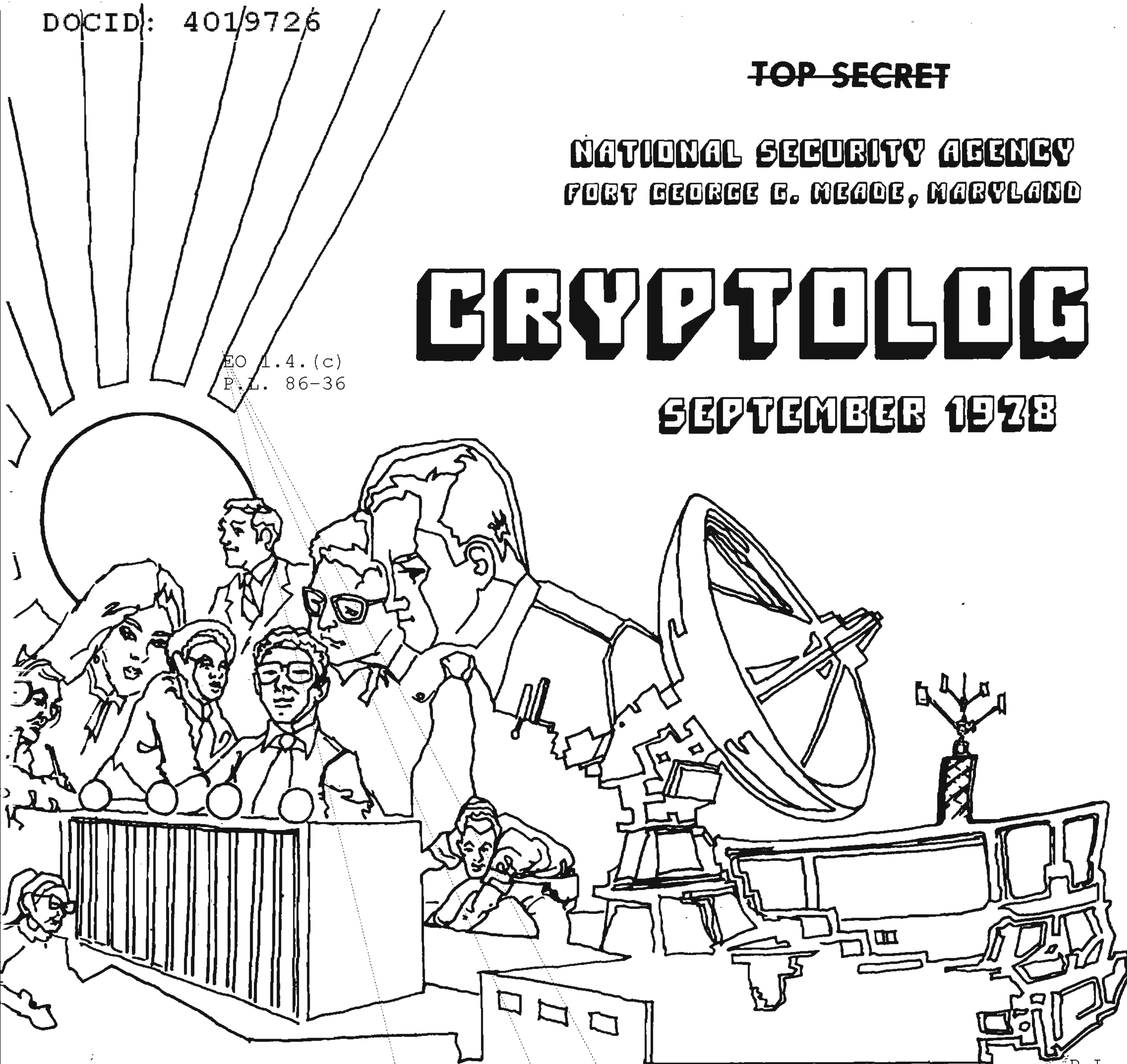
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

SEPTEMBER 1978

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



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

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

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,

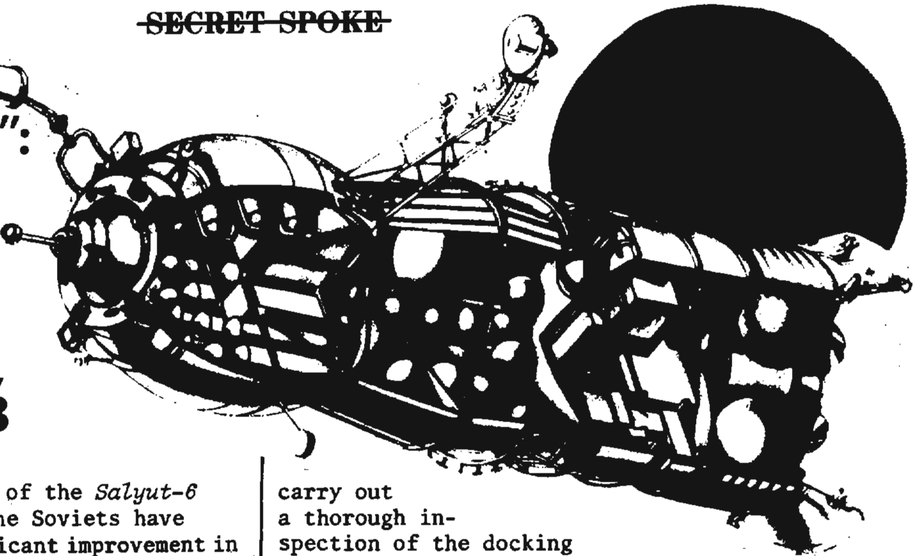
for the Personnel of Operations

VOL. V, NO. 9 SEPTEMBER 1978

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

"PROGRESS-1": SOVIET SPACE STATION REFUELING

John Cahill, A433



With the creation of the *Salyut-6* space station, the Soviets have achieved a significant improvement in the design and function of a space vehicle's propulsion system. There are two types of engines on the *Salyut* station: huge, powerful thrusters for raising the station to a higher orbit and for making orbital corrections; and smaller engines for station orientation on the earth or sun. On all previous stations (and on all *Soyuz* spacecraft) the power for each of these engine types was different. The large thrusters worked on a dual-component fuel and had their own separate tanks for fuel and oxidizer. The small thrusters, on the other hand, used a single-component fuel and likewise had their own separate storage tanks.

