a knowledge of Egyptology who attempted to read it on the theory that it was some sort of variation—a much later modification—of Egyptian hieroglyphic writing. These old chaps gave it up as
The next period of importance in the brief account of the history of cryptology is the one which deals with the codes and ciphers used by the contestants in our Civil War, the period 1861-65. It is significant and important because, for the first time in history, rapid and secure communications on a large scale became practicable in the conduct of organized warfare.
and world-wide diplomacy. They became practicable when cryptography and telegraphy were joined in happy, sometimes contentious, but long-lasting wedlock.
a bad job. Not too many years ago it came to the attention of a young man who knew very little about Egyptian hieroglyphics. He saw it only as a simple substitution cipher on some old language. He tackled the Michigan Papyrus on that basis and solved it. He found the language to be early Greek. And what was the purport of the writing? Well, it was a wonderful old Greek beautician's secret formula for further beautifying lovely Greek young beauties—maybe the bathing beauties of those days.

There is one person I should mention before coming to the period of the Civil War, or, as some people prefer to call it, the war between the States, in U.-S. history. I refer here to Edgar Allan Poe, who in 1842 or thereabouts, kindled an interest in cryptography in newspapers and journals of the period. For his day he was certainly the best informed person in the country of U.-S. on cryptologic matters outside the regular employees of Government departments interested in the subject, and in saying this I am assuming that cryptology was used to a limited extent by our Department of State for communicating with ambassadors and consuls abroad. I suppose that the Army and Navy used codes but the record is a bit fragmentary, and I won't be able to come to them a little later, when I'll show you examples of them.
To return to Poe, one of our early columnists, there's an incident I'd like to tell you about in connection with a challenge he printed in one of his columns, in which he offered to solve any cipher submitted by his readers. He placed some limitations on his challenge, which amounted to this—that the challenge messages should involve but a single alphabet with variants. In a later article Poe tells about the numerous challenge messages sent him and says: "Out of perhaps 100 ciphers altogether received, there was only one which we did not immediately succeed in resolving. This one we demonstrated to be an imposition—that is to say, we fully proved it a jargon of random characters, having no meaning whatever." I wish that cipher had been preserved for posterity, because it would be interesting to see what there was about it that warranted Poe in saying that "we fully proved it a jargon of random characters."

Maybe I'm not warranted in saying of this episode that Poe reminds me of a ditty sung by a character in a play put on by some undergraduates of one of the colleges of Cambridge University in England. This character steps to the front of the stage and sings:

"I am the Master of the College,
What I don't know ain't knowledge."
REF ID: A62852

If you are interested sufficiently to wish to learn something about Poe’s contributions to cryptography, I refer you to a very fine article by Prof. W. K. Wimsatt Jr., entitled “What Poe Knew about Cryptography,” Publication of the Modern Language Association of America, New York, Vol. LVIII, No. 3, September 1943, pp. 754-79. In it you’ll find references to what I have published on the same subject.
Thus, Poe. What he couldn't solve wasn't a real cipher--
a very easy out for any cryptologist up against something
tough.

This completes the third lecture in this series.

In the next one we shall come to that interesting period
in cryptologic history in which codes and ciphers were
used in this country in the War of the Rebellion,
the War Between the States, the Civil War--you use your
own pet designation for that terrible and costly struggle.
In the brief time at my disposal this afternoon, it will be impossible to touch upon all phases of code work. Hence I shall confine myself chiefly to those phases which will probably at some future time concern most of those present; namely, the safeguards and precautions which must be observed in code or cipher operations in order to maintain the secrecy of the system of communication adopted.

A preliminary word of explanation with regard to the two terms "Code" and "Cipher" may be necessary. To most of you, the two words mean practically the same thing, but such is not the case. Modern cryptography draws a rather sharp distinction between the two terms.

A CIPHER, taken in a broad sense, is the name applied to any system of cryptography which involves the transformation of the individual letters of the original, intelligible text of a message into a secret or unintelligible form by means of previously established agreements which subsequently permit of the reconstruction of the original text from the secret text.

The original, intelligible text of the message is called the PLAIN TEXT. The resultant unintelligible or secret text is called the CIPHER TEXT.

The operation of transforming the Plain Text into the equivalent Cipher Text is called Enciphering; the reverse operation is called Deciphering.

A CODE is the name applied to a specialized system of cryptography which involves the transformation of the original, intelligible plain text of a message into a secret or unintelligible form by means of a book or a document which gives conventional words, or uniform, arbitrary combinations or numbers as the equivalents of not only the letters, but also the words, phrases, or entire sentences of the original text. It is obvious that identical copies of the Code or Code book must be in the possession of the correspondents. The operations which apply to this system are called ENCODING and DECODING.

While there are some ciphers which resemble code or tend to approach code, yet the distinction which exists and which should be made between cipher and code is this: in cipher one deals with the individual letters as units; in code, while one may deal occasionally with the individual letters, the operation is

Approved for Release by NSA on 11-18-2013 pursuant to E.O. 13526
principally concerned with the phrases or sentences taken as units.

When the code designations of the encoded words of a message are afterwards enciphered, or in other words, when a message is first encoded and then the code equivalents are enciphered, the result is called ENCIPIERED CODE. For example, if the code word for the phrase, "By order of the Commander-in-Chief" is FOSAL, and if this code word is then enciphered into the form CITAX or into the number 17521, the latter is then known as enciphered code.

So far as I am aware, a system of secret communication which is absolutely impregnable against solution by the enemy and which at the same time is suited to the needs of naval, military, or diplomatic offices, is not known to the science of cryptography. I do not know how sufficiently to impress upon your minds the necessity for exercising the most rigid and painstaking care in the use of the codes or ciphers which may at some future time be entrusted to you. I have seen elaborate code and cipher systems rendered absolutely valueless through the carelessness and ignorance of one man. From the point of view of the Intelligence Department it seems to me that a man who flagrantly disregards or violates the rules and regulations laid down by the Code and Signal Section is as deserving of the extreme punishment for a breach of discipline resulting in the actual or potential loss of life of his comrades as is the man who consciously betrays them by furnishing information to the enemy. Let me tell you of one instance which to my knowledge had disastrous consequences.

You will recall that in March 1918 the Germans launched their last and greatest offensive on the Western front. Careful preparations and provision had been made for nearly everything. On the day of the opening of the offensive an absolutely new type of code went into effect in every sector simultaneously on the whole front. Months of work by the allied intelligence department upon the German trench code were rendered worthless at one stroke. We had to begin all over again and while the general situation on the whole battle front looked very dark, during those critical weeks, things looked especially dark to the members of the code and cipher section.

Among the very first messages, in the new code that were intercepted by our own Signal Corps was a set of three messages passing between two stations opposite the front held by the American forces. Here they are:

This solution was of vastly greater importance than is apparent on the face of the decoded message. The message itself meant, for us, at least nothing. Even to this day I can only surmise what it meant. But the most important feature
of the message was that it at once gave definite clues with regard to the nature and mechanics of the new system. Certain features of the groups in this message led to the making of some assumptions which were tested upon other messages; they proved to be correct. At one blow the whole new system fell like a house of cards.

I have said that this message meant nothing to us; it may have meant but very little more to the Germans between whom the message was exchanged. But this message led to the breaking of the whole code. Certainly the German operator would not have committed this inexcusable blunder had the message been of great tactical importance. But for the code solver all messages are of equal importance — and most often the messages of least consequence as regards the tactical situation, yield the most far reaching results, and are therefore the most disastrous as far as maintaining the secrecy of the code is concerned. (Practice messages) were used regularly at 6 a.m. and 6 p.m. while the real news in code was being transmitted.

I might add that to complete the dramatic situation resultant upon the solution of this first message, the news, together with the date, was sent to the general headquarters of our allies by special aeroplane because at that time direct telegraphic communication between the American and the other code offices had not yet been established.

How many of his comrades lost their lives as a direct result of this one German's blunder, no one can say. He was guilty of violating one of the most important rules of code work, namely, a message once transmitted in code or cipher must NEVER be repeated in any other form whatsoever.

If it must be repeated because of mutilation or garbles, an exact duplicate of the original code or cipher text must be sent. If after several repetitions the message is still unintelligible, because of a failure on the part of the receiving station to be in possession of the necessary data for decodement, then it may be necessary to transmit the message in another form. Whatever this second form be, it should bear no resemblance whatsoever to the first message as regards internal form of the plain text which has been encoded or enciphered. In other words, the plain text of the original message must be altered in form to the greatest extent possible, consistent with the intent and meaning of the message. This process of altering the plain contents of a message for the purpose of changing its form, without material change in meaning, so that a close comparison between the plain text and its equivalent code or cipher text will be impossible, is called PARAPHRASING. I shall refer to it later. As far as possible no information should ever be given in any
plain text communication, code, or cipher message which may connect it in any way
with a message previously sent. Of course, I need hardly add that a message once
sent in code or cipher must never be repeated in plain text under any circumstances -
there is no exception to this rule. The danger of such a procedure is so obvious
that it is hard to conceive of any normal thinking person doing it. Yet, let me tell
you of an actual instance.
(Case 2) I can recall one at the moment.

It seems hardly necessary to say that the insertion of plain text in code
or cipher text is so highly dangerous that it should never be done under any circum-
stances. Of course it is possible that in a long report, only one or two paragraphs
might be secret, in which case, the rest of the report could be sent in plain text,
providing that the plain text matter will give no clue whatever to the encoded or
enciphered matter. However, the best plan of all would be to make them separate.
The insertion of any signs, abbreviations, or punctuation should be absolutely
prohibited. This would seem obvious but let me tell you of an instance in which the
insertion of an abbreviation lead to the solution of a message. (Case 3).

The plain text and code or cipher messages should never appear on the
same sheet of paper; in the event of the loss of the papers or their capture, there
would be less likelihood of the two being compared. As soon as a message has been
encoded or decoded, all the work sheets used in the process must be destroyed by
burning in strict accordance with the regulations set forth. A waste basket in a
code room is the most dangerous article of furniture in it. If it is necessary to
keep an exact copy of the plain text, the same should be kept in the coding room and
guarded with as much secrecy and care as the code itself. Where a plain text copy of
the message must be furnished to departments whose files are not secret, the plain
text must be carefully paraphrased.

The work of paraphrasing requires considerable skill and practice, and
in the case of matters of very great importance, the paraphrasing should be done or
supervised by the higher officers. In all cases the paraphrasing must be done before
the message leaves the coding room.

To many of you paraphrasing a message is more or less unfamiliar, and
it might be advisable for me to give an illustration. It will do no good to change
merely the order of a word or two in each sentence. The entire form of the message
must undergo the change. The message should be altered by the substitution of
synonyms, the elaboration of phrases, the change from active to passive voice and vice versa, etc. all of which should be without essential change in the significance of the message. Then the sentences may be shifted about so that the final result bears very little resemblance to the original form of the message. The best way of approaching the task is first to read the message over very carefully in order to get a clear idea of its meaning. Once that is done the principal ideas are to be expressed in a form as different as possible from the original, without material alteration in the intent of the message. (Case 4)

With all these precautions, it hardly seems necessary to remind you that encoded or enciphered messages must never be filed with their equivalent plain text. I have personal knowledge of such an instance.

All the precautions that I have mentioned so far are of a general nature, but I must add one more: NEVER SEND CODE OR CIPHER MESSAGES BY WIRELESS OR BY ANY MEANS SUSCEPTIBLE OF EASY INTERCEPTION WHEN A MORE SECRET MEANS IS AVAILABLE AND WHEN THE MATTER DOES NOT REQUIRE IMMEDIATE ATTENTION. If there are reports upon matters of no particular importance at the moment, they might better be sent by courier or through the regular channels rather than transmitting them by wireless. The reason for this is that the greater the amount of traffic an enemy can intercept, the greater his chances for breaking into the code. Furthermore, the enemy may in certain cases gain valuable information merely from the number of messages sent and their length, without being in a position to read a single one of them. That applies more to military affairs, I suppose, than naval. It may be interesting to you to learn a few facts bearing upon this phase of the question by giving you an instance from the recent war.

(Case 5) The following are used to send reports by wireless:

I should think that it would be wise to regulate the amount of traffic during an actual state of war so that the enemy can draw no conclusions from the number of messages. In regulating the amount of traffic, routine messages such as daily or weekly reports, especially if they are of set forms, must be sent by other means. They are highly dangerous because of the similarities of contents. There is a method of breaking into a code, called the Analogy Method, which makes use of just such messages.

(Case 6)

The sending of short messages should be avoided because the nature of such messages is rather limited and if they are apt to be very frequent they
constitute favorite points of attack. (Case 7.)

One way to eliminate this danger is to make good use of the dummy groups; but their use must be judicious. (Case 8.)

The use of dummies is to be emphasized, especially in phrases or between words likely to be repeated several times in the same messages or in several messages. They must be employed in the spelling of such words as are not present in the code. Avoid the use of words and phrases not in the code when other words or phrases with the same significance are present, because it is absolutely necessary to avoid spelling out words or phrases as much as possible. There are advantages in spelling out such words when it is unnecessary and moreover such procedure opens the way for an attack by the enemy because it has been found that the spelling groups in a code constitute the weakest elements of thousands. The fewer spelling groups used the more secure will be the code. It may sound far-fetched to you if I tell you that the code man, after a careful study of the text of a considerable number of messages, is able to determine, for the majority of the groups that appear, which ones represent punctuation; which, spelling groups; which, military or naval units; etc.

In the case of the spelling groups after a sufficient number of them have been classified as being spelling groups, there is involved only a more or less simple case of substitution cipher. Once a few of the spelling groups have been solved a great break has been made into the code. Remember then, use the spelling groups as little as possible, and when they must be used exercise caution and use your best judgment. (Cases 9 and 10)

Another rule, which seems almost too obvious to mention, is that all operations applying to the system of enciphering, or encoding, must be completed. If there are three operations necessary, it would be highly dangerous to leave off one of them, say the final one. I know of two cases in which an encipherer, either through carelessness or a foolish belief that one operation was sufficient, left off the final operation in enciphering. The results were most disastrous.

