

## NATIONAL SECURITY AGENCY CENTRAL SECURITY SERVICE FORT GEORGE G. MEADE, MARYLAND 20755-6000

NSA PRESS RELEASE

27 January 2012 For further information contact: NSA Public and Media Affairs, 301-688-6524

## National Cryptologic Museum Opens New Exhibit on Dr. John Nash

Renowned mathematician Dr. John Nash wrote a series of letters to NSA in the 1950s proposing a new encryptiondecryption machine. Copies of his letters are on display at the National Cryptologic Museum. (NSA photo.)

FORT MEADE, MD - When people hear the name "John Nash," many recall the movie *A Beautiful Mind*, in which actor Russell Crowe portrays the mathematical genius whose game-theory research as a graduate student at Princeton University earned him the Nobel Memorial Prize in Economic Sciences in 1994.

The National Cryptologic Museum's newest exhibit, "An Inquisitive Mind: John Nash Letters," features copies of correspondence between Dr. Nash and the National Security Agency (NSA) from the 1950s when he was developing his ideas on an encryption-decryption machine.

At the height of his career in mathematics, Dr. Nash wrote a series of letters to NSA, proposing ideas for such a machine. While the agency acknowledged his ideas, they were never adopted. The letters were preserved with NSA's analysis in a collection of unsolicited correspondence received in 1955.

The unclassified letters and the agency's analysis, portions of which were classified, remained protected in NSA's records center until 2011, when the entire collection was reviewed and declassified. The entire collection is being formally accessioned to the National Archives and Records Administration and will be available for public viewing later this year.

Copies of Nash's letters to NSA are on display at the National Cryptologic Museum with complete copies available for review in the museum's library and on the museum's web page at http://www.nsa.gov/public\_info/\_files/nash\_letters /nash\_letters1.pdf.

The National Cryptologic Museum is located at the intersection of Maryland Route 32 and the Baltimore-Washington Parkway (I-295), adjacent to the headquarters of NSA. Hours of operation are 9:00 a.m. to 4:00 p.m. Monday through Friday (except federal holidays), and 10:00 a.m. to 2:00 p.m. on the 1st and 3rd Saturdays of each month.

For more information on this press release, call the NSA Public Affairs Office at 301-688-6524. For information on museum tours, educational programs, and hours and days of operation, click on the National Cryptologic Museum tab at www.nsa.gov. Admission and parking at the museum are free.

Defending Our Nation. Securing The Future.

Please Note: These FOLLOWING historical documents are PDF images of formerly classified carbon paper and letters that have been declassified. Due to the age and poor quality of some of the PDF 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.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY CAMBRIDGE 39, MASS.

236

DEPARTMENT OF MATHEMATICS

Deor Major Grosjean, I have worther RAND concerning the machine description. This was hand written and was sent to NSA late last spring, I believe, or sent to someone there. Essentially the same machine description was once sent to a Navy commication for to a Navy commication sent to a Navy communication Center in Washington, I think. I have discussed the machine and theory general machine and theory general exponential conjecture with R.C. Blanchfield and A.M. Gleason Blanchfield and For NSA. Recently a conversation with Prof. Hoffman here indicated Prof. Huttman here manual working that he has recently been working that he has recently been working objectives. Since he will be objectives. Since he will be consulting for NSA I shall