The *Salyut-6* station, however, has a single dual-component fuel for both its large and small thrusters and fuel tanks for these engines. This new consolidated propulsion system, which [redacted] can now be refueled by a "tanker" spacecraft, and thus the *Salyut* space station can remain in orbit for longer and longer periods of time. Soviet cosmonauts have [redacted] with the successful refueling of *Salyut-6*, the [redacted] has become a reality and ensures continuous manning by Soviet cosmonauts.

The *Soyuz-26* crew, Commander Lieutenant Colonel Yurij Romanenko and Flight Engineer Georgij Grechko, had successfully docked at the aft end of the orbiting *Salyut-6* space station on 11 December 1977. After transfer into the station, the cosmonauts checked out and activated the onboard equipment. Several days later, Flight Engineer Grechko exited the station through the transfer hatch at the forward end of the station, in a special space suit, to carry out a thorough inspection of the docking mechanism which was thought to be damaged by the *Soyuz-25* crew. *Soyuz-25* cosmonauts, Commander Lieutenant Colonel Vladimir Kovalenok and Flight Engineer Valerij Ryumin, had maneuvering difficulties during the approach and docking phase of their flight and on 10 October 1977 had to abort their mission after three unsuccessful attempts for a "hard dock" onto the station. The *Soyuz-26* cosmonauts had docked their spacecraft at the station's second or aft docking port -- a totally new concept in Soviet space station design. All previous stations had only one docking port at the forward end of the station.

After about 30 days on board the station, the *Soyuz-26* crew was visited by the crew of *Soyuz-27* under the command of Lieutenant Colonel Vladimir Dzhanibekov and Flight Engineer Oleg Makarov. The *Soyuz-27* spacecraft successfully docked at the forward docking port (which, it turned out, had not been damaged by the *Soyuz-25* crew's abortive docking attempts), and now, for the first time, a *Salyut* space station had spacecraft docked at both ends and was manned simultaneously by two separate crews. After five days together, the *Soyuz-27* crew departed the station and returned to earth, not in their own *Soyuz-27* spacecraft but in the *Soyuz-26* craft. This was yet another "first" for Soviet cosmonautics.

The now vacant aft docking port was soon occupied by a modified *Soyuz*-type spacecraft called *Progress-1*. This new vehicle brought needed supplies for the station's crew and also tanks loaded with fuel and oxidizer to replenish the *Salyut*'s own fuel tanks. [redacted]

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

The spacecraft can carry up to 1,300 kilograms

This article represents, for the most part, a compilation of information from open-source Soviet space literature. The overall classification of the article, however, is ~~SECRET SPOKE~~ [redacted]

J.C.

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

of dry cargo (including water in containers) and up to one ton of fuel components and compressed gas. Its net load is around 33 percent of the gross weight of the spacecraft.

There are three compartments in *Progress-1*: a cargo compartment, a compartment housing the station-refueling tanks, and an instrument-assembly compartment. The cargo compartment is [redacted] of a *Soyuz* and is 6.6 cubic meters in size. Special racks were created to house the various "cargo" needed for resupplying the station's crew. Cargo includes sets of clothing, film cassettes, magnetic tapes, new medical and scientific-research instruments, and such large and heavy items as new air regenerators. The compartment itself is pressurized with a usual atmospheric pressure of 760 mm of mercury and a temperature of 3° to +30° C. On the outside of this compartment are the main fuel lines which are fed into the docking assembly. These fuel lines are similar to those on *Soyuz* spacecraft, but they have, in addition, two hermetically sealed connectors which enable the pumping over of fuel from the refueling tanks in the "tanker" spacecraft's "refueling" compartment after docking with the station.

[redacted] this compartment does not need life-support systems, powerful radiation and heat shielding, or a parachute system (since no part of the *Progress-1* was to be returned to the earth).

The final compartment -- the instrument-assembly compartment -- has three sections: a nonpressurized section where part of the mooring and orientation engine system and the fuel tanks for this system are located; a pressurized instrument section; and an assemblies section with the approach and correction propulsion system found on all *Soyuz*-type spacecraft.

The *Progress-1* cargo spacecraft is launched by the same boosters used to launch all *Soyuz* spacecraft. After orbital insertion, radar antennas of the approach and docking system (installed on the cargo and instrument-assembly compartments) are deployed. The Flight Control Center monitors the spacecraft's orientation via two television cameras installed on the outer hull of the cargo compartment. One of the cameras shows the space station during the approach maneuver, so that the ground can follow the approach and docking procedures if necessary. The *Salyut* station's crew can view the approaching cargo spacecraft via the station's stern-mounted television camera. Special lights on *Progress-1* aid the crew in determining the spacecraft's position relative to the station on both the day and night side of the planet. These lights are uniquely arranged on retractable rods mounted on the outside of the "cargo compartment." One light is in front, with two lights behind it on the sides. When the approach and docking is going normally, the lights appear to be in a straight line. If there are any contingencies during this procedure, the crew can stop the docking process.

