

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOVEMBER 1975



P.L. 86-36

WHEN CENSORSHIP BACKFIRES.....	James Killough.....	1
[REDACTED]	[REDACTED]	3
DESKPAD: A PROGRAMMER'S TOOL.....	[REDACTED]	7
[REDACTED]	[REDACTED]	9
IN PRAISE OF SOLITS..... NOTES ON BLUE RUSSIAN..... NATIONAL CRYPTOLOGIC SCHOOL OFFERS COURSE-EQUIVALENCY TESTS.....	Louis C. Grant... [REDACTED]	12 12 13

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~Classified by DIA/NSA/CHESS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

~~TOP SECRET~~

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

VOL. II, No. 11NOVEMBER 1975

PUBLISHER

WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief..... Arthur J. Salemme (5642s)
Cryptanalysis..... [redacted] (8025s) P.L. 86-36
Language..... Emery W. Tetrault (5236s)
Machine Support..... [redacted] (3321s)
Special Research..... Vera R. Filby (7119s)
Traffic Analysis..... Frederic O. Mason, Jr. (4142s)

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

~~TOP SECRET UMBRA~~Soviet Revelations, 1973-1974

Though Shabad may not have known how close he came, the guardians of the secrets at Glavlit and the Ministry of Medium Machine Building (the ministry with overall responsibility for the Soviet atomic-energy program) knew only too well and must have had some unkind thoughts for our wily correspondent. While he had not completely spilled the beans, he had tipped them very precariously. They could be fairly certain that Shabad had focused the attention of at least a few Western intelligence analysts on the Leninabad area.

Given the choice of stonewalling it or letting the chips fall where they might, the censors apparently decided the jig was up and took the wraps off the "secret city."² In 1973, Volume 14 of the Third Edition of the *Large Soviet Encyclopedia* was published. It contained a short article on Leninabads'kaya Oblast' and identified the seventh city as *Chkalovsk* (of which "Skalows I" had obviously been a garble). In typical Soviet fashion, the censors refused to show the city on the map accompanying the encyclopedia article.

In 1974, however, perhaps realizing the futility of their predicament, they passed two publications:

- a map showing Chkalovsk as a city a few kilometers southeast of Leninabad, with between 10,000 and 30,000 souls; and
- an administrative-territorial handbook listing *Chkalovsk* as a city with 26,000 inhabitants that had been created in 1956 (the year Oplanchuk was transferred from East Germany), with administrative responsibility for three widely separated settlements: *Taboshar*, about 45 kilometers north of Chkalovsk; *Palas*, about 15 kilometers to the east; and *Naugarzan*, in the extreme northern tip of Tadzhikistan, over 90 kilometers northeast of Chkalovsk. None of these four locations were included among the 63,499 entries in the 1969 USSR Postal Index (similar to our ZIP code listing). NSA's Soviet Localities File contained no open-source references to Chkalovsk or Taboshar, and no references at all to Naugarzan or Palas. But in 1974 the lid was off.

²Statements concerning the motives of the censors are of course pure speculation, in view of the lack of defectors from Glavlit.

Soviet 1975 Republic-Level Elections

Which brings us now to the 1975 republic-level elections. With the censors presumably chastened by Shabad's exposé, there was no repetition of the 1971 shenanigans: no electoral districts were omitted from the published list. This time all the four deputies from Chkalovsk were either employees of the Combine or had been nominated by workers of the Combine.³ This clearly shows Chkalovsk to be a "company town" whose administrative control over Taboshar, Palas, and Naugarzan is a result of its uranium mining and refining activities.

All of this, including the reference to "Skalows I," began to make sense. Presumably for reasons of security and economics, the ad-P.L. 86-36 administrative headquarters of Combine 6, along EO 1.4. (c) with support elements and other non-mining facilities, were relocated to a new city incorporating an area of extensive recent construction and the older settlement of Chkalovskij from which it took its name. In order to maintain complete control over its subsidiary mining operations, it was necessary to subordinate the local soviets of Taboshar, Palas, and Naugarzan to the Chkalovsk City Soviet. Thus, since reference to Chkalovsk was forbidden, mention of the other three locations was also taboo. The situation was not unique, but was certainly very unusual. For 15 years the blackout succeeded, and therefore may be said to have served its purpose, but in the end it was its own undoing. Were the Soviets ready to reveal their "secret city" anyway, and was Shabad's article a mere embarrassment? I doubt it.

Moral:

Excessive censorship may betray that which it is supposed to protect; or
It pays to read Soviet publications with an eye to what is not said.

³This time the censors tried to confuse us by calling it "a construction combine." Ah what tangled webs we weave. . .