MASSACHUSETTS INSTITUTE OF TECHNOLOGY

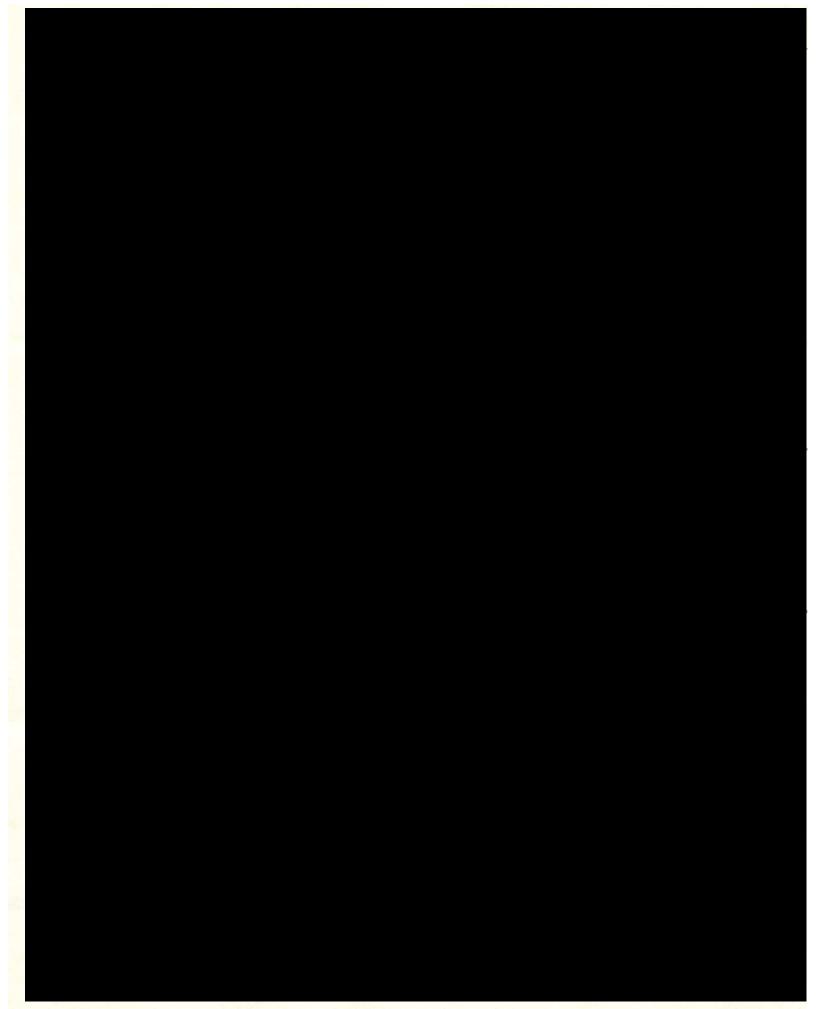
CAMBRIDGE 39, MASS.