Progress-1 successfully docked with the station on 22 January 1978, but the actual fuel transfer did not occur until 2 February.

Within the docking mechanism of the *Progress* vehicle (as in all *Soyuz*-type spacecraft) there are both electrical and hydraulic lines which automatically connect with the station after docking. [redacted] valves the fuel is moving to the engines. There are numerous buttons on the control panel for sending the required commands to move the fuel.

After the *Progress-1* docked with the *Salyut-6* station, the two fueling lines -- one for oxidizer, the other for fuel -- were connected to the station; the hermetic seal of the lines was checked for leaks; and the pressure in the station's tanks was lowered. First the fuel and then the oxidizer was pumped from the "refueling" compartment into the station's tanks. After the refueling operation was completed, the fueling lines were purged and vacuum-evaporated with the use of the compressed nitrogen gas.

Besides fuel replenishment, the station's atmosphere was renewed with air from tanks in *Progress*'s "refueling" compartment. This operation was necessary to replenish air lost during the earlier EVA (extra-vehicular activity) and because some air is lost during various garbage-dump operations performed by the crew through a special airlock. [redacted]

Progress-1 was also used as the first "space tug." Its own propulsion engines were switched on and the spacecraft was used to boost the *Salyut-6* station into a higher orbit.

One final experiment was conducted with *Progress-1* before it was allowed to burn up in the earth's atmosphere. After undocking, a test check of the spacecraft's own reserve automatic search and approach system was made. The test was successful and on 8 February 1978 *Progress-1* disintegrated as it reentered the earth's atmosphere.

~~(SC)~~

LETTERS TO THE EDITOR

P.L. 86-36

To the Editor, CRYPTOLOG:

The following letter was prompted by Eugene A. Gilbertson's letter to the editor (CRYPTOLOG, June 1978) with regard to [redacted] earlier article "What Ever Happened to COPES?" (CRYPTOLOG, January 1978).

Now that COPES has been with us for a number of years I shall make again an observation which originally was a theoretical warning (properly discounted, since in many people's minds "theoretical" is synonymous with "most likely wrong") but which is now capable of observation and verification.

I accept the fact that COPES has had an influence on distribution of effort and resources. How sure are we that it has provided a reasonably objective base for such allocation decisions? My concern stems from admissions made privately and off the record that when COPES objective satisfaction is low we change the objectives so that the rate of satisfaction looks better, and when things look too good we add objectives to preclude a cut in resources. This should not be surprising; it is a natural response and could have been anticipated (theoretically) as the way people react. If this is indeed taking place, consciously or unconsciously, the rate of objective satisfaction is more a measure of how well we have adjusted our objectives to some acceptable norm than a basis for collection resource allocation decisions.

I am not a strong opponent of COPES. It does give us a much better understanding of what collection is doing that we had in pre-COPES days. We must, however, be very careful as to how we use such data.

Donald Y. Barrer, P1

(U)

To the Editor, CRYPTOLOG:

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

I enjoyed your overlon... member SPELLMAN" (CRYPTOLOG, Jul...), concerning the long-defunct Agency project which had the twin aims of training people [redacted] The first half of the task is no less preposterous today than it was when proposed 20 years ago. The second half, however, is, on the surface at least, a reasonable one, which was nevertheless ultimately abandoned as being beyond the capabilities of the persons involved. This resolution of the problem, you might be interested to know, was not limited to the NSA task group.

In the article from the 1957 Soviet encyclopedia quoted in your article, Stenotypy is treated as a major office-skills advance, and several advantages over "ordinary stenography" are cited: shorter training time, absence of distortion at high transcription speeds, reduced fatigue for the transcriber, etc. Altogether an upbeat view.

Contrast this with the parallel piece in the 1976 edition of the same encyclopedia. In a much briefer article, Stenotypy is succinctly described, then evaluated with this final comment:

> "Stenographic machines have not been widely accepted. Because of the development of magnetic sound-recording technology, in particular the Dictaphone, their production was dropped in the 1950s."

So cheer up. You're in good company.

David H. Williams, P16

~~(S-CCO)~~

NONSECRET ENCRYPTION (Public Key Cryptosystems)

[redacted]

"We stand today on the brink of a revolution in cryptography." So begins a paper entitled "New Directions in Cryptography" which appeared in the November 1976 issue of the *Transactions on Information Theory* journal published by the Institute of Electrical and Electronics Engineers (IEEE).

We shall examine the developments to which the authors of that paper refer, discuss the potential for cryptographic revolution, and mention some effects which may be felt at NSA.

As early as 1969, mathematicians at GCHQ were considering the possibility of secure encipherment without the necessity of a key being held commonly between sender and recipient. To do this the mathematical properties of "finite fields" were to be employed. It turns out that in finite fields, which are much the same as the real numbers but which are better adapted for computer use and for key production, it is easy, given a and x, to calculate the expression a^x. However, the problem of recovering x when given a and a^x is extremely difficult to solve. One's intuition suggests that, as in the reals, an approximate solution might be satisfactory but the finiteness of the field precludes this. We see here a pair of "inverse" tasks, one of which (exponentiation) is easily performed while the other (solving the equation $y = a^x$ for x means taking the "logarithm" of y) is very difficult.