After a consideration of the general principles and rules that apply in the preparation of messages, we come to a discussion of some special and detailed features.

I suppose, if I were asked what is the most important of the minor rules with regard to all cryptographic processes, for the purposes of making them secure, I should say that it is the principle of random selection or use of anything pertaining to the system. I do not know how to impress upon you the importance of this
principle. One of the factors which most often led to a first break into the
German systems, was the methodicalness of the German mind. The typical German
mind is so fascinated with the idea of doing everything systematically and in
accordance with a set form that everything he does must be done according to system, then
when he has once adopted a system he never departs from it unless it is specifically
called to his attention. It was his slavish adherence to set forms that most often
gave the leading clues. And if he was told that he must vary his procedure, he
varied it according to a system.

I must confess, however, that our own forces were not a great deal better
in this respect than the German. Time and again we called attention to the flagrant
violations of the rules by men in this regiment or that regiment. But the seriousness
of the violations, I am sorry to say, was little appreciated by the superior officers
of the men who were guilty. You know how difficult it is to get action on things
like this through the usual channels. The men in action think that there are a lot of
old fogies back at headquarters, who have nothing to do but amuse themselves getting
up a lot of "fool rules and regulations" with which to pester them. They say to
themselves "How the devil can the enemy get anything out of a code message that is
nothing but a jumble of letters? If this thing were not safe they would not give it
to us". It may be that it is psychologically impossible to make most men realize the
seriousness of the hundred and one minute precautions that must be observed, except
by actually letting them see how solutions are achieved from the most slender of
threads and far fetched clues.

For example, in almost every code for secret communication, alternates or
variants for the most frequently used groups are given. I cannot tell you how
difficult it is to get operators to use these variants and use them at random.
A systematic selection of those variants would be dangerous. For example, at first
the German operators had the idea that if a word, or a spelling group, or a
punctuation sign occurred several times in a message, the variants were to be used
in succession, the first one the first time it was used, the second the second time,
etc. Or if the group was only used once in a message, the first variant was to be
used. Such a procedure as the latter does not accomplish the purpose for which the
variants are intended. (Case 11)

Another source of danger is the repeated use of the same expression, whether
it be in the beginning, middle, or end of message. I wonder how many of you realize
the danger involved in such important parts of a message as the address and signature. In cipher work especially, these two parts of a message are always the first to be attacked. Now, as often happens, messages contain the same addresses and signatures many times, solution is particularly easy in certain forms of ciphers. For example, one of the safest ciphers I know can be solved if one has two \textit{exact} short messages in the same key, in which the signature is the same. And recently we solved another cipher, which was heralded even by other experts as being absolutely indescribable by taking advantage of the fact that the addresses of the messages were in cipher too, even though they were all different. It is not so much the fact that addresses or signatures are dangerous as the fact that the beginnings and ends of messages are always weak points. It is just as dangerous, if not more so, to have a more or less set form of beginning messages, such as "Acknowledging your message number so and so" or "Referring to your message number sp and so". The only guiding point in such matters can be: avoid all \textit{stereotyped} expressions and adhere to no regular forms in doing anything in cryptographic work.

The use of punctuation in a code or cipher message, except where the sense would be ambiguous without it, should be avoided. I should say that one of the greatest sources of clues in our work on the German Trench Codes lay in the excessive use of all forms of punctuation by the German operators.

There is one more caution that I might mention. Never give the enemy a chance to make any deductions with respect to the contents of any messages if it can possibly be avoided. Let us suppose for example that the units of a squadron are in maneuvers. A short message followed by a certain maneuver would enable a vigilant enemy to make certain deductions as to the contents of the message which dictated the movement. Similarly a message sent from A to B, followed by a short message from B to A, followed by a repitition of the first message by A would certainly indicate a request for repetition on the part of B. Or a long message sent by A, then a short message from B followed by a repetition of the first message from say the thirtieth group would certainly indicate a statement from B to A to the effect that the message was intelligible from the thirtieth group on. All such clues must be suppressed.

I have referred once before to the dangers of short messages. A short message from A to B followed by a longer message from B to A, say within ten or fifteen minutes, would indicate that possibly "question and answer" had been exchanged between the two stations. By watching these short messages the initial groups are apt to be easily solved.
because questions most often begin with interrogatives such as "When" "Where" "How" or verbs such as "Is" "Are" "Have" etc.

Those responsible for the use of code books should regard it as part of their duties to send in to headquarters from time to time a list of words or phrases which are not present in the code and which are used sufficiently to warrant their being incorporated. In this connection I may tell you of the most peculiar anomaly of the German trench code. It had no word for code book. Consequently, every reference to it had to be spelled out. Now it was the regular practice to notify the stations, after a new code book went into effect, to return the old codes. Consequently, in the traffic the first day of the life of a new code one or more messages could always be found instructing the stations to send back the old code books. Since the word Code Book had to be spelled out, the finding and solving of such a message at once enabled us to make a great hole into every new code. If I were asked what word in all the German messages gave the most useful clues to solution, I should say it was this word "Satzbuch". This went on for over two years—all for the lack of a man with sufficient initiative and regard for his duty to inform the proper authorities. (Case 12)

I have told you about some of the things which helped us in our work on the German codes and ciphers used on the battle front, and have hinted at successes. Of our failures, I have told you nothing—and they were many. I am of the opinion and have good reason to suspect, that toward the end of the war the German intelligence department gave special courses of instruction in the use of code and cipher to the operators in charge of transmitting communications. The reason I suspect this is that as time went on the material became increasingly difficult to solve in spite of our continued experience with the material. The enemy evidently came to a realization of the importance of the correct use of their codes and ciphers and the result was that a most rigid discipline in communications came to be enforced. They even had inspectors whose duty it was to go from station to station and correct the errors being committed. One amusing incident in this connection may interest you. (Case 12.)

The idea of having an inspector or a sort of a "Security service" is fundamentally a very excellent one. The security service should be, it seems to me, a branch of the Code and Signal Section, because they are in a better position to realize all the mistakes and pitfalls and the seriousness of violations of the rules and they should also be able to keep a close watch over all the traffic. Such a department might seem superfluous but I believe that in the end it would more than
pay for itself. A poor code in the hands of experts can be used more safely than an excellent code in the hands of careless or ignorant operators. Finally, I might add that no code or cipher system known to me may be said to be "fool proof". Since the secrecy of operations is a fundamental prerequisite to success in warfare, it is hardly necessary to point out that the proper training of the personnel which is to be entrusted with the work of encoding and enciphering, and decoding and deciphering, is one of the most important factors in the realm of military or naval science.
<table>
<thead>
<tr>
<th>MEMO ROUTING SLIP</th>
<th>NEVER USE FOR APPROVALS, CONCURRENCES, OR SIMILAR ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FROM NAME OR TITLE</strong></td>
<td><strong>DATE</strong></td>
</tr>
<tr>
<td>Mr. W. F. Friedman</td>
<td>31 Dec 55</td>
</tr>
<tr>
<td><strong>ORGANIZATION AND LOCATION</strong></td>
<td><strong>TELEPHONE</strong></td>
</tr>
<tr>
<td>5/ASST</td>
<td>NSA-142</td>
</tr>
<tr>
<td><strong>INITIALS</strong></td>
<td><strong>COORDINATION</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DATE</strong></td>
<td><strong>FILE</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>COORDINATION</strong></td>
<td><strong>NECESSARY ACTION</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FILE</strong></td>
<td><strong>NOTE AND RETURN</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>INFORMATION</strong></td>
<td><strong>SEE ME</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NECESSARY ACTION</strong></td>
<td><strong>SIGNATURE</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**REMARKS**

This is the only edition thus far. However, Dr. Campagne is working on a revision, and he expects to complete it in about two months.

5 August 1955

Is in Dr. Campagne's Office for typing then will have to be reproduced. Approximately 2 to 3 months before dissemination.

k
Did we ever get out another edition of this?  
(This is marked "Preliminary")
Mr. Friedman's Appointments
1954 + 1955
In the Hospital

12 APR 1955

[Handwritten text not legible]
31 MAR 1955
Commander's Conference Cocktail Party

1 APR 1955
11:00 CWG mtg Poy's office
13:00 CWG mtg in Friedman's office
16:00 Mr. McPherson

4 APR 1955
In the Hospital

5 APR 1955
In the Hospital

6 APR 1955
In the Hospital

7 APR 1955
In the Hospital

8 APR 1955
In the Hospital

11 APR 1955
In the Hospital
TDY Europe

14 MAR 1955

TDY Europe

15 MAR 1955

TDY Europe

16 MAR 1955

TDY Europe

18 MAR 1955

TDY Europe

21 thru 25 March 1955

TYD EUROPE

28 MAR 1955

Return to duty (first day)

2:00 Dr. Wright (Folger Library)

29 MAR 1955

No meetings

30 MAR 1955

10:00 Mr. A.B. Clark
REF ID: A59461

2 MAR 1955
TDY Europe

3 MAR 1955
TDY Europe

4 MAR 1955
TDY Europe

7 MAR 1955
TDY Europe

8 MAR 1955
TDY Europe

9 MAR 1955
TDY Europe

10 MAR 1955
TDY Europe

11 MAR 1955
TDY Europe
17 FEB 1955

10:00 Briefing in Gen Canine office by R/D
10:15 Collect long-distance call from Princeton

Dr. von Neumann, 4 mins. $1.20 plus tax
2:00 Dr. Kullback

18 FEB 1955

TDY Europe

21 FEB 1955

TDY Europe

23 FEB 1955

TDY Europe

24 FEB 1955

TDY Europe

25 FEB 1955

TDY EUROPE

28 FEB 1955

TDY Europe

1 MAR 1955

TDY Europe
9 FEB 1955

10:00 Col Marcy's Office, AHS
3:00 Conf with Mr. Otis Wilson
Long Distance Call to Dr. Tukey (4 Mins.$1.20 plus tax)

10 FEB 1955

Long distance call to Mr. McPherson
2:00 Classification Advisory Panel Mtg

11 FEB 1955

1030 USCIB Mtg.
3:00 Bureau of Standards

14 FEB 1955

1:00 Briefing at AHS for Trip

15 FEB 1955

8:30 Gen's Staff Meeting
9:30 Mr. Corry and Dr. Stukey
3:00 Mr. McPherson, Gen Canine, Mr. Clark

16 FEB 1955

12:45 Mrs. BAGGOSH Gibson, AHS, PERS

1:00 Briefing for trip from PROD
1 FEB 1955

8:30 Gen's Staff Mtg.
2:00 CWG

2 FEB 1955

10:00 CWG
Shots at Disp.
3:30 CWG

3 FEB 1955

10:00 CWG

4 FEB 1955

9:00 CWG
2:00 CWG

7 FEB 1955

10:00 CWG
Lunch with Mr. Friendly at Cosmos Club
3:00 mtg with Dr. Leibler, Mr. Clark, Dr. Tompkins re SCAG

8 FEB 1955

8:30 General's Meeting
10:00 Technical Journal Meeting
21 JAN 1955

Sick Leave

24 JAN 1955

8:30 Dr. Tukey
9:30 Ad Hoc Mtg of CWG
10:30 CWG Mtg

25 JAN 1955

10:30 General's Staff Mtg (AHS)

26 JAN 1955

Lunch with Dr. Tukey at Cosmos Club

27 JAN 1955

AHS all morning
4:00 CWG

28 JAN 1955

8:00 Technical Journal mtg
9:30 CWG

31 JAN 1955

9:30 CWG Mtg, State Dept.
4:00 CWG Mtg, State Dept.
JAN 1955

9:00 Classification Meeting
10:00 Mtg. in Mr. Polyizoides office, State

13 JAN 1955

1330 Personnel Development Board

14 JAN 1955

Dr. Wilks
9:30 Mtg Mr. Polyizoides Office State
2:00 Technical Journal Board

17 JAN 1955

9:30 Mtg Mr. Polyizoides Office - State
2:00 Civilian Promotion Review Board

18 JAN 1955

8:30 Generals Staff Mtg
1:30 Film "Mission"

19 JAN 1955

1:30 Members of SCAMP (introduced to Gen Canine)

20 JAN 1955

1:30 Length of Service Awards
2:15 Ad Hoc Mtg Polyizoides Office State
9 JAN 1955

11:30 Dr. Tukey

4 JAN 1955

10:00 Meeting in Mr. Polyozides Office

5 JAN 1955

10:00 Meeting at Mr. Polyozides Office
2:00 Meeting with Mr. Hartstall
2:30 Meeting with Mrs. Crawford

6 JAN 1955

No Meetings scheduled

7 JAN 1955

1:30 Arlington Hall, Col. Marcy-SCAMP

10 JAN 1955

2:05 Called Dr. Sam Wilks, Princeton University
3 mins, 1 dollar plus tax

11 JAN 1955

8:30 General's Staff Meeting
9:30 Dr. Suits, talk with Capt Holtwick
11:45 Gen Canine's Office plus lunch(Cosmos Club)
2:00 Dental appointment
REF ID: A59461

2-2 DEC 1954
Sick Leave

2 3 DEC 1954
Sick Leave

2 7 DEC 1954
Sick Leave

2 3 DEC 1954
4 hrs sick leave

2 9 DEC 1954
2 hours sick leave

3 0 DEC 1954
2 hours sick leave
1:30 Mr. McPherson

3 1 DEC 1954

19 DEC 1954
3:00 Reynolds and Leibler

10 DEC 1954
Lunch with General Canine, Mr. Crean
2:30 USCTB Meeting (110th mtg)

13 DEC 1954
1:30 - 4:00 General's Promotion Board

14 DEC 1954
8:30 The General's Staff Meeting

15 DEC 1954
4 hours sick leave

16 DEC 1954
11:00 Generals' Office Re: Dr. Pettengill
12:00 Lunch with Colonel Zeller
   (10:00 Capt McDonald attended meeting in Pentagon
    with Mr. Bond)

17 DEC 1954

20 DEC 1954
Sick Leave

21 DEC 1954
Sick Leave

PL 86-36/50 USC 3605
EO 3.3(h)(2)
30 NOV 1954

Attended lecture at AWS - invited by A. B. Clark - at 1330.