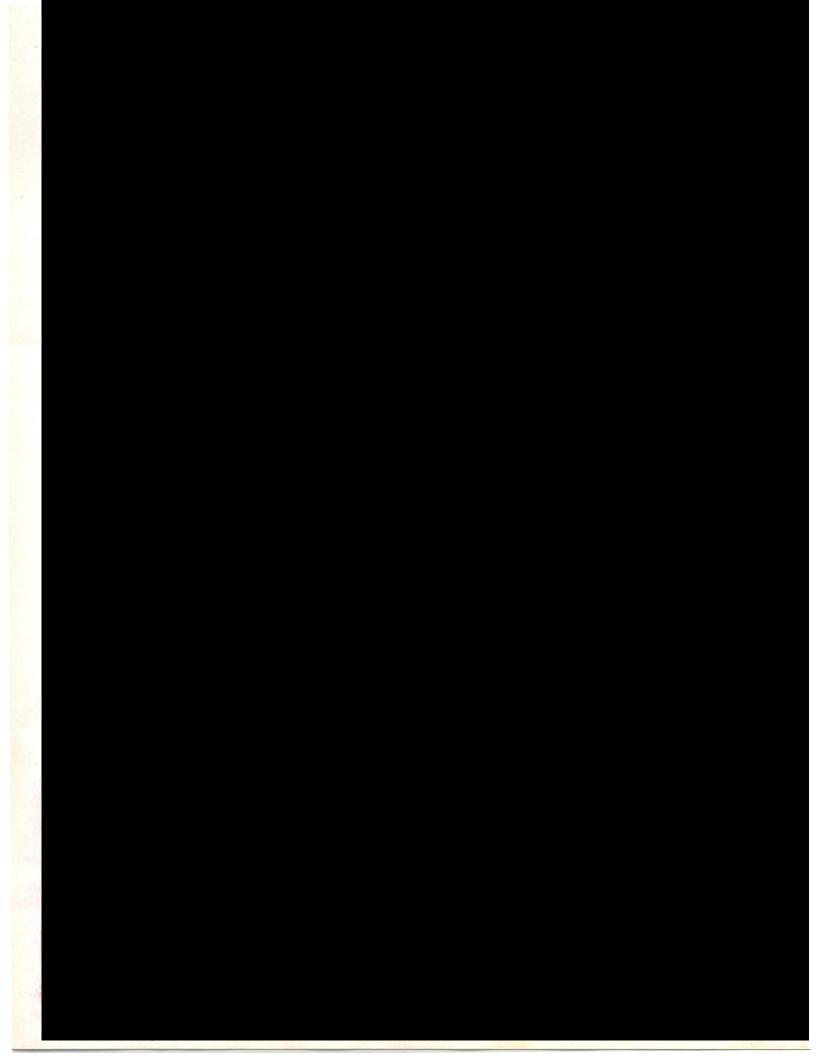
DEPARTMENT OF MATHEMATICS

letter concerns ENCIPHERING

Dear Sires: An enciphering-deciphering machine Cingeneral outline) of my invention has been sent to your asgonization by way of the RAND cosposation. In this letter I make some remarks on a general principle relevant to encipheing in general and to my machine in posticulor. This principle seems quite impostant to me and I have some reason to believe you may not be fully aware of it. with a finite "key", operation ing on binary messages . Specifically, we can assure the process described by a function Y: = t(x, d2, .... Xr; X:, Xi-1, Xi-2, .... Xi-n) where the d's, X's, and y's are mod 2 and where if xis is changed, with the other x's and is left fixed then Yi is changed.

The is denote the "key". 12 Containing & bits of information. n is the spon maximum spon of the "memory" of the process. If n were the asguments give below would not be basically altered. To consider the resistance sham enciphering process to being broken we should assure that at same times the enemy knows everything but the key being used and to break it need only discover the key bon this intermation. me see immediately that in principle the enemy needs Very little information to begin to break down the process. Essentially, as soon as p bits of anaphred message have been toons mitted the key is about determined. This is no security, for a practical key should not be too long. But this does not consider how easy lit is bes the energy to make the computation determining the key. If this computation

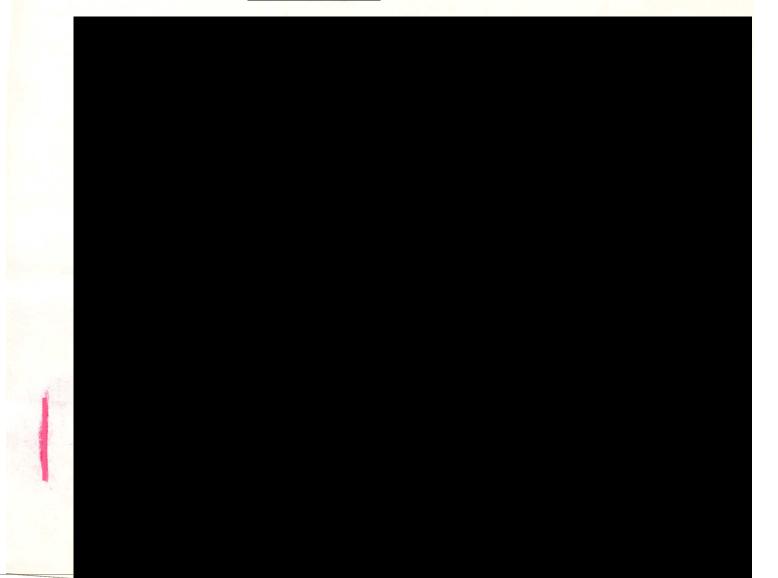




The nature of this anjecture is l's such that I annot prove it, even for a special type of ciphe. Nor do I expect it to be prover. But this does not destroy its signifiance. The probability of the touth of the conjecture can be guessed at on the basis of experience, with enciphering and deciphering. believe in the exponential conjecture the I think we (the U.S.) can not afford not to make use of it. Also we should try to keeps toack of the progess of foregen nations towards inbreakable" types of ciphers. Want other nations to use ciphers we connot expect to break, this general principle should probably be studied but the kept secret. I believe the enciptering deciphring machine I mented and had toonsmitted to the N.S.A. VIA RAND has this "inbreakable" property. In addition it has several other advantages in that