The idea, first announced by J. H. Ellis in a GCHQ paper, is to create a system in which the cryptographer may use only "easy" algorithms while the analyst is obliged to solve a "hard" problem. Suppose that we wish to send a message to a friend but we have no mutual cryptovariable. Suppose further that we have a small computer capable of performing finite field exponentiation. We may "randomly" select an integer x_1 and calculate a^{x_1} for some a which is fixed and known both to our ally and to the enemy. We transmit $y_1 = a^{x_1}$ (as a string of bits) across an insecure channel, so that both our ally and the enemy may be assumed to be in possession of y_1. The only secret we have is x_1 and even our ally doesn't know x_1.

At the other end our friend receives our bit stream and prepares himself for communication by choosing randomly another integer x_2, calculating $y_2 = a^{x_2}$, and transmitting the corresponding bit stream to us. We assume that the enemy also acquires knowledge of y_2. Now we are ready to determine the key which will be used for encipherment: we calculate $y_2^{x_1} = a^{x_1 x_2}$ and use the corresponding bit stream as key. Our friend is able to calculate the same key, using $y_1^{x_2}$. But the enemy, who knows a, y_1, and y_2, has no convenient way to calculate $a^{x_1 x_2}$ unless he can, for example, determine x_1 as the logarithm of y.

This novel method, called nonsecret encryption by Ellis, received scant attention in the intelligence community because there was no recognized application for such a system. One advantage of this system is that there is no need for key distribution; on the other hand, there are several problems of implementation. First, there is the matter of selection of the "randomly chosen" integers: maybe certain choices are weaker than others. Certainly the choice $x = 1$ would be totally insecure and one should consider the possibility that the product $x_1 x_2$ will be a weak choice even though x_1 and x_2 are not weak. Then there is the problem of errors in channel transmission. To ensure that the enemy cannot solve our system by brute force, the "finite field" must be very large (allowing a large range of inequivalent choices for x_1 and x_2) and so the bit streams y_1 and y_2 are very long. For successful communication, both y_1 and y_2 must be received with complete accuracy. At the very least this may require some error-correcting capability and the capacity of the channel must be considered, as well as the capability of the computer at each end of the link. The fact that a great deal of computation must be performed will also limit the bit rate at which transmission can be effected. Finally, there is a serious problem with authentication: since the enemy knows our system, he will be able to establish communications with us (just be sending some $y_3 = a^{x_3}$) unless we can check on his identity.

We in the intelligence community have become accustomed to holding a monopoly on useful advanced cryptologic knowledge, so it is with surprise and apprehension that we have witnessed in recent years an increasing interest in cryptology on the part of American academicians*. With the advent of digital technology in the storage and transmission of vast quantities of data, it was inevitable that security questions would arise. Engineers, mathematicians, and computer scientists see in this area a relatively uncharted

[redacted]

Charles Sullivan,

[redacted]

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

field in which new and important results may be available without the obligation to assimilate enormous bodies of information. Efforts to find and analyze better algorithms could easily lead to rapid advancement and recognition for academic-based researchers.

One of the first opportunities for scholarship arose with the development of the Data Encryption Standard (DES). Several papers have been written both by university researchers and by Bell Laboratories personnel, which are critical of the algorithm or of the size of the cryptovariable. The authors express their anxiety about the (classified) principles underlying some of the design. While the published analyses are not of the quality one would expect to find from experienced crypto-knowledgeable analysts, the intelligence and perception of the authors is easily recognized.

Foremost among the investigators is Martin Hellman, a bright young associate professor of electrical engineering at Stanford University. Widely known among information theorists for his scholarship, Hellman has published several recent articles on cryptology. With his student Whitfield Diffie he published "An Exhaustive Cryptanalysis of the NBS [National Bureau of Standards] Data Encryption Standard" in *Computer* magazine, extending an earlier "Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard" which they and five others published at Stanford. It was the Hellman-Diffie duo which, in *New Directions in Cryptography*, introduced to the public the notion of a "trapdoor function." Hellman's ability to attract press coverage has caused their ideas to receive considerable attention. Last year an episode of a popular television series featured a "code expert" who spoke knowingly of trapdoor functions.

The interest of Hellman and Diffie in criticizing DES is clear. If they were able to destroy the confidence of industry in the DES algorithm, then perhaps their own ideas would gain recognition as an effective security scheme, with a resulting financial windfall. Already Hellman, Diffie, and another Stanford graduate student, Ralph Merkle, have applied for a patent on a device based upon their publication. Taking advantage of the reluctance of NBS (and NSA) to discuss the strengths of DES and the weaknesses of the new approach, articles have appeared which strongly suggest that the Hellman-Diffie algorithms are "unbreakable for all practical purposes" and that the DES has "fatal flaws" which allow a successful attack to be mounted for between $20 and $5000 per message, with an elapsed time of "anywhere from six minutes to 12 hours." One of the more sensational of the articles alleged that "what is beyond dispute is the fact that any system employing the same key both for encoding and decoding is just too awkward for everyday use" (Robert C. Cowen, in *Technology Review*, December 1977).

A public key cryptosystem (this is the name given by Hellman and Diffie to the concept which we know as nonsecret encryption) is envisioned as a convenient communication scheme for a large loose network. Potential users would be financial and industrial organizations. We may think of a nationwide net of banks and brokerage houses, any pair of which may at some time have a desire to communicate securely. Each user K will have a pair of algorithms, E_K for encryption, D_K for decryption, such that, for any message m, $D_K E_K m = m$. Furthermore, D_K and E_K are algorithms which may be accomplished quickly, but it must be that knowledge of one of the algorithms does not allow the other to be deduced. Such a system is really a set of "trapdoor one-way functions," in the sense that it is computationally infeasible to find D_K given E_K. The algorithms E_K are made public. Thus anyone desiring to transmit a message to K may look up the enciphering algorithm and send the message $E_K m$. Only user K will be able to decrypt the message because only user K is in possession of the algorithm D_K.