~~TOP SECRET UMBRA~~

November 75 * CRYPTOLOG * Page 3

~~TOP SECRET UMBRA~~

P.L. 86-36
EO 1.4.(c)

November 75 * CRYPTOLOG * Page 4

~~TOP SECRET UMBRA~~

EO 1.4. (c)
P.L. 86-36

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

DESKPAD: A Programmer's Tool

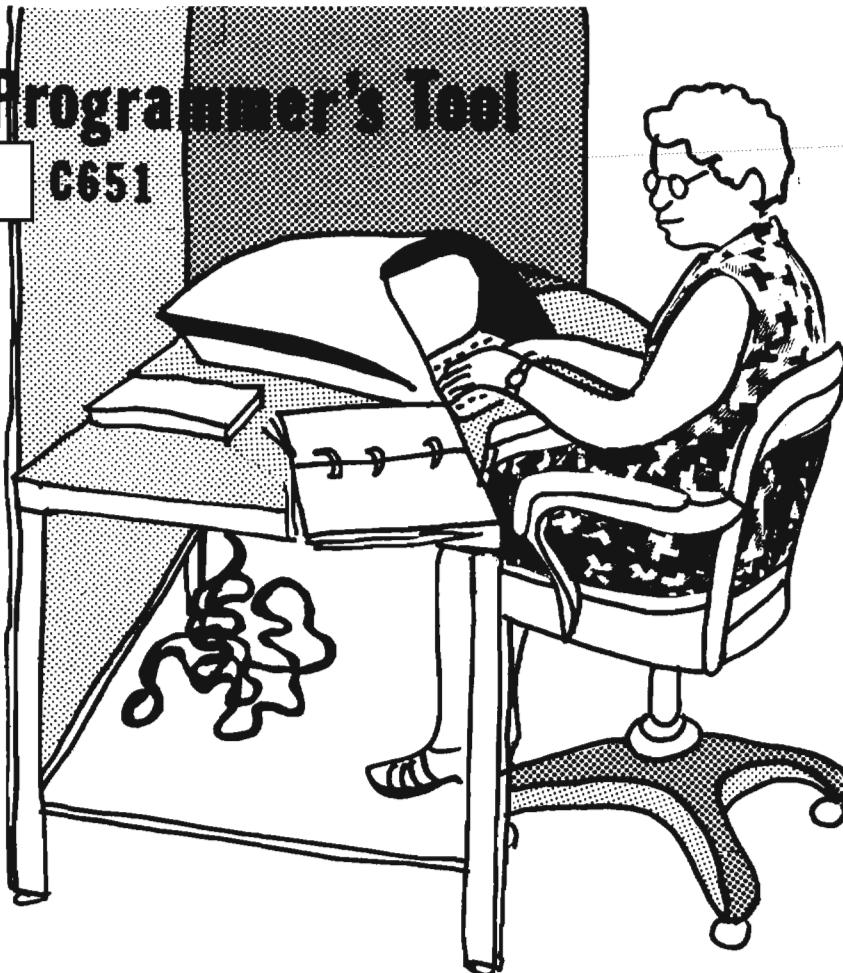
By [redacted]

Software is getting more costly and taking up more of the Data Processing budget. More work is being requested of fewer people. Software is becoming more sophisticated and more complex. How can management meet the new challenges? Increased productivity is one way, and DESKPAD is a way of attaining this goal.

DESKPAD is a remote-terminal, time-sharing, software-development system. The DESKPAD system provides the full capability of an on-line computer system to the programmer when he needs it. By assisting the programmer, DESKPAD increases overall productivity in areas such as documentation, generation of specifications and design plans, as well as the actual programming. The remote system saves the programmer time in various ways: travel to and from machine areas is reduced since updating is performed on-line; the time-consuming task of making corrections, on tape or cards, to programs is eliminated; there is no longer a need to wait for a machine run to see how a piece of code fits in, since the program text is available on-line; and documentation is kept up to date, since it can be changed as the program is modified or generated while the program is being developed.

With the increased productivity made possible by DESKPAD, the system can pay for itself in less than 5 years. The average salary of a programmer is \$12,800 a year. A 5-percent increase in his productivity will yield an increase in his value of \$640. In a division of approximately 70 people, the total increase in value will be \$44,800 a year, which is approximately one-fifth of the \$180,000 cost of the DESKPAD system.