1 DEC 1954

Physical Exam

Headache of Armed Forces Communication Association - with Mr. Dougley and Lt. Col. Courtney.

2 DEC 1954

No meetings

3 DEC 1954

3:35 Polyozdes Office - State

6 DEC 1954

2:00 Cryptography Committee Meeting

7 DEC 1954

8:30 Director’s Staff Meeting

9:30 Colonel Jacobs

1:00 Promotion Screening Board (GS 14 and above)

8 DEC 1954

1000 Generals Office

1300 USCIB Briefing in General's Office
15 Nov 1954

2:00 - 4:30 Civilian Promotion Review Board

16 Nov 1954

No meetings

17 Nov 1954

Lunch with "someone"

at Cosmos Club 1240-1440

18 Nov 1954

1300-1435 Personnel Development Board

19 Nov 1954

No meetings

22 Nov 1954

Sick leave (8 hrs)

23 Nov 1954

Lunch off the station with "someone"

24 Nov 1954

No meetings

25 Nov 1954

Holiday

26 Nov 1954

Sick leave (8 hrs)

29 Nov 1954

Lunch with daughter

19 Dec 1954

Meeting (1030) at CIA [incl: Dingley, Parker, Erikson] for "demonstration"
1 NOV 1954

No Meetings

2 NOV 1954

9:00 General's Staff Meeting

3 NOV 1954

1:00 - 4:30 AHS

4 NOV 1954

Lunch with General Canine, Alexandria, Christi

5 NOV 1954

No meetings

8 NOV 1954

No meetings

9 NOV 1954

General's Staff Meeting

10 NOV 1954

9:30 RADAC Meeting

2:00 Briefing - USCIB Mtg

Lunch with Mr. Pineau

12 NOV 1954

Annual Leave
20 OCT 1954
½ day at Justice Department

21 OCT 1954
Lunch with Thelma Pierce, May, and Kay and daughter
2:00 Miss Mary Jo Dunning

22 OCT 1954
Annual Leave

25 OCT 1954
2:00 - 4:30 USGIR Mtg.

26 OCT 1954
No meetings

27 OCT 1954
No meetings

28 OCT 1954
0830-1200 PBA Meeting
2:9 OCT 1954
No meetings
1 thru 8 October
At work

1 1 OCT 1954
Lunch with General Penny

1 2 OCT 1954
9:00 Staff Meeting
1:00 Gen Canine luncheon for Gen Sinclair
3:00 Gen Canine's Office - Al Friendly

1 3 OCT 1954
Meeting all day with Investigating Committee

1 4 OCT 1954
Met with Drs, Shaw, Shinn, Tordilla most of day
Mr. Sidney Smith

1 5 OCT 1954
Justice Department
Lunch with General and Mrs. Penny
USCIB Meeting

1 6 OCT 1954
Justice Department
2:00 - 3:30 CivProBd

1 9 OCT 1954
Justice Department
23 SEP 1954
10:15 Mr Bane

20 SEP 1954
Annual Leave

27 SEP 1954
No meetings

28 SEP 1954
Gens Mtthly Staff Meeting
Meetings at AHS 'til 3:00

29 SEP 1954
Spent most of day with Dr. Tukey and Mr. Weaver

30 SEP 1954
All morning spent at AHS
Dr. Tukey for short conference
Lunch with Dr. Sinkov

4 hours annual leave
10 September 1954
No meetings

13 September 1954
No meetings

14 September 1954
Annual Leave

15 September 1954
Annual Leave

16 September 1954
Annual Leave

17 September 1954
No meetings

20 September 1954
Annual Leave

21 September 1954
Director Meeting 1½ hours

22 September 1954
Gen Ackerman's Office 9:00-10:30
Lunch with Mr. McPherson
EXSAB NSASAB 1:00-3:00
30 August

8:15 Colonel Herrelko

31 August 1954

8:30 Directors Staff Meeting

10:00 Dr. Kullback

10:30 Mr. Hogan, R/D

1 SEP 1954

9:00 Brief - Holtwick - General Canine

10:00 Ad Hoc Committee

4:00 CIA - Briefing SAC

2 SEP 1954

Annual Leave

3 SEP 1954

Annual Leave

7 SEP 1954

Annual Leave

8 SEP 1954

Annual Leave

9 SEP 1954

No meetings
July 8 - August 19

TDY in London with five (5) days annual leave

20 AUG 1954

First day at work

23 AUG 1954

9:30 - 11:30
2:00 - 3:30 Mr. Callimahos

24 AUG 1954

8:00 - 1:30 Arlington Hall (Generals Monthly Meeting)

1:30 - 4:30

25 AUG 1954

8:30 Classification Advisory Panel
10:00 General Canine

26 AUG 1954

PL 88-367/50 USC 3605
EO 3.3(h)(2)

No meetings

27 AUG 1954

Ad Hoc 10:00 - 1:00

Mr. F. Rupp 1:30 - 2:00

Mr. Darby and Miss Church 3:00 - 3:30
28 June
10:30 - 12:00 State Dept.

29 June
10:30 General Monthly Staff Meeting (AHS) Connolly
2 hours Annual Leave

30 June
Annual Leave

1 July
Annual Leave

2 July
9:30 General Staff Connolly
2:30 State

6 July
6:30 General Staff Meeting
10:00 Dr. Pettigrell & Mayor

7 July
No Meetings
17 JUN 1954
10:30 PBA - Conference Room

18 JUN 1954
8:30 PBA - Conf. Room (12:00)

21 JUN 1954
11:00 - 13:00 Ad Hoc mtg of CWG
9:00 CIV. Prom. Bd.

2-2 JUN 1954
8:30-9:00 Staff Conference
10:30 - 1:00 CWG (State)

2-3 JUN 1954
9:30 - 12:00 RADAC MTG
2:30 - 3:30 GEN Poker Match

2-4 JUN 1954
9:00 - 10:00 Mr. with Dr. Littell, Dr. Rogers
10:30 - 12:00

2-5 JUN 1954
10:30 - 12:00 State Dept.
18 JUN 1954

• Prog. Bd. Met. Cons. 10:30
  Cda. Prior. Bld 1:30

9 JUN 1954

9 JUN 1954

• Prog. Bd. Met. Res 10:30

10 JUNE

1000 Add. Med to CG
1045 CG Med Res Poly
2:30 Mr. Flister

11 JUNE 1954

8:30 PBA Mtg.
XXX 1:30 Briefing for USCI

14 JUNE 1954

2:20 USCI Mtg Meeting Cda.

15 JUN 1954

No Meetings.

1.6 JUN 1954

Mr. Christie, General Jorden

9:00 - 9:30

2:30 Mr. Clark's Office (MTG)
26 May
Bilh Tanne

27 May
none

28 May
none

29 - 31 May Vacation

1 June
2:00
Meeting w/ Consultants in GS Office

2 June
Served at Coonoor Club

3 June
none

4/6 June
none

7 Jun 1954
none
1100 CWG - STATE
2:00-4:30 Dr. Stoker office

1 2 MAY 1954
3:00 Mr. Cornett
4:00 Dr. Heble - Command

13 MAY 1954
9:00 Visit w/ Col. Campbell JSE
2:30 6th Group 154th affairs

14 MAY 1954
2:30 USC 13 Meeting (103rd)

17, 18, 19 May Annual Leave

20 May
MA Scientific Advisory Board

21 May
MA Scientific Advisory Board

24 May

25 May
1000 General Staff Meeting
1:45 Dr. Buckle
27 APR 1954

Monthly Doy Meeting at 8:15

28 APR 1954

29 APR 1954

1100 Brig Gen. Johnston (said goodbye)

30 APR 1954

1145 lor Symonds

4 MAY 1954

0930 Col. Pierson (to Gen. Cannon office
1300 Mr. Nathanson (to Gen. Cannon

5 MAY 1954

0930 Mr. Lee Rosen
1300 Rosen - Austin
2030 at Lee Rosen - State

6 MAY 1954

1230 A.G. Friendly - Conner

7 MAY 1954

0830 Pettengill - Willoughby
1200 Working Conv. Col. Room
12 APR 1954

13 APR 1954

10:30 Mr. Bogue

14 APR 1954

2:30 Lunch at Cosmos Club

15 APR 1954

12:00 Tour of the capital hill Club

16 APR 1954

10:00 - 12:00 Meeting

19 APR 1954

2:00 Bel air tennis club. Postponed

6:30 CIA Party at hill Club.

20 APR 1954

09:30 Working committee

1000 - 1700 Scientific Advisory Board

21 APR 1954

0900 - 1700 Scientific Advisory Board

26 APR 1954

11:00 - Mr. Shehovt CMA

24 Mar 1954
25 Mar 1954
26 Mar 1954

Annual Leave

29 Mar 1954
0900 Program & Budget Advisers

30 Mar 1954
Maxwell AFB

31 Mar 1954
Maxwell AFB

6 Apr 1954
Dr. Petty
1 Apr 1954
Dr. Petty called Dr. A. Cairns

1 Apr 1954
Ms. McPherson here

15 Apr 1954
Annual Leave
16 Apr 1954

17 Apr 1954
Lunch with Deott

18 Apr 1954
0900 Program
2.5 MAR 1954

0830 NSA - Project & Budget Advisor
Bldg 19

230 USEC Meeting

15 MAR 1954

200 Civilian Promotion Board

16 MAR 1954

830 Staff Meeting

17 MAR 1954

1000 Captain Sapor
200 Mr. Rupp

18 MAR 1954

1100 Class Adv. Panel

19 MAR 1954

1100 Wacker - Austin

22 MAR 1954

Lunch with Miller & Albert

23 MAR 1954

1000 Ad Hoc Staff

1000
1 MAR 1954

---

8:30 Staff Meeting
10:05 Ad Hoc - Polyphases
10:30 Ad Hoc - Class Spec. (did not attend - too busy)
19:00 Budget Advisory Meeting
4:00 Ad Hoc State

---

4 MAR 1954

---

5 MAR 1954

---

8 MAR 1954

---

9 MAR 1954

---

08:30 Staff Meeting

---

9 MAR 1954

---

09:30 Mr. Horton
10:00 Princeton Dr. Von Neumann

---

10 MAR 1954

---

11 MAR 1954

---

11:00 State - Comb. Working Group
13:00 Ad Hoc Polyphases
17 Feb 1954
1:30 AFSAC Meeting (Pentagon)

18 Feb 1954
8:30 Classification
10:00 Briefing Sec. Comms and depth
2:00 NATOain - W/Capt. Frock

19 Feb 1954
9:00 A. B. Clark - Director of

23 Feb 1954
10:00 AHS Staff Conf.

24 Feb
0930 RADAC Meeting (H.Q.)
20:00 NSS

25 Feb 1954
0830 Class. Asst. Biz. Panel

26 Feb 1954
1230 Army Reserve Club (ARCC)
with MELYSHIDES (W. K.)
Luncheon
Leave 12:30 16:30
1 FEB 1954
NONE

9 FEB 1954
0830 Staff Meeting

10 FEB 1954
1230 Lunch, Brig Siltman, Plyzka
(Manchester)
2:30 Briefing

11 FEB 1954
2:30 Board Meeting

12 FEB 1954
NONE

15 FEB 1954
0200 Classification Board Meeting
1145 AA Albert

16 FEB 1954
0830 Staff Meeting
1000 Ad Hoc
130 NSA Specialtie AHS
28 Jan

9:15 to 11:30. Adm. of Co. U.
       State Mt. Polygarden
12:30. Mr. Becker, Chinese Club

29 Jan

8:30. Class at Federal Conf Rm
       10:00. Capt. Nelson, AHS
       12:00. Dr. Potter
       2:30. Mr. Polygardeen Office

1 Feb

0800. Mrs. Zelenke

2 Feb

0830. Staff Meeting
       11:00. Dr. Waterman (Dr. Ainsworth)
       1520. H.S. Pm. M-H
       (Old Cosmos Club Bldg)

3 Feb

0930. State Dept. Polygarde

4 Feb

None

5 Feb

None
14 JAN
3:00 Frank Lewis

15 JAN
9:00 Ms. Garlow

18 JAN
12:00 At Cafeteria Dr. Clean
200 Civic Promotion Rev Board
Conf. Rm. 1

20 JAN
10:00 Nelson
1:00 Attend to plane
City Counsel Office

21 JAN
12:15 Lunch-Clean, Nelson, Clean

22 JAN
9:15 Gen. Clean re- Peterson
10:30 Gen. Clean re- Peterson

26 JAN
10:30 Monthly Staff Meeting AHS

22 JAN
10:30 R+D Presentation
4 JAN 1954
None

5 JAN 1954
8:30 - Weekly Staff Meeting - Conf. Rm.
10:00 - Operations Analysis Briefing - Capt. Holtwick - Conf. Rm.
1:30 - Meeting w/Dr. Engstrom and DIR in DIR's office.