Immediately one is forced to do something about authentication, since the receiver has no way to verify the identity of the transmitter of a message. Fortunately, there is a neat solution. Suppose that, for all K, the algorithms D_K and E_K also enjoy the property that $E_K D_K m = m$ for all m. Then if A desires to send a message m to B, he first applies the secret decryption algorithm D_A followed by the public algorithm E_B. When B receives the message $E_B D_A m$, he first applies his secret decryption algorithm D_B followed by the public algorithm E_A. The result is $E_A D_B E_B D_A m$. Since $D_B E_B x = x$ for all x, this simplifies to $E_A D_A m = m$, so that the intended recipient can indeed recover the message. Only he can decipher the transmission $E_B D_A m$, for only he has the secret algorithm D_B. Additionally, when he has recovered m, he knows that it was indeed A who sent the message, for only A has the secret algorithm D_A which must have been used (unless by chance some other algorithm could convert m to $D_A m$; this can occur, but with small probability, one would expect).

For this attractive and simple concept to succeed we shall require the existence of a suitable family of trapdoor functions. Several candidates have been proferred and an intensive search is underway to find others. The first to attract national attention was embodied in an MIT paper, "On Digital Signatures and Public-Key Cryptosystems," by Ron Rivest, Adi Shamir, and Len Adleman, which appeared in April 1977. In Martin Gardner's popular "Mathematical Games" column in *Scientific American*, August 1977, appeared a "challenge cipher" based on the MIT paper. A prize of $100 has been offered to the first solver of the cipher. The family of trapdoor functions is based on the difficulty of factoring large numbers and will be detailed below.

On the heels of these advances, the IEEE scheduled an international symposium on information theory, to include two sessions on cryptography, at Cornell University in October 1977. Interest was heightened when the organizers of the symposium received a letter from an NSA employee which suggested that the symposium might be in violation of laws. This letter and the responses of Hellman and others were publicized in the widely read *Science* magazine. The sessions on cryptology were well attended, especially the presentations of Hellman and Rivest. Three NSA employees attended these sessions. Two Stanford graduate students, Merkle and Stephen Pohlig, did not present their work for fear of legal action. At one of these sessions, Hellman remarked that he and his associates would like to analyze (and publish the analysis of) some of the "classical" cryptographic systems. He specifically mentioned rotor devices and "Hagelin." Both Hellman and Rivest have presented their ideas at meetings of scholars throughout the country. NSA employees have attended a talk by Hellman at Catholic University and a presentation by Rivest at the Applied Physics Laboratory. We should expect that considerable research effort will be devoted to cryptology in the next few years.

Computational complexity is the area of mathematics which is most intimately involved in the search for trapdoor algorithms. It is an area which has blossomed with the development of high-speed computing equipment. The difficulty of a problem can be measured by the time required to solve the problem. In general, this will depend upon some parameter associated with the problem. For example, we can consider the time required to invert a square matrix of size n, where n is a positive integer. Naturally the time required will increase as n increases, but how fast does it increase? We say informally that a problem is in class P if there exists an algorithm to solve the problem such that the maximum time required to execute the algorithm is a polynomial function of the parameter. A precise statement would involve the notion of a Turing machine, which we choose not to introduce. A problem is in class NP (nondeterministic polynomial) if an algorithm exists, with time which is a polynomial function of the parameter, to solve the problem using a computer with an unlimited degree of parallelism. The class NP includes the class P but it is not known if there is indeed a problem in class NP which is not in class P. There is a large class of problems, known as NP-complete, which share the property that if any one of them is in class P, then $NP=P$. It would be very surprising if the equality $NP=P$ could be shown. At the moment the problems which are NP-complete are regarded as sufficiently difficult to resist solution if the parameter is chosen large enough.

The goal of the theoretical cryptologist, then, is to create a system so strong that to break the system the enemy analyst must solve a problem which is NP-complete. It must be realized that this is not an assurance of a secure system. There is, until a proof that $NP \neq P$ is found, a possibility that a fast algorithm exists to solve an NP-problem. Even if this is not the case, recall that the definition of class P was a "worst case" definition and it is conceivable that although no fast algorithm exists to solve the problem for all cryptovariables, perhaps a fast algorithm can be found which often, or sometimes, solves the problem.

For a curious example of the distinction between class P and class NP, consider the problem of assigning compatible roommates, given a group of people together with their lists of satisfactory partners. If two roommates are to be assigned to each room, a clever algorithm given by Jack Edmonds of the University of Waterloo will accomplish the pairing in polynomial time, but the same task when three are to share each room is known to be NP-complete.

Suppose that a traveling salesman who must visit n cities wishes to schedule his itinerary so as to minimize the mileage driven. This problem is NP-complete but there exists a fast algorithm to find a good, but not always optimal, route.

One NP-complete problem which has been suggested in connection with cryptographic schemes is known in some circles as the knapsack problem. A pertinent paper is by Merkle and Hellman, "Hiding Information and Receipts in Trap Door Knapsacks." Suppose that you publish a list of, say, 200 very large integers $a_1, a_2, \ldots a_{200}$ and accept communications as follows. I write out my message as a streams of 1's and 0's and break it up into groups of 200. I encipher each block by adding together the a_i which correspond to 1's in my message. Upon receipt of my message, you immediately decipher the text but the enemy cryptanalyst who intercepts the message is unable to decipher it. How is this possible? It seems that both you and the enemy have the same information: the sum of certain ones of a known set of numbers.