The DESKPAD system consists of a Digital Equipment Corporation (DEC) PDP-11/45 computer with 112K of main memory and 40 megabytes of mass storage. The system contains various peripherals including magnetic tape, paper tape, 16 VT05 CRT terminals, a link to the UNIVAC 1108 computer, and a REDACTRON Communicating Type-writer. Hardware is under control of the RSTS/E (Resource Sharing Time Sharing/Extended) system

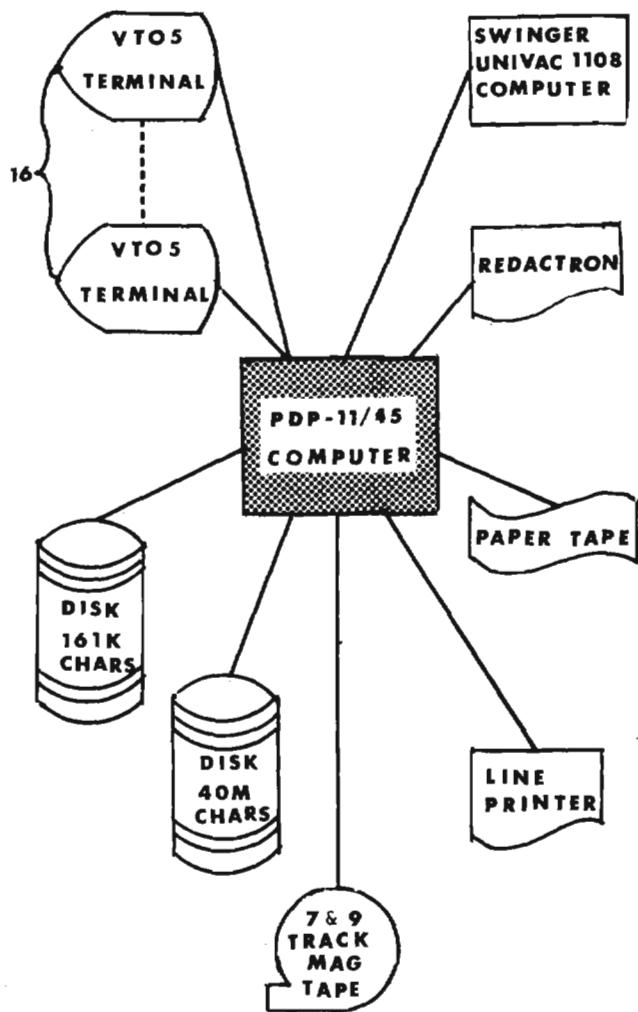


P.L. 86-36

purchased with the system from DEC. RSTS allows the users to perform time-sharing with the Basic-Plus language. Basic-Plus performs matrix manipulation, alphanumeric string operation, virtual memory addressing, and many other functions that allow both simple and advanced programming to be performed. Also available are many utility programs to standardize redundant operations needs for everyday use. These utilities include a peripheral interchange program (PIP), an accounting information program (MONEY), a system status reporter (SYSTAT), a file recovery program (BACKUP), a character/line editor (EDIT), and a powerful cursor control editor (PAGE). PAGE is the most frequently used software package on DESKPAD. The editor was obtained at no cost to the government through our membership in the Digital Equipment Computer User Society (DECUS). It provides the user with total control of the VT05 terminal. PAGE makes the task of editing more enjoyable than one the programmer resents doing. In addition to the previously mentioned software, a software interface has been purchased from the Oregon Museum of Science and Industry (OMSI). The interface allows RSTS users to make use of the RT11 single-user system. The

UNCLASSIFIED

DESKPAD HARDWARE



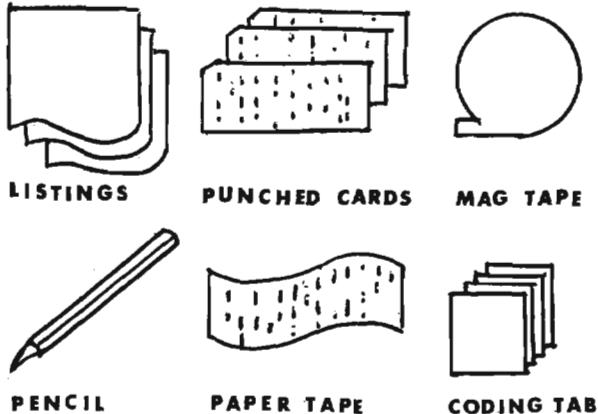
RT11 system provides the user the capability of running the PDP-11 Macro Assembler and Linker as well as FORTRAN IV. With the OMSI-supplied interface, DESKPAD expands its capability to compete with most of the large-scale systems in the Agency.

The DESKPAD system is currently in use in the Field Software Support Division of C6. With the division supporting 26 small systems, some with virtually no updating facility or so primitive that it takes 2 to 3 passes to complete a single update, it is easy to see why DESKPAD has become quite popular. DESKPAD currently supports 69 people using 700 files assigned to 144 accounts. A "HELP" program is available to provide users with current system information. HELP provides information ranging from sign-on instructions to execution of a FORTRAN program. A "GRIPE" program gives the user a means of communicating with the system manager. It informs him of system deficiencies as the user sees them. All gripes are answered within one week by the system manager. Technical

notes are generated to provide users with documentation of user-written utility programs and to provide additional documentation on any other area of DESKPAD that requires it.