6 JAN 1954
None

7 JAN 1954
8:45 Miss Dunning
9:15 Miss Fox
11:30 USCIB Meeting - CIA

8 JAN 1954
9:00 Smith (here) is on the Cotter
10:30 State Mr. Palmeides

8:30 Staff Meeting
LONG DISTANCE PHONE CALLS
Placed by Mr. Friedman
(as of 15 February 1954)

<table>
<thead>
<tr>
<th>DATE</th>
<th>TIME</th>
<th>PERSON</th>
<th>COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 FEB</td>
<td>11:05</td>
<td>Col. Robert W. Griepin</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Air CMO &amp; Staff Sch.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maxwell AFB, ALA.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(x 3212) spoke to his acct.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maxwell No. 7341</td>
<td></td>
</tr>
<tr>
<td>3 Mar</td>
<td>12:10</td>
<td>Prof. John von Neumann, Private</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(living in home phone)</td>
<td></td>
</tr>
<tr>
<td>4 Mar</td>
<td>1:25</td>
<td>Prof. John von Neumann</td>
<td>$1.25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Princeton</td>
<td>1.00 + tax</td>
</tr>
<tr>
<td>29 Mar</td>
<td>2:20</td>
<td>Same as 15 Feb</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Col. Robert W. Griepin</td>
<td></td>
</tr>
<tr>
<td>2 Apr</td>
<td>2:45</td>
<td>Caesar S. Cairns</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mr. McPherson here</td>
<td></td>
</tr>
<tr>
<td>16 Apr 1954</td>
<td>9:00</td>
<td>Mr. Stephen Russell</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Laidlaw 2-5826 Tone</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Office Phone 3-1980 Ext 579</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Call made to Plaza $1.10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>16 Apr 57</td>
<td>4:30</td>
<td>ASA Claude Shannon</td>
</tr>
</tbody>
</table>
19 APR 1954

19 Apr. 1000 for Neumann $1.10
Princeton, N.J.
"COLLECT FROM"

19 Apr. 1309 Dr. Baker (diner's expense)
Segarman, N.Y.

27 Apr. 3:30 Mr. Mrs. De Plovan, New York

30 Apr.
Mr. Leo Roche Boston
3 American $7.55 plus 10% tax
EF made collect

8 June
Received one expense call from
Mr. J. Howard (Pbka.)

18 Aug.
Dr. A.S. Wilke 9:30
Princeton University
$1.00 - $1.50 plus tax

21 Sept.
Dr. S.S. Wicke 10:30
Princeton University
6 mins, $1.00 plus tax
10 June
Princeton University
Sam Wilks
SUBJECT: Report on Temporary Duty, ETO

TO: Commanding General
Army Security Agency

1. Pursuant to attached orders (Enclosure 1), I left Arlington Hall Station at 0900 hours on 14 July 1945 and returned to that station at 0900 hours on 14 September 1945. Although the temporary duty was originally scheduled to be of three months' duration, Colonel Cook and I both felt that the work for which SID asked that I be sent to the ETO had been completed at the end of two months and there seemed to be no reason for staying any longer. Attached hereto (Enclosure 2) is a detailed account of my movements and duty on this trip.

2. a. A great deal of useful and important information was accumulated by participation in the work of TICOM. In my opinion the results of the TICOM operation have been extremely fruitful and it will take considerable time to assess and properly evaluate the mass of data gained thereby. It is believed that the innermost secrets of German cryptography and cryptanalysis have been laid bare and we are already in excellent position to give an overall picture of the results the Germans achieved, their successes, and their failures. In a separate paper to be prepared I hope to give a detailed report thereon, but at this moment I think it warranted to state that the British and American achievements in both main fields far surpass those of the Germans.

b. In the cryptographic field the Germans made progress -- but never so rapidly or in so coordinated and integrated manner as to prevent or delay for any considerable length of time the continued reading, by the Allies, of the innermost secrets of German military, naval, air force, or diplomatic high- and low-grade communications. Attempts to improve their cryptographic machinery were nearly always obstructed by jealousies, bickerings, and administrative incompetence on the part of those concerned in the research

Declassified and approved for release by NSA on 06-06-2013 pursuant to E.O. 13526
and development work involved. For example, they started in 1939 to improve on the Enigma machine and by May 1945 had produced but a single complete model; in another case, they started work on an all-mechanical machine, an improvement on the Hagelin, in 1941; by May 1945 only a few machines had been produced and saw very little service. They produced a half-dozen different variations of a teletype encipherment machine, each of which except the very last was solved on a daily basis by the British. The early models of these machines were put into service without any serious attempt to study their security. German efforts to produce secure speech secrecy devices were dismal failures.

c. In the cryptanalytic field, they had but a mere half-dozen first-rate technicians and they failed to make even a dent in the high-grade cryptographic machines of the British or the United States. Their greatest achievements were the solution (up to the end of 1945) of the British Naval Cipher No. 5, British Naval Code, and American Strip Cipher using 30 strips regularly. When the channel interruption system was introduced in the last-mentioned system, they could do nothing further with it. They were completely baffled by our Sigaba traffic; they apparently did not even attempt a serious study of our SIGCOM or SIGTOT traffic, possibly because they were not too successful in intercepting it; they were apparently absolutely oblivious to or unaware of our SIGSALY transmissions. Their cryptanalytic deficiencies may, in part, be attributed to faulty organization and internecine warfare; there were at least half-dozen different, uncoordinated and competing cryptanalytic establishments, each one jealous of its own secrets and unwilling to cooperate except in a sporadic and faltering manner with any one of the other establishments. If there was a high-level coordinating agency, TICOM has failed to uncover it thus far. However, it does appear that the Germans had considerable, if not almost complete success with Russian military and naval cryptography—because it presented in most cases only the most elementary of cryptanalytic and traffic analysis problems.

d. It must also be stated that while the Germans had very little success, judged by our own standards, with British and United States high- and medium-grade material, they did not lack for certain important information gleaned from traffic analysis. The latter success was only possible because of our own shortcomings in radio procedures, practices, and security doctrine. A wide field for improvement in this respect remains for us to explore and to propagandize, with the hope of bringing about changes in attitude on the part of signal operating personnel.
3. My second visit to GC & GB can hardly be said to have been as interesting as my first: V-E Day and the imminence of V-J Day had diminished activities and operations to but a mere shadow of their former stature. An air of the graveyard and tomb hung over each of the "huts" and buildings. Gone was the bustle, hurry, sense of urgency, and hum of wheels turning; every day fewer faces were seen. However, I found the visit interesting nevertheless and was glad of an opportunity to renew acquaintance with many old friends, all of whom endeavored to impress me with their earnest desire to continue our collaboration during the peace and to cement further the cordial relations that existed at the end of the war.

2 Incls:
1. Copy of orders
2. Account of movements & duty on trip

WILLIAM F. FRIEDMAN
Director of
Communications Research
AG 201 Friedman, William F. hak - 2B-939 Pentagon
(10 Jul 45)OB-S-B

11 July 1945.

SUBJECT: Travel Orders, Shipment IJ-Paris-YC.

TO: The Commanding General,
   Air Transport Command;
The Chief of Transportation,
   Army Service Forces.

1. Mr. William F. Friedman, P-8, is hereby directed
to proceed from Arlington, Virginia, to Washington, D. C.,
for further movement by air, on or about 14 July 1945, to
Paris, France, and to such other places within the European
Theater as may be directed by the Commanding General, United
States Army Forces there on temporary duty for a period of
approximately ninety (90) days, and upon completion of this
temporary duty to return to Arlington, Virginia. UST-3-10975-WDP-JUL.

2. Prior to departure from the continental United
States, he will be required to have completed the pre-
scribed immunizations in conformity with current War Depart-
ment instructions.

3. Regulations governing the procurement of military
clothing and equipment in the United States are published
in Section I, Circular 399, WD, 1944. Mr. Friedman is in
Group 6. A uniform is required by the overseas commander.
(Note Tab A, attached.)

4. Just prior to departure for port of aerial embarka-
tion, he will advise correspondents that all mail will be
addressed to him at APO 24441, c/o Postmaster, New York,
New York. Upon arrival at destination overseas, he will
contact the nearest Army Post Office to arrange for receipt
and dispatch of official and personal mail. Civilian per-
sonnel using an APO mailing address are not entitled to the
free mailing privilege.

5. Baggage to accompany the individual will be marked
with the owner's full name, will be limited to sixty-five
(65) pounds, and will accompany the individual to the port
of aerial embarkation. Baggage will not be marked so as to
disclose the overseas destination.
Travel Orders, Shipment JF-Paris-YO. (Cont'd.)

6. Travel by military, naval or commercial aircraft and common carrier is directed as necessary in the military service for the accomplishment of an emergency war mission and is chargeable to 601-3 P 432-02 212/60425 S 99-999.

7. In lieu of subsistence, a flat per diem of $6.00 while within and $7.00 while outside the continental limits of the United States is authorized in accordance with existing law and regulations while traveling and absent from permanent station. No per diem is authorized while traveling on board ships where the cost of passage includes meals.

8. The Chief of Transportation, Army Service Forces, Washington, D. C., will issue Certificate of Identification, WD, AGO For.: No. 65-11 to Mr. Friedman with assimilated rank of Field Grade Officer. Upon the return of Mr. Friedman to the United States, Certificate of Identification will be surrendered to the Commanding General, Port of Entry.

9. Mr. Friedman is designated as official courier for the purpose of transporting official documents. Each package or envelope containing official matter which is to be exempt from examination will be sealed and will bear on its exterior cover the inscription "Official United States Army Communication, Exempt from Censorship", followed by the signature and official title of the authority dispatching the documents, who will furnish the courier with a letter addressed to the Collector, United States Bureau of Customs, Port of Aerial Embarkation, Washington, D. C., so describing the exterior cover or covers of the communications to be exempt from censorship as to enable the Customs Collector to identify them.

10. He is authorized to carry a camera, film and equipment and, subject to the restrictions of the theater commander, to take such photographs as may be necessary for the accomplishment of his mission.

11. In the interest of security there should be no discussion with unauthorized persons of the overseas destination involved herein.

12. The Commanding General, Air Transport Command, and the Chief of Transportation, Army Service Forces, will each furnish the transportation for which he is responsible and coordinate with all concerned.
Travel Orders, Shipment IJ-Paris-YC. (Cont'd.)

13. Mr. Friedman may be contacted thru Captain Robert S. Travis, Military Intelligence Service, War Department, Washington, D. C., telephone REPUBLIC 6700, extension 72468.

By order of the Secretary of War:

/s/ Donald M. Davis
Adjutant General

1 Incl.

TAB A.

COPIES FURNISHED:
CG, ETO (8); CO, PoAE, Wash., D. C. (2);
OPD, WDOS (1); APS, AGO (2); Mr. Friedman, THRU:
   Capt. Travis (10); Capt. Travis, MIS (2);
Ch/Transp., ASF (Maj. Warker) (1).

I certify that this is a true copy:

Thurman R. Hamman
Major, Signal Corps
1945

14 July -- Left Washington Airport at 1130 hours (ATC terminal) by C-54 airplane. Stops at Newfoundland and Azores.


16 July -- Reported in at ETO HQ; 0CSig0; SID HQ. Preliminary conference with Colonels Bieber and Cook.

17 July -- Continued conference with Colonel Bieber and Cook; review of SID current operations and situation; conference with Captain Wilkins, in charge of historical projects, SID.

18 July -- Continued conference with Colonels Bieber and Cook; conference with them and with Lieutenant Colonel Hilles, MIS representative in ETO, in regard to SIGTOT installation at Bletchley Park in British area. Formal call on and luncheon guest of General Rumbough, CSig0 of ETO.

19 July to 25 July, inclusive -- Began one week's motor trip into U. S. Occupation Zone in Germany, with Colonel Bieber and Lieutenant Colonel Allen, on inspection tour of SID installations in Germany, including the following: (a) The Vierling Laboratory (an important TICOM target); (b) SID Advanced HQ (Detachment D), at Rüsselsheim; (c) 116th Signal R. I. Company at Scheyern; (d) 118th Signal R. I. Company at Rosenheim; (e) fixed intercept station at Große Geräu. Visited Berchtesgaden en route.

26 July -- SID HQ in Paris. Continued conference with Captain Wilkins on historical project; conference with Colonels Bieber and Cook on TICOM matters; review of new TICOM documents; discussions with regard to new ETO security document; discussion with regard to box of OKW/Chi documents recovered from Lake Schliersee.

27 July -- En route to London with Colonel Bieber, by ATC; reported SID HQ at Weymouth Street. Review of TICOM situation and matters with Lieutenant Colonel Johnson.
28 July  -- To Bletchley Park with Colonel Bicher; lunch and conference with Commander Travis; formal TICOM meeting in afternoon; tour of TICOM HQ and informal discussions with TICOM representatives.

29 July  -- Visit to OSDIC HQ at Beaconsfield, to listen in on interrogation of an important German P/W (Mettig). Conference with Captain Ginsburg of OSDIC.

30 July to 7 August inclusive -- TICOM HQ; study of TICOM documents and preparation of special questions to be put to P/Ws; discussions with TICOM members on current matters; conferences with Major Seaman, Mr. Lewis, Brigadier Tiltman, Captain Hastings, Paymaster Cmdr. Dudley-Smith, Mr. Hinsley. Tour through Bourbon section with Colonel Pritchard. Conferences with Mr. Ben Shute, chief MIS representative on Combined Historical Project, and with Mr. Birch (CO & CS), Editor in Chief of the Project.

8 August  -- Spent day in London, visiting Berkeley Street. Conference (and lunch) with Captain Hastings and Major Stone (MIS representative at Berkeley Street); conference with Mr. Kendrick, technical head; conference with Lieutenant Colonel Johnson on TICOM matters. Courtesy call on Brigadier General Van Voorst, Assistant U. S. Military Attache.

9 August to 14 August inclusive -- Continued work at Bletchley Park. Study of new TICOM documents; TICOM meetings and discussions; conferences with Major Seaman and Mr. Lewis on Bourbon project; conferences with Mr. Shute and Captain McCown (SSA representative on historical project).

15 August  -- Official V-J Day. Trip to Cambridge with Cmdr. Travis to tour Cavendish Laboratory and visit Professor Vincent.

16 August to 24 August inclusive -- Continued work and conferences as per 9-14 August cited above; conferences with Brigadier Tiltman and Cmdr. Travis; conferences with Mr. C. L. S. Williams on intercept and intercept control for Berkeley Street traffic; conferences with Dudley-Smith on questions arising from TICOM operations.