The secret behind this method of encryption lies in the choice of the 200 numbers a_i. Suppose that another set of 200 positive integers b_i has the property that for each $i > 1$ the number b_i is bigger than the sum $b_1 + b_2 + b_3 + \ldots b_{i-1}$ of all the preceding numbers. It would be very easy to decipher a message sent using these numbers to encipher: if the message is larger than b_{200} then the 200th bit of the message was 1, otherwise 0; if a 1, subtract b_{200} from the message and repeat with b_{199}, etc. In this case no security is afforded by the encryption procedure. The principle behind the knapsack scheme is for you to transform a simple case into a difficult case in such a way that only you know how to reconvert the difficult case into the simple case which readily yields a solution. As an example, suppose you select the five integers 171, 196, 457, 1191, and 2410. These numbers satisfy the criterion for simplicity. Now you choose as your cryptovariable the numbers 3950 and 8443 (in a real-life example, the numbers would be much longer). We require that the two numbers be relatively prime and that the second be at least twice as large as the largest of the previously chosen integers. It is easy to find a number x such that $3950x \equiv 1 \bmod 8443$; $x = 2550$. Multiplying our five integers by 2550 and reducing modulo 8443 we obtain the a_i: 5457, 1663, 216, 6013, and 7439. If I wish to transmit the message 11001 I just add 5457 + 1663 + 7439 = 14559 and send that number. Upon receipt, you multiply 14559 by 3950 and reduce mod 8443 to get 2777 which is easily deciphered in your simple scheme. The enemy analyst, not knowing the cryptovariables, faces the task of exhausting over all 2^{200} possibilities: or is there a better approach?

The proposed trapdoor function which has received the most attention is the MIT scheme which was featured in the *Scientific American* article and upon which the "challenge cipher" is based. Two positive integers s and r are published, with r large. To encrypt a digital message, it must first be broken into segments with each segment having fewer digits than r. To encipher a segment x the number $x^s \bmod r$ is computed; this is easily done using current technology. To decipher, only one cryptovariable is needed: an integer t such that $x^{st} \equiv x \bmod r$ for every x. For example, if r is prime, the condition is that st should be 1 modulo r-1, and t is easily determined if s has no factors in common with r-1. Because of the ease of determining t in this case, it is not good to allow r to be a prime. It is also weak to select an r with small factors. The most promising choice seems to be $r = pq$, the product of two large primes which are not close together and which enjoy certain other interrelationships. It is easy to find pairs of appropriate primes. If it should happen that x has a factor in common with r, the decryption algorithm may need modification. The strength of the method rests on the inability of the enemy cryptanalyst to factor r into its factors p and q.

Algorithms to factor integers have been developed recently which are substantially faster than those known before this decade, but the factoring of integers of, say, 100 digits is still well beyond the capability of current computers and known algorithms. It seems that a major (and quite unexpected) breakthrough would be required to factor a typical r of 100 digits in a reasonable time. If this is the best attack on the MIT algorithm then it may be regarded as secure under present conditions. It is not clear that this is the case. If the primes p and q are poorly chosen, special approaches, which would not do in general, may succeed. It is not the case that the time taken to factor is a function solely of the size of the factors.

There are a great many problems still to be solved before public key cryptosystems find widespread usage. We have already mentioned the low rate of transmission and the need for error-correction capabilities. Let us consider an application for which the scheme was intended: a large-scale financial network. The ability of any member of the net to communicate securely with any other is very difficult to realize using conventional cryptologic equipment, but it seems to be a requirement that each user have a computer with the capability of performing the necessary arithmetic operations and with the ability to acquire the public encryption data readily; reliability may be a problem. A central facility may be necessary for the storage of the data; this would introduce additional security considerations. Some provision must be made for the possibility of a compromised decryption algorithm and the ensuing loss of authentication for that user. It is conceivable that a user might intentionally allow his private decryption algorithm to become known so that he may subsequently disavow an unfortunate purchase or sale to which he had agreed. If electronic means are used for transactions, how can the recipient be prevented from making unauthorized copies of, say, stock certificates? For the authentication scheme which is used to guarantee signatures to be wholly satisfactory, legal precedents must be established and penalties specified.

When two algorithms are to be applied consecutively, it may well happen that two different moduli are involved. The message is blocked to allow the application of the first algorithm but it may happen that the integers which result are larger than the second modulus. Solutions to this problem have been proposed but are not entirely satisfactory; perhaps others will be forthcoming. Probably the

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

[redacted]

One application for which these algorithms seem well suited is the verification of identification or credit card data. The capture of one of the decrypting boxes by criminals would not allow the preparation of bogus cards with correctly coded data, as would have been the case if the decryption algorithm were identical with the encryption algorithm.

[redacted]

[redacted]

While public key cryptosystems are not likely to have a significant impact on American military communications in the foreseeable future, we must stay abreast of developments in the area. If implementation can be effected in inexpensive and reliable components, nonsecret encryption may provide secure communication in carefully chosen situations. [redacted]

~~(S - CCO)~~

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

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

NEWS OF THE CRYPTO-LINGUISTIC ASSOCIATION

On 18 May 1978 a large number of CLA members and their guests attended the annual banquet, which was held this year at the Sheraton-Silver Spring Motor Inn. CLA President Donald G. Lasley introduced those seated on the dais. They included the CLA officers and their wives; Joseph P. Burke, Commandant, National Cryptologic School; past CLA President Dr. James R. Nielson; Mrs. Annette Jaffe; and the evening's guest speaker, Dr. Robert T. Meyer. Dr. Meyer, a scholar of international renown in the field of Celtic studies, is currently Professor of Celtic and Comparative Philology at Catholic University, as well as Consultant on Celtic for the Library of Congress He gave an informative and witty talk on "Linguistic Exploration in West Kerry, Ireland."