With austerity hitting all parts of the Agency, systems such as DESKPAD can provide the needed technology to meet the ever-increasing demand on the diminishing work force.

TOOLS OF THE TRADE Without DESKPAD



With DESKPAD



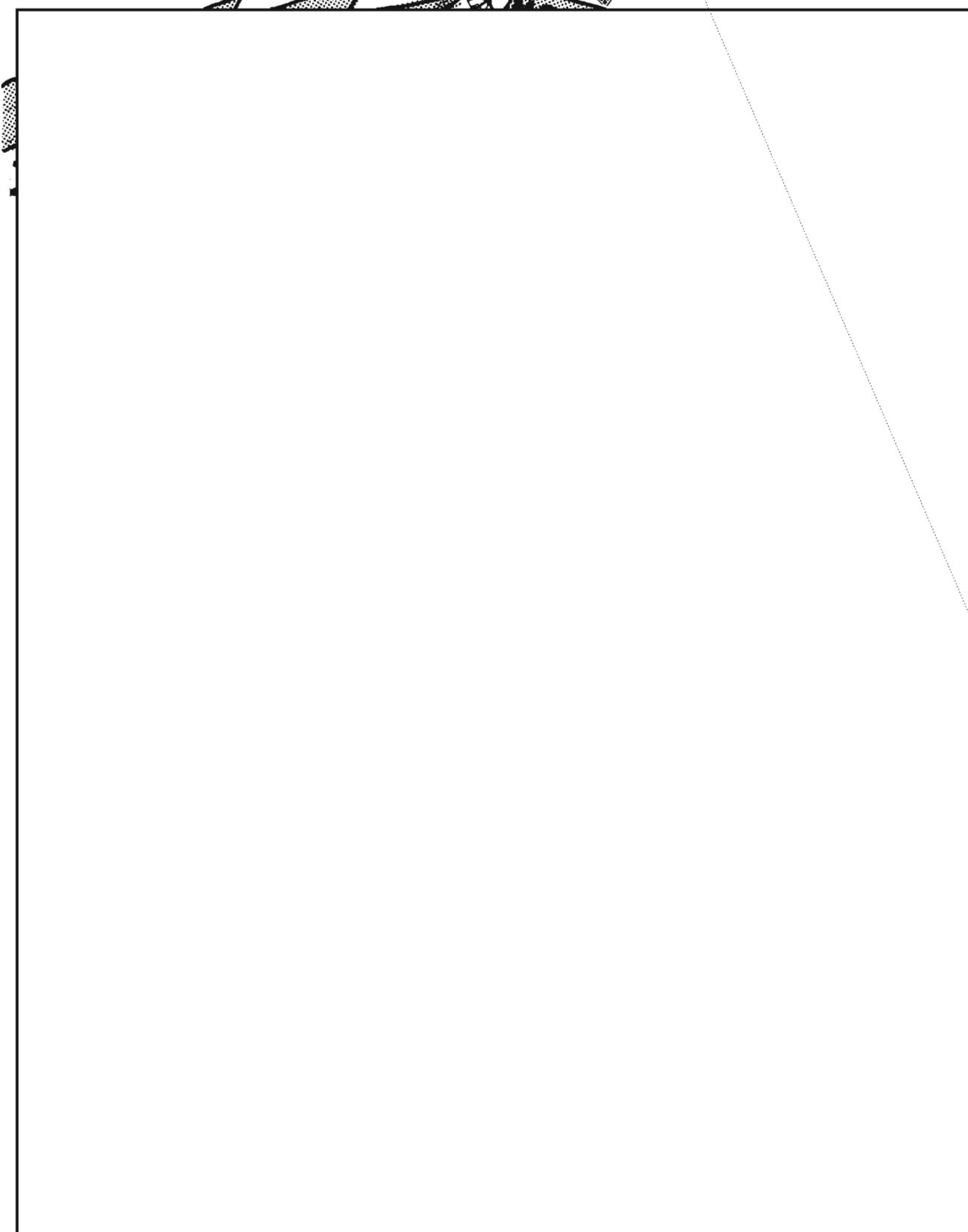
Solution to NSA-crostic No. 1
(CRYPTOLOG, October 1975)

[redacted] "Uncertain Origins": P.L. 86-36

"The analysts I met were anything but desolate. Working in a pair of tottering quonset huts at tables they had made themselves and harassed by wind, dust, and erratic electricity, they saw themselves in league against the forces of evil -- variously embodied in the VC, the weather, and NSA."