25 August  -- Second visit to OSDIC HQ to listen in on further interrogations of German P/Ws (Huettenhain, Fricke, et al).
26 August -- In London, second visit to Berkeley Street; continued discussions with Mr. Williams and conferences with Messrs. Catty, Rees, Kendrick.

27 August -- Continued conferences at Berkeley Street; lunch with Captain Hastings; visit to Queens Gate House to tour special Berkeley Street tape-reading operation; conferences with Lieutenant Colonel Johnson on TICOM and SID matters.

28 August --

29 August -- To Frankfurt, by air, via Paris.

30 August to 2 Sept inclusive -- Conferences with Colonel Cook on TICOM matters; second visit to Detachment D (BARN) and to Intercept Station at Grosse Gerau; formal call on and luncheon guest of Major General Lanahan, OSigO, USFET; tour through Signal Corps installations at USFET HQ with General Lanahan; continued conferences with Captain Wilkins on historical project.

3 Sept -- To London with Colonel Cook, by air.

4 Sept -- To Bletchley Park with Colonel Cook for last formal TICOM meeting.

5 Sept to 7 Sept

5 Sept -- Completion of TICOM work; final farewells to GC & OS people, etc.

8 Sept -- Return to London; made arrangements for return to U. S. by air.

9 Sept to 10 Sept inclusive

9 Sept -- Final visits to Berkeley Street; conferences with Captain Hastings, Messrs. Williams, Kendrick, Catty, etc.

11 Sept to 14 Sept inclusive

11 Sept -- Left London for Prestwick, by air; to Iceland; return to Prestwick on account of bad weather; to Azores, thence Bermuda and New York, where arrived at 0300 hours, 14 Sept; then by rail to Washington, arriving at 0830.

14 Sept -- Reported in at SSA, HQ, 0900.
MEMORANDUM FOR: Distribution

SUBJECT: SCAG Conference

Enclosures: (A) Draft agenda
           (B) Notes to accompany draft agenda

1. The enclosures are forwarded for telephonic concurrence and/or comments (Ext. 60240).

2. It is proposed to distribute copies of the agenda to SCAG members at the opening session. Enclosure (B) is intended only for AFSA personnel.

Distribution:

Adm. Stone - 1 copy
Col. Collins - 1 copy
Capt. Wenger - 1 copy
Col. Hetherington - 1 copy
Capt. Holtwick - 4 copies
Capt. Harper - 4 copies

This letter may be reduced to CONFIDENTIAL when enclosures are removed.

APPENDED DOCUMENT CONTAINS CODE WORD MATERIAL

Declassified and approved for release by NSA on 09-23-2014 pursuant to E.O. 13526
SPECIAL CRYPTOLOGIC ADVISORY GROUP
(SCAG)

Agenda
for
First Conference of SCAG
4-5 June 1951
SPECIAL CRYPTOLOGIC ADVISORY GROUP (SCAG)

Agenda for
First Conference of SCAG
4-5 June 1951

OPENING SESSION
Morning of 4 June 1951

Time: 10:00 A.M.
Place: Office of the Director, Armed Forces Security Agency, Room 118, Building 19, Naval Security Station, 3801 Nebraska Avenue, North West, Washington.

10:00 1. Address of welcome:
   Dr. William Webster, Chairman, Research and Development Board (RDB)

10:05 2. a. Presentation regarding the Armed Forces Security Agency (AFSA):
   Organization of AFSA; position in Department of Defense and Armed Forces; relationships with other U.S. agencies and bodies such as the United States Communications Intelligence Board (USCIB), and the Armed Forces Security Agency Council (AFSAC).
   Rear Admiral Earl E. Stone, USN, Director, AFSA
   b. Question and discussion period.

10:30 3. a. Presentation regarding the use and value of communications intelligence (COMINT) in national defense:
   Capt. J.N. Wenger, USN, Deputy Director, AFSA
   b. Question and discussion period.

11:00 4. a. Presentation on procedural matters in connection with the functioning of SCAG as an agency of RDB and a consultative body of AFSA:
   Mr. Edwin A. Speakman, Executive Director, Committee on Electronics, RDB
   b. Question and discussion period.

11:30 5. Outline of program for technical sessions:
   Mr. William F. Friedman, Technical Consultant, AFSA

11:35 6. Indoctrination of SCAG members not already indoctrinated:
   Capt. J.N. Wenger, USN, Deputy Director, AFSA

12:00 Luncheon: Conference Room, adjoining Admiral Stone's Office, Room 19-125.

ARMED FORCES SECURITY AGENCY

TOP SECRET AGORN

Encl. "A"
TECHNICAL SESSIONS

Commencing after lunch on 4 June 1951

Time: 1:00 P.M.

Place: Room 202, Building 20, Naval Security Station

1. a. Presentation to illustrate how a complex COINT problem was success-
fully handled in World War II:

LCDR Andrew M. Gleason, USNR

I. The cryptographers' point of view

A. Requirements
B. Codes and ciphers
C. Mechanics of a cipher system

II. Single-letter substitution ciphers

A. General description
B. Machine systems
C. Pad systems; additives

III. Wired-wheel machines and the German Enigma

A. General description
B. The commercial Enigma
C. The steckered Enigma
D. The Bombe
E. Duenna

2:00 b. Question and discussion period.

3:00 2. a. Tour of special cryptanalytic machines at the Naval Security Station:

Dr. H. Campagna and Dr. J.J. Euchau

I. Atlas

Presentation regarding AFSA’s position and program in the
field of electronic computers

II. Demon I and Demon II

III. Goldberg

IV. World War II Bombe for Enigma solution

4:00 b. Question and discussion period.
TECHNICAL SESSIONS, Cont'd

Morning of 5 June 1951

Time: 9:00 A.M.
Place: Room 202, Building 20, Naval Security Station

PRESENTATIONS REGARDING A CURRENT HIGH-PRIORITY AFSA PROBLEM

1. a. Introduction to Albatross
   I. Background of the Albatross problem
   II. What is known about the machine
   III. Present indicator system
   IV. The Round Robin machine

To be presented by Mr. F.A. Raven and Mr. D.H. Shepard

10:00
b. Question and discussion period.

11:00
2. Isomorphism and wheel recovery
   I. Discussion of isomorphism
   II. A sample problem in wheel recovery

To be presented by Mr. A.N. Levenson and Mr. E.D. Marston

12:00 Luncheon: Executive dining room, Naval Security Station Cafeteria
This sheet of paper and all of its contents must be safeguarded with the greatest care. Utmost secrecy is necessary to prevent drying up this sort of vital intelligence at its source.

Afternoon of 5 June 1951

Time: 1:30 P.M.
Assembly point: Room 1082, Building "A", Arlington Hall Station, 4000 Lee Boulevard, Arlington, Virginia. (Transportation from Naval Security Station to Arlington Hall Station will be provided for SCAG members)

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:30</td>
<td>1. Tour of AFSA machines, to be conducted by Mr. Frank D. Rowlett, assisted by Dr. A.E. Highley and Mr. William J. Lawless.</td>
</tr>
<tr>
<td></td>
<td>I. The IBM installation</td>
</tr>
<tr>
<td></td>
<td>II. RAE equipment</td>
</tr>
<tr>
<td></td>
<td>A. Abner</td>
</tr>
<tr>
<td></td>
<td>B. Robin</td>
</tr>
<tr>
<td></td>
<td>C. ASAF-1</td>
</tr>
<tr>
<td>2:30</td>
<td>2. a. Discussion period on isomorphism and wheel recovery.</td>
</tr>
<tr>
<td></td>
<td>To be held in Room 2010, Building &quot;B&quot;, AHS</td>
</tr>
<tr>
<td></td>
<td>b. Coffee will be served during this period.</td>
</tr>
<tr>
<td>3:30</td>
<td>3. a. Presentation regarding AFSA project S EAT.R: Matrix projection</td>
</tr>
<tr>
<td></td>
<td>(Room 2032, Bldg. &quot;B&quot;)</td>
</tr>
<tr>
<td></td>
<td>Mr. Albert E. Roberts</td>
</tr>
<tr>
<td></td>
<td>This presentation is of interest primarily to those members of SCAG who are specialists in the field of mathematics.</td>
</tr>
<tr>
<td></td>
<td>b. Presentation regarding electronic representation of rotors (Room 2010, Bldg. &quot;B&quot;)</td>
</tr>
<tr>
<td></td>
<td>Dr. Eachus, assisted by Mr. Ray L. Bowman and Mr. Roger Moulton</td>
</tr>
<tr>
<td></td>
<td>This presentation is of interest primarily to those members of SCAG who are specialists in the field of electronics and electrical engineering.</td>
</tr>
<tr>
<td>4:30</td>
<td>4. Final discussion.</td>
</tr>
<tr>
<td></td>
<td>To be held in Army Security Agency Conference Room (Room 117), Headquarters Building, Arlington Hall Station.</td>
</tr>
<tr>
<td>5.</td>
<td>Closing remarks.</td>
</tr>
</tbody>
</table>

Rear Admiral Earl E. Stone, USN, Director, AFSA

ARMED FORCES SECURITY AGENCY

TOP SECRET AGORN
REF ID:A66052

TOP SECRET

OPENING SESSION
Morning of 4 June 1951

Time: 10:00 A.M.
Place: Office of the Director, Armed Forces Security Agency, Room 118, Building 19, Naval Security Station, 3801 Nebraska Avenue, North West, Washington

Time
10:00 1. Indoc trination of SCAG members not already indoctrinated:

Capt. J.N. Wenger, USN, Deputy Director, AFSA

10:15 2. a. Presentation regarding the Armed Forces Security Agency (AFSA):

Organization of AFSA; position in Department of Defense and Armed Forces; relationships with other U.S. agencies and bodies such as the United States Communications Intelligence Board (USCIB), and the Armed Forces Security Agency Council (AFSC)

Mission for SCAG:

Rear Admiral Earl E. Stone, USN, Director, AFSA

b. Question and discussion period.

10:40 3. Remarks on behalf of Lieut. General Walter B. Smith, USA, Director of Central Intelligence:

Mr. Kingman Douglass, Assistant Director, CIA

10:45 4. Address of welcome:

Mr. William Webster, Chairman, Research and Development Board (RDB)

10:50 5. a. Presentation regarding the use and value of communications intelligence (COMINT) in national defense:

Capt. J.N. Wenger, USN, Deputy Director, AFSA

b. Question and discussion period.

11:20 6. a. Presentation on procedural matters in connection with the functioning of SCAG as an agency of RDB and a consultative body of AFSA:

Mr. Edwin A Speakman, Executive Director, Committee on Electronics, RDB

b. Question and discussion period.

11:50 7. Outline of program for technical sessions

Mr. William F. Friedman, Technical Consultant, AFSA

12:00 Luncheon for SCAG members; Director's Office, Room 19-118.
TECHNICAL SESSIONS

Commencing after lunch on 4 June 1951

Time: 1:00 P.M.

Place: Room 202, Building 20, Naval Security Station

1. a. Presentation to illustrate how a complex COMINT problem was successfully handled in World War II:

LCDR Andrew M. Gleason, USNR

b. Question and discussion period.

2:00

2 a. Tour of special cryptanalytic machines at the Naval Security Station:

Dr. H. Campagne and Dr. J.J. Eachus

I. Atlas

Presentation regarding AFSA's position and program in the field of electronic computers

II. Demon I and Demon II

III. Goldberg

IV. World War II Bombe

3:00

b. Question and discussion period.

4:00
TECHNICAL SESSIONS, Cont'd

Morning of 5 June 1951

Time:  9:00 A.M.

Place: Room 202, Building 20, Naval Security Station

PRESENTATIONS REGARDING A CURRENT HIGH-PRIORITY AFSA PROBLEM

Time
9:00  1. a. Introduction to Albatross

To be presented by Mr. F.A. Raven and Mr. D.H. Shepard

10:00  b. Question and discussion period.

11:00  2. Isomorphism and wheel recovery

To be presented by Mr. A.N. Levenson and Mr. R.D. Marston

Luncheon for SCAG members and AFSA conference: Executive dining room, Naval Security Station Cafeteria.
Time: 1:30 P.M.

Assembly point: Room 1082, Building "A", Arlington Hall Station, 4000 Lee Boulevard, Arlington, Virginia. (Transportation from Naval Security Station to Arlington Hall Station will be provided for SCAG members)

Time
1:30 1. a. Tour of AFSA machines, to be conducted by Mr. Frank B. Rowlett, assisted by Dr. A. E. Highley and Mr. William J. Lawless.

   I. The IBM installation
   II. RAM equipment

   b. Tour of AFSA machines under development, to be conducted by Dr. Eachus, assisted by Mr. G. J. Schierlmann.

2:30 2. a. Discussion period on isomorphism and wheel recovery.

   To be held in Room 2010, Building "B", ABS.

   b. Coffee will be served during this period.

3:30 3. a. Presentation regarding AFSA project SWEATER: (Room 2032, Bldg. "B")

   Mr. Albert E. Roberts

   This presentation is of interest primarily to those members of SCAG who are specialists in the field of mathematics.

   b. Presentation regarding electronic representation of rotors (Room 2010, Bldg. "B")

   Dr. Eachus, assisted by Mr. Ray L. Bowman, Mr. Roger Moulton, Mr. Robert E. Gordon and Mr. Arthur Moulton.

   This presentation is of interest primarily to those members of SCAG who are specialists in the field of electronics and electrical engineering.

4:30 4. Final discussion.

   To be held in Army Security Agency Conference Room (Room 117), Headquarters Building, Arlington Hall Station.