1978 Jaffe Award

The Crypto-Linguistic Association's highest recognition of exceptional achievements in the field of language, the Sydney Jaffe Award, was given to [redacted] G9, with the presentation of an engraved plaque by Mrs. Annette Jaffe. Previous winners of the award, which was established in 1972 in memory of the CLA's founder, have been:

P.L. 86-36

1973 - Frances Blank and Dr. Mary Roberta Irwin
1974 - Norman Wild
1975 - [redacted]
1976 - John D. Murphy
1977 - [redacted]

1978 CLA Essay Contest

[redacted] awarded the following prizes to winners in this year's Annual CLA Essay Context:

1st Prize ($100) - [redacted] "The Iron Thumb" (CRYPTOLOG, March 1978)

2nd Prize ($50) - Jacob Gurin, "Words and the Intelligence Value of Conversations" (to be published in *NSA Technical Journal* and *NSA Cryptologic Spectrum*)

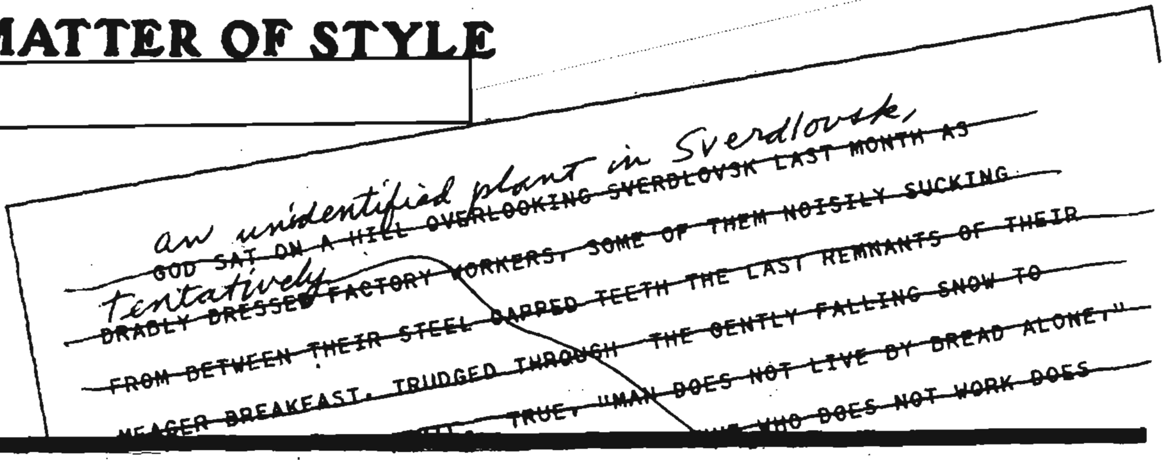
3rd Prize ($25) - A. J. Salemme, "A Linguist's Suggested Solution for the 'Language Problem'" (*NSA Cryptologic Spectrum*, Winter 1977, Vol. 7, No. 1)

Judges in this year's Essay Contest were: [redacted] Shirley Shamp, and Dr. [redacted] (U)

P.L. 86-36

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

A MATTER OF STYLE



"No passion in the world, no love or hate, is equal to the passion to alter someone else's draft."

H.G. WELLS

The idea for this article came about as the result of sending in a note to CRYPTOLOG, asking to have my name added to the distribution list. The editor, in replying to my request, added the postscript, "I like your style! Why don't *you* send in an article?" A nice compliment, taken at face value, but what exactly is meant by "style"? A quick look at Webster's yields this definition:

> "*style* a: mode of expressing thought in language, esp: a manner of expression characteristic of an individual, period, school or nation; b: manner or tone assumed in discourse; c: the custom or plan followed in spelling, capitalization, punctuation, and typographic arrangement and display."

This is not altogether helpful. There is an excess of verbiage contained in the definition but the reader remains essentially unenlightened. It is obvious that everyone is able to express thought in language, hence everyone has style. Granted, the method of expression by some leaves much to be desired, yet they still have style.

Of course, more is meant than just expressing thought in language. It should be done logically and progressively so that the reader can get from point A to point B without getting lost in a tangle of words. It must follow that NSA condones certain styles while rejecting others. Discovering the acceptable course is usually by trial and error, IS-250 and other courses notwithstanding. Even if a report has been prepared in the acceptable "style," there is always someone along the line willing and eager to change your report -- *your* report! -- in some manner. Since all of us are prone to error, some of these changes are warranted. Others are inexplicable.

USSID 300, that faithful old standby, does give the writer a better idea of what is expected. Hence, one finds on page 13 of the latest edition some guidelines listed after the word "Clarity":

> "Write product in a style that clearly and simply conveys the foreign intelligence information to the reader."

Here, at least, is some sense of what is wanted, i.e., a logically written report. To continue with the definition:

> "Be consistent in style, mechanics and grammar."

There's that word "style" again! If one assumes the "a" definition from Webster's, then a writer's style should never change at a given time, although it may change gradually through the course of his writing career. In a sense, we are back where we started. This being the case, let us press on:

> "Be specific in facts, background and analysis."

Good advice but, obviously, if you didn't write clearly and simply, this advice would be spurious.

> "Use short, plain, concrete words. Avoid passive verb phase."

Here we come to the crux of the matter. Here is the *style* (I use the word too) the Agency is looking for. It can allow for precisely what is needed -- a clear, concise, and logical report.