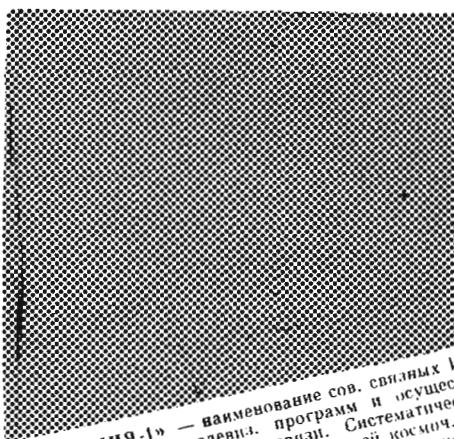
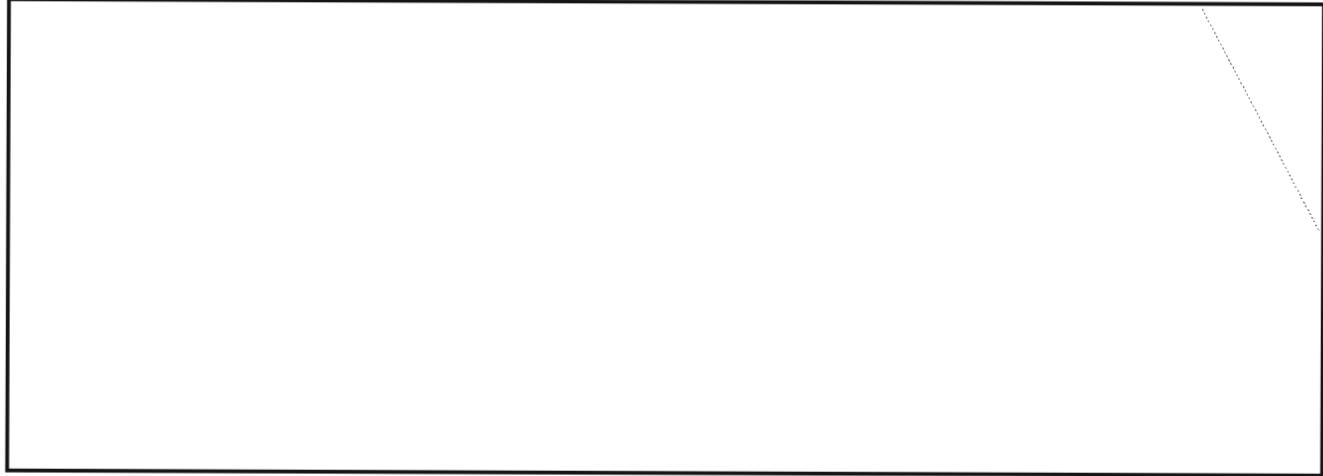
(UNCLASSIFIED)

~~TOP SECRET UMBRA~~



~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

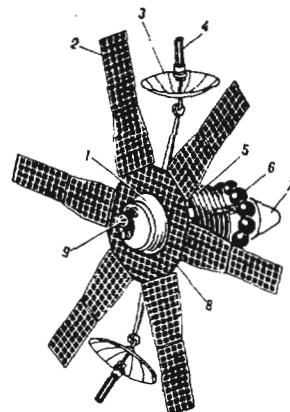
~~TOP SECRET UMBRA~~

«МОЛНИЯ-1» — наименование сов. связных и для ретрансляции телевиз. программ и осуществляется с 1965: входит в состав системы дальней связи. Систематически бывают в совместно с наземными приемными радиотел. Имеют сильно вытянутую эллиптическую орбиту над Северным полушарием ок. 40 тыс. км. (для пунктов, находящихся на территории Сев. полушария) обеспечивает сеансы связи 8—10 час. «М.-1» имеет двигат. установки для синхронизации с целью изменения времени весн. ИСЗ. Ретранслятора «М.-1» (40 ат) существенно более мощный, чем у предыдущих ИСЗ. В полете осуществляются связь с землей и с другими ИСЗ. В СССР впервые запущены в космос в мае 1965 г. Первый ИСЗ «М.-1» запущен 23 апр. 1965 г. и регулярно обеспечивал обмен геодезической информацией между Москвой и Владивостоком. Второй ИСЗ «М.-1» запущен 25 апр. 1966 г. и осуществил связь с Европой. Третий ИСЗ «М.-1» запущен 14 окт. 1966 г. и осуществил связь с Францией. С помощью телевиз. аппарата «М.-1», с мая 1966 г. передаваемого изображение в цвете, впервые получено цветное изображение Земли в глобальном масштабе. Всего запущено до 4 окт. 1970 г. 13 ИСЗ «М.-1» и телевизоров СССР и других стран.