531 Serial: 25 JAN 1955

Mr. John Nash Department of Mathematics Massachusetts Institute of Technology Cambridge 39, Massachusetts

Dear Mr. Nash:

Your recent letter, received **#** January 1955, is noted. Technicans at this Agency recall a very interesting discussion with you which took place approximately four years ago, and will welcome the opportunity to examine your ideas on the subject of cryptography.

A check within this Agency has, unfortunately, disclosed no information on your machine. A description of the principles involved will be appreciated.

Sincerely,

cc: AG C/S COMSEC (3) 412

E. M. Gibson Lt. Col., AGC Assistant Adi. Gen.

A. Lyons, 4128, 60372, in

M/R: In Jan 1955, Mr. Nash offered general remarks on cryptography and requested evaluation of descriptive material which he had forwarded through Rand Corp. NSA Ser 236, 12 Jan 55 informed Mr. Nash that the material had not arrived. Mr. Nash in letter rec'd 18 Jan 55 states the material was sent to NSA and to a Navy Communication Center in Wash. late last spring. A check of Agency records and discussions with various individuals (R/D mathematicians and persons who might have had contact with Rand Corp.) within the Agency has undovered nothing concerning the system. This correspondence requests a description of the machine.

In 1950 Mr. Nash submitted material, in interview, which was evaluated by NSA as not suitable.

Serial: 236 1 2 JAN 1955

Mr. John Nash Department of Mathematics Massachusetts Institute of Technology Cambridge 39, Massachusetts

Dear Mr. Nash:

Reference is made to your recent letter concerning enciphering processes. The information regarding the general principles has been noted with interest. It will be considered fully, and particularly in connection with your enciphering-deciphering machine.

The description of your machine has not yet been received from the Rand Corporation. As soon as details are received, the machine will be studied to determine whether it is of interest to the Government.

The presentation for appraisal of your ideas for safeguarding communications security is very much appreciated.

Sincerely,

cc: AG C/S COMSEC (3) 412

D.M. GROSJEAN IMAJOR WAC Actg. Asst. Adjutant General

M/R: Mr. Nash offers remarks on a general principle relevant to enciphering in general and to his machine in particular. The machine, which he is sending via the Rand Corporation, has not yet been received.

This letter informs Mr. Nash that his remarks are being noted and that the machine will be studied as soon as details are received. This reply coordinated with Mr. M. M. Mathews, NSA-31. This is an interim reply.

M. A. Lynes, 4128, 60372, in

C/SEC 2-2

MASSACHUSETTS INSTITUTE OF TECHNOLOGY CAMBRIDGE 39, MASS.