5. Closing remarks.

   Rear Admiral Earl E. Stone, USN, Director, AFSA
TOP SECRET

NOTES

(for AFSA personnel)

TO ACCOMPANY AGENDA FOR FIRST SCAG CONFERENCE
Notes (for AFSA personnel) to accompany Agenda for First SCAG Conference
4-5 June 1951

1. a. Arrangements have been made to issue "Conference Badges" to all SCAG members (except in the case of Dr. Engstrom, who already has a "White A" Badge).

b. The badges will be available by 0630 hours on 4 June, and will be picked up by Captain Mary C. Lane, who will deliver them as follows:

<table>
<thead>
<tr>
<th>Badge for:</th>
<th>To be delivered to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. William Webster</td>
<td>Capt. Hazard</td>
</tr>
<tr>
<td>Mr. Edwin A. Speakman</td>
<td>Capt. Hazard</td>
</tr>
<tr>
<td>Dr. John von Neuman</td>
<td>LCDR Gleason</td>
</tr>
<tr>
<td>Dr. Stewart S. Cairns</td>
<td>LCDR Hall</td>
</tr>
<tr>
<td>Dr. Charles B. Tompkins</td>
<td>LCDR Hall</td>
</tr>
<tr>
<td>Dr. R.K. Potter</td>
<td>Dr. Kullback</td>
</tr>
<tr>
<td>Dr. Claude E. Shannon</td>
<td>Dr. Campaiguo</td>
</tr>
<tr>
<td>Mr. John Howard</td>
<td>Dr. Eachus</td>
</tr>
<tr>
<td>Mr. Joseph Deach</td>
<td>Dr. Eachus</td>
</tr>
<tr>
<td>Mr. John C. McPherson</td>
<td>Dr. Eachus</td>
</tr>
</tbody>
</table>

2. a. The indicated AFSA personnel will act as "guides" for the following SCAG members:

<table>
<thead>
<tr>
<th>SCAG member</th>
<th>&quot;Guide&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. von Neuman</td>
<td>LCDR Gleason</td>
</tr>
<tr>
<td>Dr. Cairns</td>
<td>LCDR Hall</td>
</tr>
<tr>
<td>Dr. Potter</td>
<td>Dr. Kullback</td>
</tr>
<tr>
<td>Dr. Shannon</td>
<td>Dr. Campaiguo</td>
</tr>
<tr>
<td>Mr. Deach</td>
<td>Dr. Eachus</td>
</tr>
<tr>
<td>Mr. McPherson</td>
<td>Dr. Eachus</td>
</tr>
</tbody>
</table>

b. It is assumed that the other members of SCAG (Dr. Tompkins, Dr. Engstrom, and Mr. Howard) are sufficiently acquainted with AFSA and Washington as to make it unnecessary to assign specific "guides" for them; however, AFSA personnel should make every effort to assist those members whenever appropriate.
3. a. In addition to SCAG members, only the following will be present at the opening session of the Conference at 1000 hours, 4 June, in the office of DIRAFSA, Bldg. 19, NSS (See page 1 of Agenda):

Adm. Stone
Mr. Webster
Mr. Speakman
Mr. Douglass
Capt. Wenger
Col. Hetherington
Capt. Harper
Capt. Holtwick
Mr. Friedman

b. Luncheon for SCAG members, Mr. Speakman, Mr. Douglass, DIRAFSA, the Deputies and Mr. Friedman will be served in the Director's Office after 1200 hours.

4. a. In addition to the SCAG members, the following will be present at the first technical session, 1300 hours, 4 June, in Room 20-202, NSS (See page 2 of Agenda):

<table>
<thead>
<tr>
<th>AFSA-02:</th>
<th>AFSA-03:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capt. Holtwick</td>
<td>Capt. Harper</td>
</tr>
<tr>
<td>Mr. Rowlett</td>
<td>Dr. Kullback</td>
</tr>
<tr>
<td>Mr. Raven</td>
<td>Dr. Campagne</td>
</tr>
<tr>
<td>Mr. Shepard</td>
<td>Dr. Eschus</td>
</tr>
<tr>
<td>Mr. Levenson</td>
<td>LCDR Gleason</td>
</tr>
<tr>
<td>Mr. Harston</td>
<td>LCDR Hall</td>
</tr>
</tbody>
</table>

Mr. Speakman, RDB
Mr. Friedman, AFSA-OCT

b. Coffee will be served at about 1500 hours.

c. At the close of this session AFSA participants will endeavor to see that SCAG members have transportation to their hotels.
5. a. In addition to the SCAG members, the following personnel will be present at the morning session, 5 June, in Room 20-202, NSS (See page 3 of Agenda):

<table>
<thead>
<tr>
<th>AFSA-02</th>
<th>AFSA-03</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capt. Holtwick</td>
<td>Capt. Harper</td>
</tr>
<tr>
<td>Mr. Rowlett</td>
<td>Dr. Kullback</td>
</tr>
<tr>
<td>Mr. Raven</td>
<td>Dr. Campaigne</td>
</tr>
<tr>
<td>Mr. Shepard</td>
<td>Dr. Eachus</td>
</tr>
<tr>
<td>Mr. Levenson</td>
<td>LCDR Gleason</td>
</tr>
<tr>
<td>Mr. Neaton</td>
<td>LCDR Hall</td>
</tr>
<tr>
<td>Capt. Dennis</td>
<td></td>
</tr>
<tr>
<td>Mr. Highley</td>
<td></td>
</tr>
<tr>
<td>Mr. Lawless</td>
<td></td>
</tr>
<tr>
<td>Mr. Kirby</td>
<td></td>
</tr>
<tr>
<td>Mr. Reimers</td>
<td></td>
</tr>
<tr>
<td>Mr. Schmitt</td>
<td></td>
</tr>
<tr>
<td>Mr. Shinn</td>
<td></td>
</tr>
<tr>
<td>Mr. Hesse</td>
<td></td>
</tr>
<tr>
<td>Mr. Speakman, RDB</td>
<td></td>
</tr>
<tr>
<td>Mr. Friedman, AFSA-00T</td>
<td></td>
</tr>
</tbody>
</table>

b. Coffee will be served at about 1030 hours.

c. A special luncheon costing about $1.00 will be served in the Executive Dining Room, Naval Security Station Cafeteria. In view of the limited facilities, only the following can be readily accommodated:

<table>
<thead>
<tr>
<th>SCAG members</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mr. Speakman</td>
<td></td>
</tr>
<tr>
<td>Col. Collins</td>
<td></td>
</tr>
<tr>
<td>Capt. Wenger</td>
<td></td>
</tr>
<tr>
<td>Col. Hetherington</td>
<td></td>
</tr>
<tr>
<td>Capt. L.S. Howarth, Op-202</td>
<td></td>
</tr>
<tr>
<td>Capt. W.H. Gullett, CO, NSS</td>
<td></td>
</tr>
<tr>
<td>Capt. Harper</td>
<td></td>
</tr>
<tr>
<td>Capt. Holtwick</td>
<td></td>
</tr>
<tr>
<td>Capt. Dennis</td>
<td></td>
</tr>
<tr>
<td>Mr. Rowlett</td>
<td></td>
</tr>
<tr>
<td>Dr. Kullback</td>
<td></td>
</tr>
<tr>
<td>Dr. Campaigne</td>
<td></td>
</tr>
<tr>
<td>Dr. Eachus</td>
<td></td>
</tr>
<tr>
<td>LCDR Gleason</td>
<td></td>
</tr>
<tr>
<td>LCDR Hall</td>
<td></td>
</tr>
<tr>
<td>Mr. Friedman</td>
<td></td>
</tr>
</tbody>
</table>

(Total: 25)
d. AFSA personnel will endeavor to insure that SCAG members requiring transportation from NSS to AHS for the afternoon technical session at AHS will be provided therewith. This should be taken care of before or during the luncheon period.

6. In addition to the SCAG members, the following personnel will participate in the tour of machine installations at AHS (See para. 1, page 4 of Agenda). (The assembly point will be Room 1082, Building "A", at 1330 hours):

AFSA-02
Mr. Rowlett
Mr. Highley
Mr. Lawless

AFSA-03
Capt. Harper
Dr. Kullback
Dr. Campana
Dr. Sackus
LCDR Glasson
LCDR Hall
Mr. Schieffmann

Mr. Speakman, RB
Mr. Friedman, AFSA-03

7. a. The personnel to be present at the discussion period indicated to follow the tour (see para. 2, page 4 of Agenda), beginning at 1430 hours, in Room 2010, Building "B", AHS, will be the same as in attendance at the session indicated in Paragraph 5, a. above.

b. Coffee will be served during this period.

8. a. For the presentation regarding AFSA project S"EATER (see para. 3 a., page 4 of Agenda), at 1530 hours in Room 2032, Bldg. "B", the following will be present:

SCAG members:
Dr. von Neumann
Dr. Cairne
Dr. Shannon
Dr. Engstrom
Dr. Tompkins
AFSA personnel:
AFSA-02:
Mr. Levenson
Mr. Shepard
Mr. Schmitt
Mr. Albert E. Roberts

AFSA-03:
Dr. Kullback
Dr. Campagne
LCDR Gleason
LCDR Hall

Mr. Speakman, RDB
Mr. Friedman, AFSA-00T

b. For the presentation regarding electronic representation of rotors (see para. 3.b., page 4 of Agenda), also scheduled for 1530 hours in Room 2010, Bldg. "B", the following will be present:

SCAG members:
Dr. Potter
Mr. Desch
Mr. McPherson

AFSA personnel:
AFSA-02:
Mr. Highley
Mr. Lawless
Mr. Murton

AFSA-03:
Capt. Harper
Dr. Bachus
Mr. Rosen
Mr. Dumey
Mr. R.E. Gordon
Mr. R. Moulton
Mr. Bowman
Mr. A. Moulton

9. In addition to all SCAG members, the following persons will attend the final session at 1630 hours, 5 June 1951, in the ASA Conference Room, Hq Bldg., ANS (see paras. 4 and 5, page 4 of Agenda):

Adm. Stone
Mr. Speakman
Capt. Holtwick
Mr. Rowlett
Capt. Harper
Dr. Kullback
Dr. Campagne
Mr. Friedman

10. Record of proceedings will be kept by Dr. Campagne, assisted by LCDRs Gleason and Hall.
THE INFLUENCE OF C-POWER* ON HISTORY.

LECTURE NO. 3

MAKING THE MOST OF A CRYPTOLOGIC OPPORTUNITY.

[PART I - INTRODUCTION]

Introduction to the Walter Cronkhite Television Story Entitled

"The Secret Message that Plunged America into War!" —

one of the episodes of his "You Are There" Program

Columbia Broadcasting System

presented over the TV network

on

23 October 1955, rebroadcast 1 August 1957.

I imagine that for many of those present this means the name Alfred

Zimmermann, German Minister of Foreign Affairs in Berlin in the years 1914-1917.

These days, he is not one that arouses much interest; in fact, I doubt that the name means anything to most of you. Yet, this gentleman, of whom I find it difficult to say "may his soul rest in peace", was the diplomat whose short and unimaginative conduct of German foreign affairs in the three critical years I've mentioned above paved the way for the United States of America to enter World War I as an active belligerent on the side of the Allies and, in sight of the United States could easily have been thrown on the other side—during the critical months of the year 1916—had the Germans been more astute. The consequences of such an event can hardly be imagined, it would be an understatement to say that history would have been changed in a spectacular manner.

*"C-power" = Cryptologic power.
What did Herr Zimmermann do or fail to do to merit so strong a statement
as the one I've just made? What he did was to send a telegram on 16 January 1917
to the German Ambassador in Washington—a telegram which was in German
simplified code and which was intercepted and solved by the British cryptanalytic unit in
London. What he failed to do was to see to it that the cryptosystem that had to
be used to encrypt his message was technically sound enough to protect its
contents. He did and failed to do something else in connection with his now
famous message—but of that, more later.

In order to prepare a proper background for the Zimmermann Telegram of
16 January 1917—that's what it's called in history—I should give you a brief
picture of the situation from the outbreak of the war, on 1 August 1914, up to about the time
to which the telegram was sent. The picture I'm going to depict is a condensa-
tion of the excellent story set forth on pages 22 and 23 of Admiral Sir

By 1914 England had become so dependent on sea-borne imports that her people
couldn't live, let alone wage war, for more than four or five weeks after her
sea-routes were broken. Keeping these routes open was therefore the principal
task of the British Navy. On the other hand, her principal enemy, Germany, was
not dependent on sea-borne imports, so that the British Navy's historic function of arresting an enemy's sea-borne trade lapsed after German shipping had found refuge in neutral ports.

There were then the British Grand Fleet and her hardly much inferior protagonist, the German High Seas Fleet, glaring at each other at a distance, and, although the Grand Fleet was becoming impatient and spoiling for a fight, the Germans didn't dare risk their fleet in major battle, confining their attacks to sporadic forays by fast units and to minelaying.

German hopes of quick victory were shattered when trench warfare in France brought things to a stalemate, and with the passing of each month it became clear that there could be no victory unless British overseas trade was cut off. Some high-laden in the government then had what appeared to be a good idea. These people thought that the success of the German small sub flotilla of 1914 pointed the way out without risking the High Seas fleets, and the government was to give highest priority to building submarines and use them to destroy British and all other shipping to shatter the British Isles.

The home war sea was not safe because merchant ship be sunk without warning, and before the crew could take to life
boats. Observation of these rules had hitherto been required by both belligerents but for Germany this severely reduced the destructive power of their submarines and from time to time their commanders were ordered to ignore them, in some almost without saying, the case of the British merchantmen. But there were bound to be mistakes and, the power of the German unrestricted submarine warfare, as to ships of neutrals were sunk, this brought a wave of resentment against the German Government, there were acrimonious notes to that government, especially from the German Government, when ships were sunk and specious excuses were given for Germany decided that unrestricted submarine warfare in the form of universal conduction of such sinkings. American antagonism was heightened by the discovery of plots and sabotage activities of German agents in America.

Even though unrestricted, The powerful German submarine offensive in 1916 soon began to take a dreadful turn for the British. With the daily toll of shipping losses was so heavy that it began to be obvious that unless some new tide set in -- or unless the United States of America could be drawn into the war on the Allied side -- there could be only one end to it, and that end would come soon.