MOLNIYA-1. Name of Soviet communication satellites intended for relaying of TV programs, and long-distance telephone and telegraph communication. These satellites have been used since 1965. They are part of the *Orbita* space system of long-range radio communication. These satellites travel on an elliptical orbit of great eccentricity with an apogee of about 40 thou. km in the Northern hemisphere. With an orbit of such shape (for points located in the USSR and other countries in the Northern hemisphere), communication may be maintained for up to 8–10 h at a time. *Molniya-1* satellites have rocket engines to make CORRECTIONS OF ORBITS in order to alter the hours of available communication time and to synchronize the travel of several satellites moving round the Earth at the same time. The output power (40 W) of the relay transmitter on *Molniya-1* is considerably higher than that on other known communication satellites. The satellite's design provides in-flight orientation of solar batteries towards the Sun and of the parabolic antenna towards the Earth.

The 1st *Molniya-1* satellite which was launched on April 23, 1965, regularly provided TV and telephone exchange between Moscow and Vladivostok for many months. On October 14, 1965, the 2nd *Molniya-1* satellite was launched for experimental 2-way long-distance TV, telephone, and telegraph communication; the 3rd *Molniya-1* satellite, launched on April 25, 1966, besides serving for communication and TV broadcasting between USSR ground stations, was also used for an exchange of TV programs between the USSR and France, this including colour TV. Since May, 1966, TV

Molniya-1 communication satellite.
1—sealed body; 2—solar battery; 3—high-gain antenna; 4—Earth sensor for antenna orientation; 5—radiative cooler; 6—working fluid for minor corrections of flight path; 7—correction engine; 8—heater panel; 9—Sun sensors.



equipment on board the *Molniya-1* satellites yields images of the Earth as seen from altitudes of 30,000–40,000 km, which contain information about cloud pattern in globular scale; a colour photo of the Earth taken from space was produced in 1967. By August 1, 1968, 13 *Molniya-1* satellites have been placed into orbits to provide regular communication and TV broadcasting over the territory of the USSR and other countries.

Kosmonavtika, V. P. Glushko, Editor-in-Chief, Moscow, 1970 (2nd edition, expanded); *The Soviet Encyclopedia of Space Flight*, G. V. Petrovich, Editor-in-Chief, Moscow, 1969 (translation of 1968 edition of *Kosmonavtika*).

(UNCLASSIFIED)

~~TOP SECRET UMBRA~~

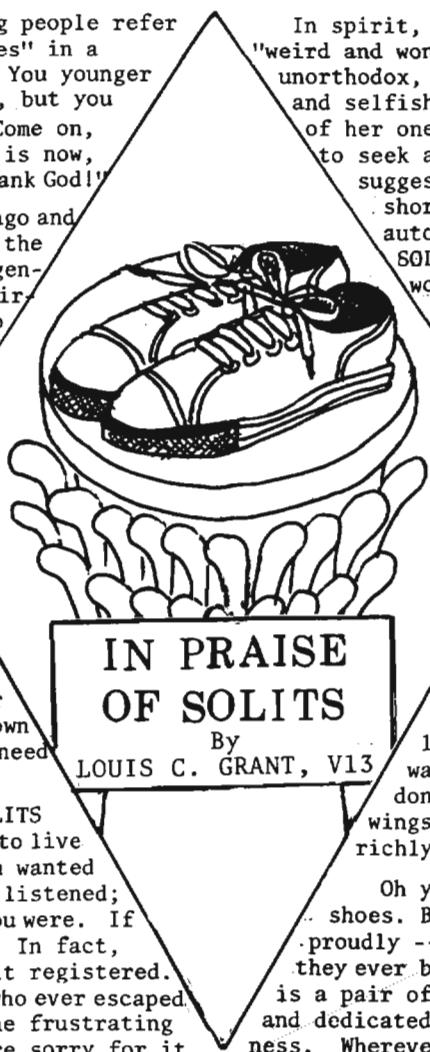
UNCLASSIFIED

I am sick to death of hearing people refer to "Some Old Lady in Tennis Shoes" in a frivolous or disparaging tone. You younger readers may not know any better, but you older hands certainly should. Come on, people! My appraisal of SOLITS is now, as it was then, very simply, "Thank God!"

I first met SOLITS 25 years ago and she amazed me. She was at once the Agency's computer system, the Agency's conscience, the Agency's spirit, and the Agency's respect. No matter where I looked, she was there: armed with the simplest tools, garbed in her idiosyncrasies, resolute in her manner, doing her thing.

SOLITS embodied all the basics of a computer: *memory bank* (she never forgot anything); *data storage* (she never got rid of anything); *retrieval* (she knew where everything was); and *rapid access* (she had instant opinions). All this and she was seldom down for maintenance, she generated her own data input, and she didn't even need air-conditioning to operate.

Like any good conscience, SOLITS was frustrating and at times hard to live with. She was there whether you wanted her or not; she nagged until you listened; and she didn't give a damn who you were. If she had an opinion, you got it. In fact, you got it over and over until it registered. And I know of no Agency senior who ever escaped the determined SOLITS touch. The frustrating part was that you inevitably were sorry for it when you failed to heed her counsel.