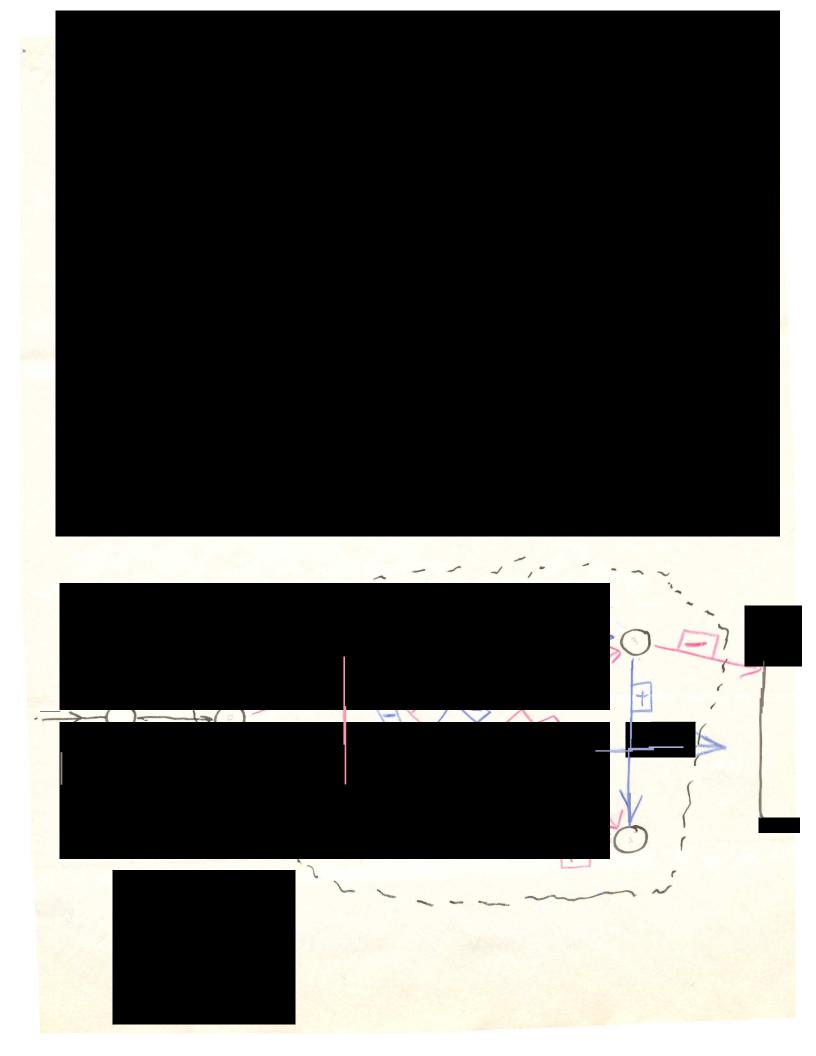
DEPARTMENT OF MATHEMATICS E.M. Gibson, Lt. Col., AGC, Asst. Adj. Gren. DEOF SIT: mput Here is a description of my enciphering deciphering machine. clo (C.P. PSE martation outpu Choose. Permuter-Reverse Adder mod 2 Arrangement ) Transmitting Retorder outpu deuphered Receiving Arrangement 2 In the receiving acrongement the some components are used except for the addition of the retorder, which is a one-onit delay. The messages are to be sequences of binosy digits (numbers mod 2). The machines work on a cycling basis, performing certain operations

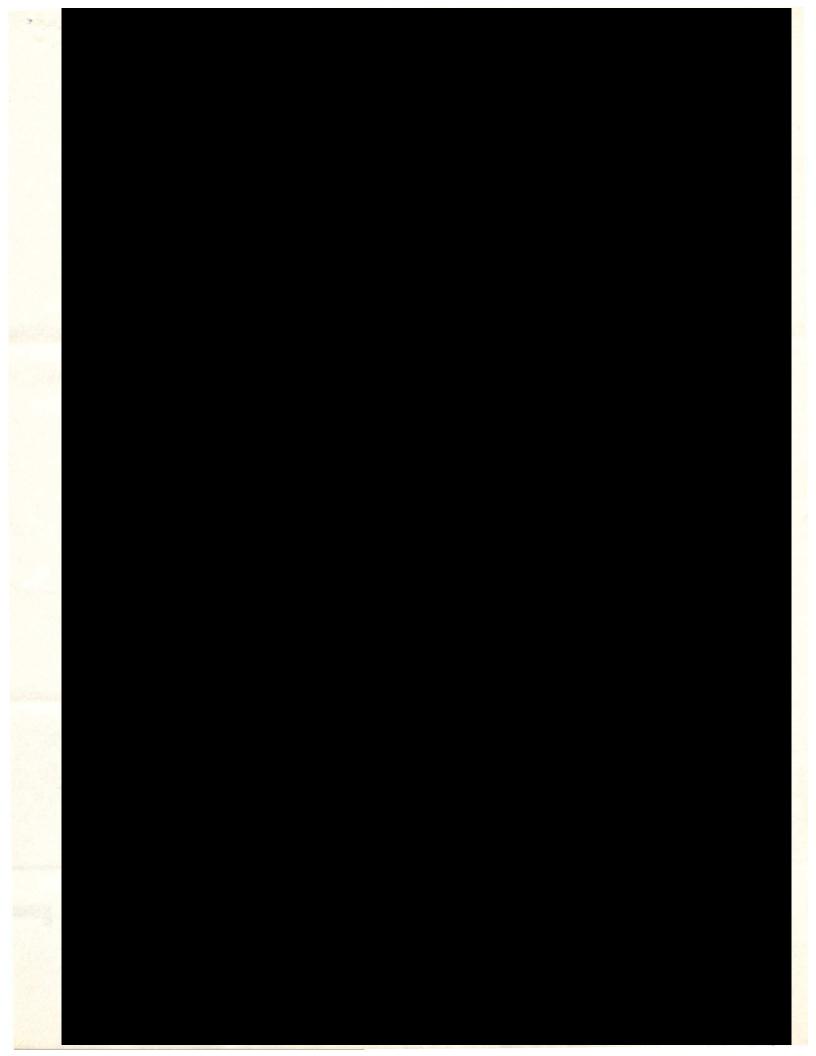
during each cycle.