Britain's problem then was two-fold: (1) To labor prodigiously to gain mastery over the German submarines; but this, it was recognized, would be a slow, a very slow, process; (2) to try not to irritate or antagonize the United States, and certainly not to exasperate America as the Germans were. The hope that the latter would
"Were serious doubts being cast in America on the genuineness of
the instructions to the German Minister in Mexico the authorities here might
reconsider their position, but as Zimmermann has admitted their genuineness
in the Reichstag this can hardly be the case."

That is what Hall greatly feared would happen--but his fears turned out
to be groundless.
sooner or later, the sooner the better, good Americans into joining the war against Germany. The British were fortunate in both respects. It turned out that thanks to the tremendous exertions of British shipbuilders, scientists, and sailors, mastery over the submarines was attained, but not until early in 1918. With this phase of the British problem as I've just stated it, we shall not concern ourselves today. It is with the other phase of it that my talk will deal.

Let's see how the Germans behaved so as to outrage practically all Americans, and make President Wilson ask Congress to declare war on Germany.

During the first year of submarine warfare the German Government respected the rights of neutral nations but when faced with the prospect of losing the war Germany felt forced to
take drastic action.

1 February 1917, it announced that as of that date German submarines would sink at sight ALL ships met on the high seas; in short, proclaimed that unrestricted submarine warfare was being resumed. And it was without all importation to the British Isles were cut off, a fateful decision.

What did President Wilson do on receipt of the German proclamation? Why, after two days later,
on 3 February he informed German Ambassador von Bernstorff that his career in the United States was at an end; diplomatic relations with Germany. Von Bernstorff wasn't given much time to pack his belongings and go home. And Ambassador Gerard was ordered home. But note that severing diplomatic relations doesn't mean war — and it didn't in this case.
PLEASE NOTE!!!

Advance Registrations MUST BE RECEIVED IN SECRETARY'S OFFICE PRIOR TO SEPTEMBER 30TH. THEREAFTER THEY WILL BE RECEIVED BY

RICHARD D. HIGGINS
Archivist of the Commonwealth of Massachusetts
Chairman Local Arrangements Committee, SAA
State House, Boston 33, Massachusetts
It was only natural for Britain to hope that we would now join the war against Germany. The American position was quite humiliating because it was clear we were unable to provide protection that was something to be proud of. But another thing he had promised to keep was to keep American merchantmen sailing on the high seas out of the war. Hence, after the German declaration of unrestricted submarine warfare, American ships kept within American harbors because they were afraid to leave and become helpless victims of submarine torpedoes—with large losses in life to be expected. Hence, President Wilson was determined to keep America out of war—just like the Scandinavian and certain other countries in Europe were keeping out of it. His position was a very difficult one; his own ambassador in London wrote in his diary:

"I predict that the President cannot be made to lift a finger for war—until the Germans should actually bombard one of our ports. It's cowardice or pacifism that holds him back every time. Self-preservation." 

On the whole, American sympathies were with the Allies but the feelings of a large German-American population had to be taken into account, especially when British high-handed action, every once in a while, severely prejudiced their case. One writer, commenting on President Wilson’s conduct, said that he "was hesitating on the brink of war, reluctant to plunge into it, clinging painfully to the idea..."
It's a nice thing to have soln., code, or cipher, or decipherd code, to have an entity, cryptosystem, and as a result.

The information which in pretty nearly all cases is indubitably authentic because it comes right out of the horse's mouth; but if you can't use it, what good is it except, perhaps, for historical purposes?

In other words, it's one thing to have COMINT—and another, to use it properly.

that is, so as not to dry up the source of the COMINT to continue to receive

the blessings which flow from your crypto-shieldness and good security.

Another way of putting the matter I'm going to discuss at some length is to say that truck pretty nearly every day. Our code hasn't been too bad and how this afternoon we're going to observe an excellent case illustrative of

Enduring Cryptologie

two phenomena which are often hard to join up in marriage, viz., using the COMINT these points which are often hard to join up in marriage, viz., using the COMINT to its utmost advantage, and at the same time protecting it source so as not to dry it up at its source.
of strict neutrality which seemed to be almost a part of his religion."

But maybe a bit of politics got mixed up with the religion because, as some of you may remember, the Democratic slogan for President Wilson's campaign for a second term was: "he kept us out of war". And let's not forget the other famous explanation he gave for keeping out of war—his statement that "there is such a thing as being too proud to fight!" I wouldn't try to defend that.

There was another factor we must keep in mind. For a large part of the United States, especially the Middle and Far West, the war in Europe was 3,000 miles across the Atlantic. It might as well have been on another planet so far as the people who lived in those parts of our country were concerned.

The "cryptologic opportunity" which formed the principal part of the title of my talk, this morning, and which, overnight, it seems, the episode entirely changed the pictures. What was this opportunity? It was the interception and solution by the British of the Zimmermann Telegram.

Now, historians may disagree as to why the United States became a belligerent in World War I; some of them even believe that we went in on the wrong side. But I think that most historians would now agree that it was the solution of the Zimmermann Telegram and the brilliant way in which the British used it, that brought us just in the nick of time, and on the right side—into the war when she was brought in, and brought the United States on the side of the Allies. It could now be no doubt whatever as to the outcome of the war.
After severing diplomatic relations with Germany, something had to be done. Of course, to try to give our merchant ships some protection, and the question of training them to protect themselves was discussed. The idea was to let the Navy provide guns and trained gunners to handle them. And on 26 February, President Wilson
addressed Congress in joint session to advocate that course of action. A bill known as the Armed Ship Bill was introduced in both Houses of Congress, and on March 1st passed the House by a vote of 403 to 13. In the Senate it was less fortunate; it became the subject of acrimonious debate which finally developed into a filibuster led by
Senator For Follette of Wisconsin. The filibuster was successful and succeeded in postponing passage of the bill Wilson wanted. But the President still had a way open to him to do what he wished done — his constitutional power to direct the Navy to furnish the guns and gunsners for American ships that had to pass through the German-declared war zones.
"While the Armed Ship Bill was under discussion in Congress another ... event took place which caused the greatest excitement throughout the country and aroused the people of the United States even more.

Secretary of State[as] wrote, "than the announced policy of submarine ruthlessness." What was this event? It was these.
is for the most part a strictly authentic and truthful account. I.
The Cronkhite film hardly needs comment to indicate the importance which
the publication of the Zimmermann Telegram exercised upon history, and
almost immediately followed the disclosure of its contents.
Publication must inevitably be considered in any study of the causes which
led to our entry of the United States into World War I and the role played
by our country.
The whole episode is replete with drama, and it has been reported in a rather dramatic manner on a recently presented TV program that was one of the series of historical episodes recounted on Walter Cronkite's "You Are There!" Some of you may have seen it when the program was presented "live"; some of you may have seen it as recorded on motion-picture film, a copy of which I've borrowed from the Office of Training, and that film we now are about to see and hear. I'd like to add that the Zimmermann Telegram of 16 January 1917 was the subject of a radio broadcast by the British Broadcasting Corporation as recently as 26 May 1958. I'm trying to get a transcript of that broadcast. I mention this to show you that the Zimmermann Telegram is quite a live subject today—40 years later!

Now let's have Walter Cronkite's "You Are There!" account of the Zimmermann Telegram episode which he presented under the title “The secret message that plunged America into war.” After that, he takes up the background and detailed account of this spectacular and fateful espionage episode of World War I.
careful study by historians as well as cryptologists. It is a story replete with lessons on the disastrous consequences of weakness in "C-power", and with lessons on the opportunities attendant upon great strength in "C-power". And in passing, I may add that the story as it now appears in the history books and popular accounts of the Zimmermann telegram episode appears contrary to some of which will be pointed out today.

I think it correct to say that history attributes our entry into WWI as a belligerent on the side of the Allied Powers to the disclosure of the contents of the Zimmermann Telegram. Note that this statement is qualified.
Just before the film really started, I said, "Let's get in a little after the community the background and detailed account of this, the most spectacular and fateful espionage episode of World War II. For that matter, I think that cryptography history was an episode of World War I."

You will recall that in the Cronkhite story, the reasons for question was raised as to the delay between the date the Zimmerman Telegram was sent, 26 January 1917, and the date its contents were communicated to the American Ambassador, 24 February, a period of almost six weeks. Why did it take so long? Many persons asked. Wasn't that suspicious? What kind of British skullduggery was being covered up? Walter Cronkhite gave an explanation. He said that the story was held back until the German changed their code. Then the Zimmerman Telegram could be published without harm to British intelligence. Well, let's see. At this point perhaps I should say that the Cronkhite story held my interest to the end. I was fascinated by it.
by a date, viz., 6 April 1917. Perhaps that would have come about without the
Zimmermann Telegram, sooner or later, for one reason or another, most
probably as a result of German ruthlessness in the conduct of submarine warfare.

But "later" might have been too late, because after 1 February 1917 unrestricted
submarine warfare started there wasn't much time left to help

Britain and her Allies, because England was being starved for food and munitions,

And if we had waited until England had been starved into starvation and
capitulation, it is possible that America would never have entered the war.

Or, if we were forced to choose by German arrogance, it might have been left to
face a powerful and jubilant Germany all alone. Who knows?

Sent on 16 January 1917, its decrypted plain text.

The fact is, however, that the Zimmermann Telegram was published on
after publication March 1st, and within a little over one month, on April 6th, we declared war on

Germany. There seems to be little doubt, therefore, that we entered the

war when we did because of the Zimmermann Telegram, or, shall we say, rather,
field should be a bit more specific and say that we entered
as a consequence, on the one hand, of German obtuseness in affairs diplomatic

and naivety in affairs cryptologic; and, on the other hand, as the fruit of
first because of
British astuteness in affairs diplomatic and brilliance in affairs cryptologic. Or,
should these two reasons be interchanged in their order. I'll let you
be the judges.
The Crookhite film has dramatically portrayed the
authenticity of the Zimmermann Telegram. The newspapers were full of
denunciations and discussions of what many people regarded a complete hoax, a patent
fraud. In the Congressional Record the debate on March 31st takes up 22 whole
pages—all devoted to the question of the authenticity of the Zimmermann Telegram,
which had so far nothing to back it except the word of the Washington Correspondent
of the Associated Press, for years the discoverer

The fabrication had not been made on the authority of the State Department,
but it had been strangely appeared merely as a dispatch sent broad-

But now let us lift the secrecy veil a bit. It will be of interest to

start in with a brief story about how the British cryptologic organization got

Sir, I should tell you that according to the historical accounts,
and I know they're true, the British government had no crypt-

Read from Ewing lecture at Edinburgh 14 December 1927

diagnostic organization in being when World War I broke out. Oh!

Read from Ewing Room 14 page 1734

Yes. I know there had been a long, long tradition of code

and cipher solving by British intelligence agencies

and this time, but that's another story, and I don't

wish to go into it at this time. All I wish to say is

that there was no cryptanalytic organization

at the British government when World War came in 1914.
There remained, in the American situation when we entered World War I, as a 'callup' in April 1917. In both cases there had to be improvisation with amateurs taking the leading roles, not professionals. Let me recall from a letter dated — make this well — August 23, 1958, written to me by Sir Arnold Dennenston, who was for a number of years before World War II, and for a couple of years during that war the head of the British cryptanalytic organization.

Dr. Dennenston's mention of Sir Alfred Ewing, a good deal of information about, requires elaboration. You will find all the information in a book by his son published in 1939, after some clearance by the authorities, and in a book entitled 'The Man of Room 40: The Life of Sir Alfred Ewing' (Hutchinson & Co, London, 1939). He was mentioned in several other books, and in particular, a book published in 1925 by Admiral Sir William Temple, entitled 'The Navy.'

In 1958, Dennenston devotes a good deal of space to the story of the British counterespionage efforts during the First World War. Here is a quote from that book:

'In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.'

After a few paragraphs on counterespionage efforts, there follows this paragraph:

'In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.'

The book describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple describes the work of Room 40 in World War I. The room was set up in 1917, and it was initially staffed by a few trained spymasters and intelligence officers.

In the book 'The Man of Room 40,' Sir William Temple des
Believe it or not, according to Furing's work for a number of months was entirely a private enterprise effort. It is not clear whether he and his small band of amateurs were paid. I must assume somehow or other Furing and his group were financed through grants, and he says so, and that the small organization did not come under any Director or Sea Lord. This situation was changed when Furing's group became a section of Naval Intelligence under the overall direction of gained a great deal of publicity as a result of the work of the people under him, Admiral Sir W. Reginald Hall. Furing continued to be the head of the group until he became Chancellor of Edinburgh University two years later.

Furing and his small team were University men—non-naval officers; as a result, their translations of German naval signals were strange things in the eyes of the very few men in the Naval Operations staff to whom the translations went. And of course, the gifted cryptanalysts of the amateurs became the butt of jokes and it was a long time before Admiral Hall was able to break down the prejudice against their work. The amazing thing to note is that Hall had assigned a Navy captain to put the translations into proper naval
Language — but that officer wasn't permitted to have access to the room where the cryptanalysts worked or to have any personal contact with them.

It is also reminiscent of certain days in the history of our own cryptanalytic organization to learn that for a good while many months only one person received the translations — the Chief of Staff — to whom they were personally handed in a sealed book! But now it's high time I got down to the real details, which had been shrouded in mystery for almost ten years before. The certain account of the information became available, because the whole of secret was lifted a bit by a story in the November issue of a now-defunct American magazine called World's Work, which was published the final installment of a book by Burton J. Hendrick, entitled The Life and Letters of Walter H. Page. Since then other accounts have appeared, perhaps the best and certainly the latest one being that by Admiral Sir William George, already published book: The Eyes of the Navy, which I've mentioned. But let's begin with the version given in the Hendrick account because it's pretty accurate having been based upon certain telegrams exchanged between our ambassa-

15
I think Walter Cronkite's story used a lot of information that appeared first in this Hendrick account. And in passing I might quote from an address delivered on 6 November 1925 by Lord Balfour who, speaking at a luncheon given at Edinburgh University, said, as reported in The Scotsman of 7 November 1925:

[Page 270 Ewing]

Soon we shall learn the part Balfour played in our story of the Zimmermann Telegram.
We shall not concern ourselves with the steps taken by President Wilson and Secretary Lansing, culminating in the publication by the Associated Press of the text of the Zimmermann Telegram. Our attention will be concentrated upon the minute details of the manner in which the message was intercepted and solved.