In spirit, SOLITS personified the phrase "weird and wonderful." Professionally she was unorthodox, crotchety, jealous, suspicious, and selfish. She was the undisputed ruler of her one-desk kingdom. You were free to seek a request, but you never dared suggest how she might grant it. In short, a royal pain. Yet under that autocratic armor was a true Queen. SOLITS reigned over her younger co-workers. She lent them money, befriended the lonely, counseled the unknowing, ministered to the sick, and comforted the bereaved. But always with an air of noblesse oblige that never betrayed her inner feelings. Indeed a regal gem.

SOLITS was deeply respected for one very simple reason: she worked. The general excellence of her effort and her profound dedication are manifested in every success the Agency ever had. SOLITS never sought the spotlight, but you can bet the script was based on something she had done. And she was always in the wings ready to cue the front man. She richly deserved the applause.

P.L. 86-36

Oh yes, she really did wear tennis shoes. But the Agency has stood in them -- proudly -- ever since the ribbon was cut. If they ever build a museum here, I hope there is a pair of bronzed tennis shoes enshrined and dedicated to the First Lady of our business. Wherever you are, SOLITS, my professional respect and gratitude are with you.

DEPARTMENT OF GOLDEN OLDIES

Most Golden Oldies were apparently written by Anon., but the author of the following one is known: NSA'er Dr. [redacted] who retired in 1972.

Notes on Blue Russian

Blue Russian is a dialect spoken by about 16 persons scattered widely over the Valdai Hills. It is called "Blue Russian" because of the characteristic tint of the faces of speakers as they hold their breath while pronouncing imperfective and frequentative verb forms.

Just to give you an example: BIT' means "to beat"; POBIT' means "to do a little beating", and its imperfective is POBIVAT'. ZAPOBIVAT' means "to begin to do a little beating," and its imperfective is PEREZAPOBIVYVAT'. This last verb, interestingly enough, has a special frequentative form: namely, PEREZAPOBIVYVYVOVAT', which may be rendered "to make a practice of making fresh starts on projects involving a limited amount of beating." Hence, the handy ex-

pression ShKOL'NO-DVOROVYJ PEREZAPOBIVYVYVUVU-ShchiJ, "schoolyard bully."

The 16 speakers of Blue Russian are under constant observation so that scientific data on the incidence of linguistic strangulation may be obtained. Their zero birth rate during the past 50 years has aroused comment. But it is still too early to assert, with Hammerkopf, that "Blue Russians are too exhausted from talking to be able to propagate." This is dogmatic theorizing in the worst tradition of the University of Berlin.

As this goes to press, it has been learned that two of the 16 Blue Russians have died. It seems that one of them, a devoted member of the Pedagogico-Organizational Committee of the 7-year School of Staraya Russa, suffocated in the midst of an impassioned speech on schoolyard bullies; and his wife died of a similar cause shortly afterwards while talking to friends about making fresh starts on projects involving a limited amount of simplification of Blue Russian.

National Cryptologic School Offers Course-Equivalency Tests

The National Cryptologic School offers employees the opportunity to earn course credit by taking EQUIVALENCY TESTS. Frequently, through experience or self-study, a person has already learned the material presented in a course. If this knowledge can be demonstrated, time and energy required to take a course can be saved. Equivalency tests may be scheduled through the cognizant NCS department. They are available for the following courses:

EA-100	Introduction to COMINT/ELINT Technology
EA-030	Introduction to Multichannel Technology
EA-100	Basic SIGINT Technology
EA-200	SIGINT Instrumentation and Measurements Techniques
EA-201	Communications Signals Measurements and Analysis Techniques
EA-202	ELINT Measurement and Analysis Techniques
EA-380	Advanced ELINT Collection/Analysis