Doring each cycle the adder A, takes in two digits and adds them and sends on the sun obtained from the previous addition. The delay in this addition necessitates the retardor R in the receiving circuit.

The permutes will be described in more detail below. It takes in a digit from D during each cycle and also pots out a number. What it does, which is the choice between two permutations is determined by what digit (1 or 0) is in D at the time. The permutes always hos a the number of digits remembered within it. Each cycle it shuffles them oround, changing some I's to zeros, sends are digit on, and takes in a digit from D.

In operation the input of the receiver is the output of the transmitter. So the input to R is the some as the input to D in the transmitter. Hence the output of P in the receiver is the same as the out-put of P in the transmitter, except for a onemit lag.





The "key" for the enciphering (5) machine is the choice of the permutations. If there are n Storage points in P, not counting the first one, which receives the digit from D, then there are  $[n! 2^{n+1}]^2$ possible teys.

Serial:

1358 3 MAR 1955

Mr. John Nash Department of Mathematics Massachusetts Institute of Technology Cambridge 39, Massachusetts

Dear Mr. Nash:

Reference is made to your letter received in this Agency on 17 February 1955.

The system which you describe has been very carefully examined for possible application to military and other government use. It has been found that the cryptographic principles involved in your system, although ingenious, do not meet the necessary security requirements for official application.

Unfortunately it is impossible to discuss any details in this letter. Perhaps in the future another opportunity will arise for discussion of your ideas on the subject of cryptography.

Although your system cannot be adopted, its presentation for appraisal and your generosity in offering it for official use are very much appreciated.

It is regretted that a more favorable reply cannot be given.

Sincerely,

E.M. Gibson Lt. Col., AGC Assistant Adj. Gen.

cc: AG C/S COMSEC (3) 412

(M/R ATTACHED)

M/R: In Jan 55 Mr. Nash offered general remarks on cryptography and requested evaluation of descriptive material which he had forwarded through Rand Corp. The Material was not received from Rand Corp. Dr. Campaigne received a letter from Mr. Nash inclosing a copy of the letter (5 Apr 54) from Rand which transmitted this material to NSA. This material was found in R/D files. In the meantime Mr. Nash sent a handwritten description of his enciphering-deciphering machine.

Mr. Nash proposes a permuting cipher-text auto-key principle which has many of the desirable features of a good auto-key system; but it affords only limited security, and requires a comparatively large amount of equipment. The principle would not be used alone in its present form and suitable modification or extension is considered unlikely, unless it could be used in conjunction with other good autokey principles.

This correspondence informs Mr. Nash that his system does not meet necessary security requirements; and expresses pleasure at the thought of an opportunity to discuss Mr. Nash's ideas on cryptography again. Such a discussion took place in 1950 when Mr. Nash submitted material, in interview, which was evaluated by NSA as unsuitable.

An interesting pamphlet on Non-Cooperative Games, written by Mr. Nash was also sent to this Agency by the author for our information.

Dr. Campaigne has been informed that the reply has been written and is not interested in further coordination.

Malyons, 4128/60372/rwb