"The most fateful message sent to America during the war." Go on with following

"In the British Admiralty this Nauen-Sayville thoroughfare was known as "the main line"; it was the most direct and consequently the one most used for sending German dispatches to the United States."

Hendrick cites no authority for the statement that the Zimmermann was transmitted by radio from Nauen to Sayville. There is very good reason to doubt it.

A few hours after outbreak of war the British, who've always recognized the importance of control of communication channels as well as sea lanes took immediate steps to isolate Germany from the rest of the World that lay beyond the
oceans, by cutting and diverting to her own service the two German cables across
the Atlantic, leaving only indirect channels of communication with her ambassador
at Washington. These were four in number.

(1) Radio - Nauen-Sayville, LaB and Tuckerton, N.J. Both supervised
by the U.S. and (well) supervised to protect our neutrality.

(2) Cable from Germany via Berlin-Stockholm-Buenos Aires, Washington-
your note government,

but this route was secret from U.S. although there is positive evidence that it was quite
well-known to the British from the first days of its use. For the cable from Stockholm
people, as Dearman told me, as "the Swedish Roundabout," to Buenos Aires passed through England; and the route was jealously called by Rommel.

(3) A different cable route -

(4) Involved inserting of secret text in ordinary news dispatches
we learned about it when this method (This was what we may call a "concealment
 concealment system) and was disclosed only after the war by Bredstrom himself.

Now

As to the first method, the use of the radio channel was prohibited except

and I am glad to say that the supervision

under American supervision/exercised by American authorities was very detailed

Hendrikk is absolutely wrong when he says (p. 25, 1st column) "... how little this
prohibition interfered with the Germans is shown by the use they made of
the Long Island station for this, the most fateful message sent to America
during the war." I have very carefully searched every available record and
for the Zimmermann Telegram
have found not the slightest evidence that this channel was actually used.

The German accounts have been examined as well as American,

in learning how the
supervision was exercised. 

I suggest you study this brochure on the Zimmermann
Telegram (pages 7 and 8), I think you'll agree that great care
was taken by the authorities who had the responsibility of seeing

No, the Zimmermann Telegram wasn't sent via that route, although

Hendrik's account makes it plausible by saying:

column to last 2 lines p. 26). Does Hendrik want to imply Béjástorff

thisSure which the Mexican President Carranza was so pvellow?

added this precious bit of enticement? No, Hendrik's explanation is quite

wrong; it is in fact misleading and perhaps intentionally

gaps and doubtful points in the text of the message as first intercepted:

It will go a long way to explaining the 6-weeks' delay we've been trying
to explain.

We come now to the second communication channel used by the German

Government etc. . . . bottom p. 8 of brochure hand of line at top p. 9

see me

-16.
There is plenty of evidence that the British knew of this circuitous route; it happened to be decades of messages that passed over this route later appeared among the hundreds in the affidavit by Admiral Hall.

in the records of the Mixed Claims Commission set up after the war.

Many passed over the Berlin-Stockholm-B. A. Wash. route. What messages the Swedish Roundabout, 

in Berlin, the Germans did was to hand their coded telegrams over to their Swedish Minister to Germany, his friends in Washington and in Berlin; the Swedish Ambassador addressed to Stockholm addressed to his own friends in Stockholm. W. I. went to the Swedish Ambassador in using a disguise that consisted of enciphering the German code groups

in Buenos Aires, who turned it over to his German colleague in Washington, who then verified the message to Berlin. There was a process of systematic alteration, and now it was clear to the difference of ordinary people that the differences between the Swedish and German code groups would not be noted.

Judge noted the disguise even before the message left Europe. He remembered that the cables from Stockholm to Buenos Aires which he received there as the cables touched London the disguise was pretty thin, as the cables touched London the disguise was definitely changed, and systematically.

The Hendrik account would make it appear as if the Zimmerman Telegram could be unravelled and read by anybody not possessing a copy of the code-book—certainly not the stupid Englishmen. And also, by the way, the disguise procedure began as early as in the summer of 1915.

The Hendrik account would make it appear as if the Zimmerman Telegram received special treatment to insure its receipt but it is clear from the German records alone that the transmission of important messages by
more than one route was routine procedure with Stettin. But Hendrik

says:

```
Read from p. 26 of Hendrik, Column 1. Hendrik's statement "In many
capitals German messages were frequently put in Swedish cipher and sent to
Swedish Ministers..."
```

implies that the British read Swedish codes, too. Now it would be easy to believe

```
Read from p. 18 of brochure—"Now it would be easy to see...
One is thus in possession of evidence I'm going to shift
over with the next state your Official in writing the publication
by the State Department on 3 September 1917 of certain wave groups too close
now as the German would have written or "other without these" messages.
```

We come now to the third and most interesting of the Zimmermann

```
That the Cronstedt story reported so dramatically as that
Telegram routings—the one used with cooperation of the State
Department. I quote from the Hendrik narrative:
```

```
Hendrik makes it appear that obtaining permission to use State Department
facilities was a rather simple matter—p. 12 brochure—all the page to
```

```
and place p. 13 marked "stop here".
```

```
I am in a position to say categorically that
The State Department was indeed careful in placing its communication
```

```
(ind s) facilities at the disposal of the Germans. Mr. Lansing not only realized...
```

```
(Read from p. 14 brochure—one para only) 2nd para on p. 11

---

--- 15
We come now to a study of the code used for the Zimmermann Telegram. Note the plural—"codes"—that's very important in this case as you shall see.

First, its passage from Berlin to Washington: There can be no doubt the code used for the Zimmermann Telegram was the one which had been appended to Berlin-Washington No. 157, and which had been sent via State Department channels. As I've already said, the British Government has officially never published any account of the interception and solution of the Zimmermann Telegram by its cryptographic agency commonly referred to as the "cryptanalysts in Room 40".

But when we study very intently telegrams that passed between the British and American Governments dealing with the Zimmermann Telegram as related in the Hendrik account—and more especially now, the account contained in Admiral James' book, published only three years ago by a close associate and wartime colleague of Admiral Hall, this is the book. This is the book, Eyes that illuminate the dark or dubious points in the story of the Navy, by Admiral Sir William James.

Admiral James in his forward says:

"Read from p. xi and xii to point marked."

But Admiral James was careful. Even though, as he says, he had no access to unreleased official papers and therefore, he says, it wasn't...
I'm fortunate to be able to show you what Mr. de Gray looked like. In my many talks with him not only did he mention the role he played in the reading of the Zimmermann telegram—nor did anyone else in the organization.
in which he was Deputy Chief to Sir Edward Ternay, the Chief.
I have no photograph of the Reverend Montgomery to show you. But I may have one of his
part of a character in Dickens or in a spine-chilling mystery in book or on stage.
necessary for him to obtain official approval for publishing his book, he
did submit it for some sort of blessing, if not approval, as this memo to
report dated 15 December from our then-Deputy-Senior Liaison Officer to GCHQ
who said: "... clearly shows:

Read from Larkin memo.

"A" attached

Apparently didn't

And perhaps it is not strange to say Admiral James himself doesn't

know the delicate and interesting technical points about the Zimmermann
Telkogram which remained obscure or in doubt until he published his book.

The same said of:

And likewise can be about his clarification, --unintentional, I'm sure,
of

other dubious points about the history and operation of Room 40. But we
can't go into these except as they deal with or impinge upon

But we shall have to confine ourselves to the verifiable facts about

the cryptology of the Zimmermann Telegram.

Let's begin by quoting from Admiral James' account. (James, p. 136)

"Then early in the New Year (read p. 136 and 137 to point indicated and comment

are the truth of what James says about the source of the De Trey-Montgomery

message. (Incidentally, describe De Trey).

There are reasons to believe that the version what we have just seen
came from the British copy of the State Department message containing Berlin's
Nos. 157 and 158 to Washington—but I don't think it would have been polite at this time or even now to reveal intimate details that the British were also intercepting and studying messages of the US Government. I wouldn't suggest mentioning such an idea were it not a fact that soon after we came into the war our ally Britain officially told us that our soldiers weren't safe! (Then go on with last paragraph p. 137 and continue with p. 138 and 139 to point indicated at middle of p. 137.)

Berstorf tried desperately to have Berlin change its decision about unrestricted submarine warfare—to no avail.

On 1 February, Berstorf presented the declaration re submarine warfare which begin that day. President Wilson broke off relations two days later, on 3 February. As we have already noted, Hall then took steps to obtain the additional evidence that he required, in the circumstances and telegraphed to his secret agent in Mexico City to get all copies of Berstorf's telegrams to Eckhardt since 18 January. These were sent to Washington and forwarded by cable to London in British cipher. No hitch developed in this nice arrangement. What James goes on: "So much progress with the reconstruction of the code had been made that by February 19 Hall had in his hands an almost perfect transcript and James then gives the text of the Zimmermann Telegram as published in the Century Books."
"Mr. T." was a British operative or secret agent in Mexico City. In a rather odd way, he turned out to be a most useful character in the drama of the Zimmerman Telegram.

When "T" was replaced by secret agent "H," the good work went on, and that's how Hall in London was able to get a copy of the Zimmerman Telegram in the form in which it was sent from Washington to Eckhardt in Mexico City. That turned out to be of crucial importance! As Admiral James says (p. 14):
But James is throwing a little dust in our eyes. The version of the

Zimmermann telegram that was finally published was not the version that

was in the telegram from Zimmerman to Balfour, which laid out a

plan for joint action against America. Balfour, in a separate

letter, was quite similar in content, as much one-part code

Hendel the message began to tell the President what

the President’s

was to do. It was in the telegram from Balfour to Zimmerman, which

stated: ‘Hendel, the plan was to fool America.

But this time Balfour had information that the German-Americans in

the United States were extremely active in their endeavors to stay the

President’s

hand. It was felt that the time had come for immediate action and formally

balloted. Mr. Bryan was pressed for a decision. On 29 February he received

Balfour’s authority

to handle the whole matter as he saw fit. James, who continued actively

in Washington, was asked by Mr. Bryan to

continue with p. 145 to end by 3rd para. on July 31.

We’ve already heard the contents of the message from Page, the

American Ambassador in London, to the President and Secretary of State

on July 31.

I won’t repeat it now; you’ll recall that it was Page’s story that the

President was not in the Council Chamber on the occasion when

loose, and that Mr. Bryan was pressing for an immediate decision. Mr.

Bryan was informed that the message in Balfour’s telegram was

the plan that was to be followed by the German-Americans in

the United States to keep America out of the war.

But by this time Ball had information that the German-Americans in

the United States were extremely active in their endeavors to stay the

President’s hand. It was felt that the time had come for immediate action and formally

balloted. Mr. Bryan was pressed for a decision. On 29 February he received

Balfour’s authority

to handle the whole matter as he saw fit. James, who continued actively

in Washington, was asked by Mr. Bryan to

continue with p. 145 to end by 3rd para. on July 31.

We’ve already heard the contents of the message from Page, the

American Ambassador in London, to the President and Secretary of State

on July 31.
that "early in the war the British Government etc. read extracted and marked paragraphs on p. 144, James.

But now listen to James: (p. 345) "It was not the case etc. -- just that paragraph and the next one and then continue from p. 16 of F-M brochure and read all the way to bottom of page 16 of brochure."

place around the cryptanalytic fact every security safeguard he could devise. Nobody can blame Hall for trying to put everyone including Page, the he would part off the wrong trail anybody else he thought might give parade security. Second, President, the Secretary of State, off on the wrong trail and to cover the tracks of Room 40. At the time this brochure was written we didn't know all the facts -- we were making inferences and deductions.

We said:

Read two marked paragraphs on p. 17 of brochure.

We felt that "cipher books," the statement that a codebook -- or at least some sort of code document -- or captured must have contained, but we didn't know -- that now was found must contain an element of truth, because here is what the Ewing method, and the British, soon after, we received the writings of their translated 130 to 135 and it pay anything about late having been constructed on the basis of a so-called code that they had. But it's exactly what they done as I have since then established. For example: (Ewing 5-15) we took the following:

Note the illuminating statement that the captured material enabled the workers in Room 40 to read much enemy dip correspondence, "thus providing a starting-point from which to penetrate, one after another, the German Foreign Office Ciphers."
Admiral top,

On-the-other-hand, James gives us much more specific and valuable information on this point—"I think it is accurate." (James, pp. 69-70)

With the aid of our able archivists I've been able to dig out of the old files of World War I—I would have used German Code 1348, butt my address, etc. It's an interesting document—As also is Englıšcher Chiffre 9972 and Code 7598—there are all in our archives;

But to get back to the Zimmermann Telegram itself again, you will recall that I said it was published in all the important newspapers of the world.

In pro-German circles the telegram was immediately denounced as a forgery on March 1st, 1917. After acrimonious debate a resolution was passed by the Congress that the President be asked to state the source of the information. He replied the same evening through his Secretary of State as follows:

Zimmermann in a statement before the Reichstag made a long, involved and foolish apology for his inept conduct, issuing up with this grave error because I held [meaning written on next page]

How naive! How could such a naive man rise to be head of the Foreign Office of a great and powerful state? It will hardly astonish you that Zimmermann continued to use Code 1348, and that he even learnt his job as Foreign Minister.
If Zimmermann had been really smart he would have denounced the telegram as a forgery, fraud, and product of British duplicity and chicanery—
even if only to smoke the British out and make them prove the authenticity of the telegram by disclosing exactly how the message and the information contained in it was obtained.

That is what Hall greatly feared would happen—-but his fears turned out to be groundless. Zimmermann was too dumb, too slow, too inept—and he soon...

Now go back to F-M brochure, p. 17 to end of 2d para.