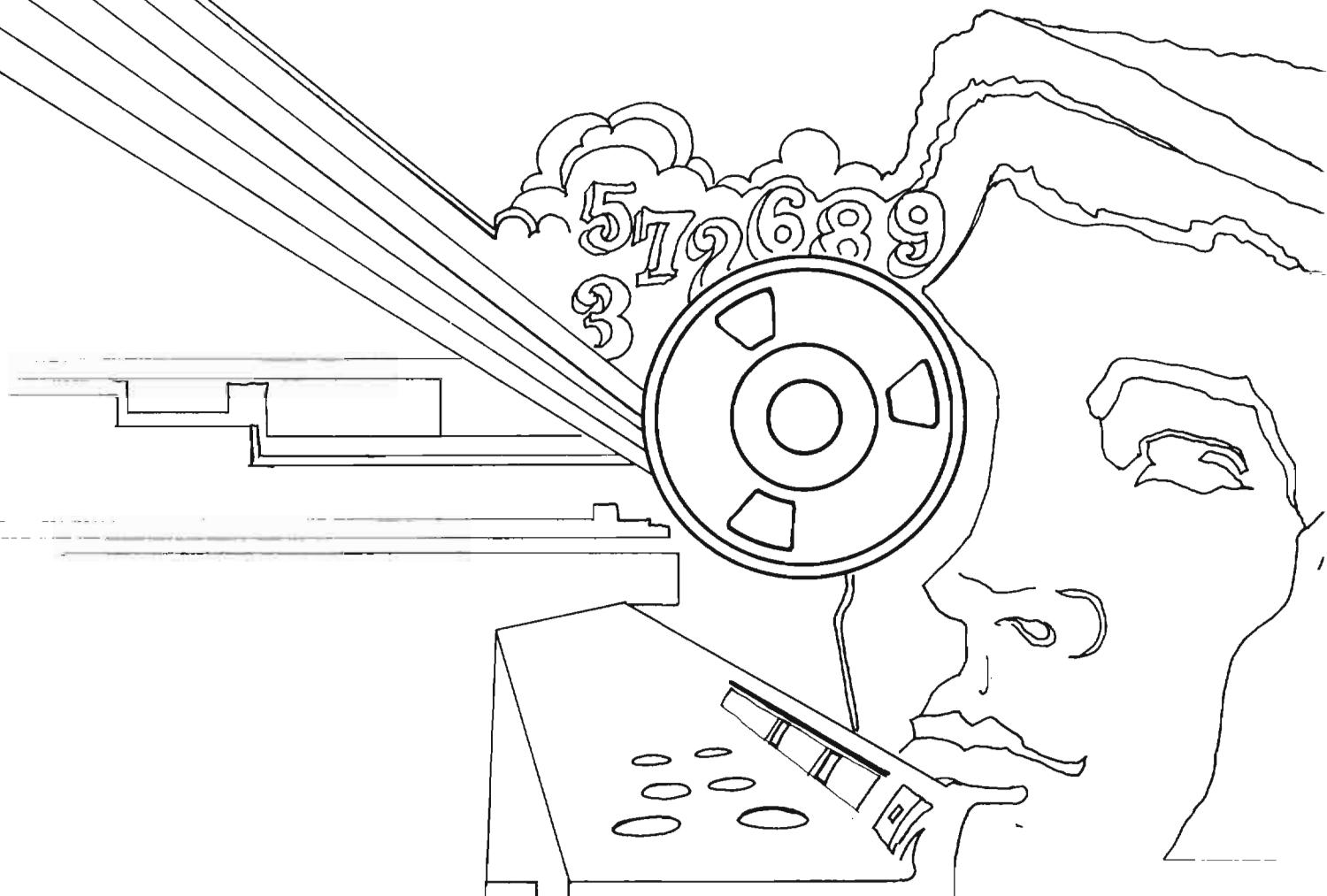
Cognizant department: E23, 8198s



ED-210	Tests and Measurements Cognizant department: E42, 8047s
ET-100	Introduction to Electronics
ET-260	Solid State Devices and Applications
ET-261	Digital Concepts Cognizant department: E24, 8975s
MA-400	Introduction to Computer Science Mathematics
MP-1B5	CDC 6600 Series System Software
MP-1B6	CDC 6600/7600 Advanced Technical Skills
MP-1C5	UNIVAC 494 RYE System Software
MP-1C6	UNIVAC 494 Advanced Technical Skills
MP-1D6	IBM 360/370 Advanced Technical Skills OS
MP-1E5	UNIVAC 1108 System Software
MP-1G5	Project HOLDER - UNIVAC 494 System Software
MP-1H5	Burroughs 6700 System Software
MP-1K6	CDC 6600/6700 Advanced Technical Skills (IDA)
MP-154	Introduction to Computer Systems Software
*MP-160	Introduction to Computer Science
MP-166	FORTRAN for Operators
*MP-188	APL Programming
*MP-277	FORTRAN Programming
*MP-230	COBOL Programming
*MP-242	PL/I Programming
*MP-243	Burroughs Extended ALGOL Programming
*MP-248	BETA Programming
*MP-267	POGOL Programming
*MP-335	IBM 370 Programming
*MP-368	IBM 370 Job Control Language (JCL)
*MP-375	PDP-11 Programming
* Toy problem also required.	
Cognizant department: E21, 8555s	
TA-200	Intermediate Traffic Analysis and Technical Reporting
TA-261	Computer Aid to Traffic Analysis
TA-361	Air Defense Technology and Traffic Analysis Cognizant department: E14, 8017s
TG-126	Target Studies - Mainland Southeast Asia Cognizant department: E12, 7119s

- A grade of "P" is assigned for passing the course through an equivalency test. Grades of "F" are not recorded. Aspirants may take the test only once.

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~