Unfortunately, there is one pitfall underlying these instructions. It allows all of us to fall into a set, lackluster form of writing. In essence, many product reports which leave this Agency read the same. The only real differences are the time of the activity and the entity involved. This kind of writing requires no creativity, but only the analyst's ability to fill in the blanks. Before irate report writers come storming in to protest, let me emphasize that this is not always the case. However, it does happen, and frequently.

All of us like to think we write well. Most of us can, given the chance. I know of analysts who deliberately pattern their writing with their editors in mind. What they have written is not necessarily their own but an aping of what the editor wants. Their own writing, not always bad, has been edited so often that they change their *style* of writing in self-defense. When a new editor appears and begins enforcing his or her interpretations about what a good report should sound like, the report writer simply apes the new style, again through trial and error. There is no pride in writing. It is simply a matter of getting the job done and moving on to something else.

It should be the job of all of us to encourage creative writing as far as possible under the guidelines established in USSID 300. All of us have an affinity for certain words. We should, however, resist the urge to emend another's report simply to replace their words with ours. Editing of reports is a required function and, done properly, can be used as a teaching experience for new writers. Emendations for the sake of preference, rather than improvement, are counterproductive. In such cases, the writer has three courses open to him. He can argue his case with the editor and try to get his wording restored; he can continue a silent war with the editor by continuing to submit his own textual preferences in the hope of slipping one by; or he can change his use of words, whether he agrees with the change or not. It is important to remember that the prime task of the editor is to strive for precision and clarity. If a report must be changed for reasons of clarity or "excess verbiage," the editor should try to discuss these changes with the writer whenever possible. Both will benefit from the experience.

(U)

SOLUTION TO NSA-CROSTIC No. 16, by David H. Williams, P16 (CRYPTOLOG, June 1978):

[redacted]

"Letter to the Editor," CRYPTOLOG, July 1977:

"My point was not to malign the fine women of our Agency or propose a process in violation of any . . . regulation, [redacted] However, the times are changing. . ."

(U)

News of the Communications Analysis Association

[redacted] P14

P.L. 86-36

Dues

Yes, dues. (*"Here he goes again, George, talking about money again!"*) You can be a member of CAA for just one dollar a year. (*"Hey, I'm a dollar-a-year man, Ethel!" "I'm too young to remember what that means, George."*) The dollar brings you all the CAA news, and minutes of meetings, and announcements of various events. If you heard about CAA events too late to attend, you're probably not on our mailing list. And you're not on the mailing list because. . . that's right! . . . because you haven't become a member.

If you used to get our announcements but you haven't seen one lately, you're an *ex*-member. (*"He means you haven't paid your dues lately, George."*) Call our treasurer, [redacted] or one of the other board members and get them to mail you an application card. Then mail it, with the dollar, to Tim. (*"Hand me a dollar, Ethel."*)

(U)

P.L. 86-36

CAA Presentations

[redacted] did stir up a lot of people with his analysis of the "Outer Space" SIGINT problem, which he gave as the June CAA presentation. Does that problem exist? Who are "*they*"? Who do they think *we* are? Protein, *indeed!*

Maybe we should consider a follow-up (discussion? series?) to Clint's talk. By the time you read this, we may have already begun, but only those on our mailing list will know *for sure*. (And, of course, "*they*" will know too, won't they?)

September presentation: Have you ever tried to use a crystal ball? [redacted] will tell you how he uses his. Watch for the announcements.

(U)

Board of Governors, CAA:

President	David Gaddy	3247
President-elect	Frank Porrino	5879
Secretary	[redacted]	8025
Treasurer	Tim Murphy	3791
Board members	[redacted]	4935
		5991
		3575
		3369

(U)

P.L. 86-36

P.L. 86-36

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

SOVIET COMINT & THE CIVIL WAR [1918-1921]

Translator's note: The following is a translation of the article "The Organization and Combat Use of Radio Intelligence During the Civil War," by Lt. Col. Yu. Ural'skij in Voenno-istoricheskij zhurnal *(Journal of Military History), Moscow, No. 11, 1972. The article gives a rare glimpse into the early operations of Soviet COMINT and the importance that the top leadership gave to it from the very beginning of the Soviet regime. Footnotes citing Soviet archival records have been eliminated, and a few explanatory footnotes, enclosed in brackets, have been added.*

When setting up control agencies, units, and subdivisions of the communications troops of the Red Army that was being created to defend the Soviet authority, the Revvoensovet [Revolutionary Military Council] of the Republic (RSVR)[1] attached great importance to the use of radio as a means of communication among the troops and to its application in the interests of intelligence[2].

During the period of the civil war, the radio situation that had developed on all fronts favored the organization of radio intelligence by the Red Army, since the combat actions encompassed a large territory of Soviet Russia and were of a mobile nature. The interventionists and White Guardists made rather broad communications use of fixed and mobile (field) radio sets, which were supplied to the headquarters of their armies, corps, and divisions, as well as to naval vessels and merchant ships that were carrying troops, arms, ammunition, and other military supplies to the White Armies of the Entente[3]. Attached to the headquarters of Kolchak, Denikin, and Vrangel' were military-diplomatic missions from the Entente countries with a staff of military advisors who had radio sets at their disposal. They maintained contact with London, Paris, Warsaw, Athens, Constantinople, and other cities.

The interventionists and the internal counterrevolutionaries carried out radio communications in the range of 250-3500 meters, with wave lengths from 290 to 740 meters being used for field communications. The White Guardists had at their disposal the radio sets of the former Russian Army, as well as American, British, and French equipment that had been supplied by the Entente. For example, Kolchak's headquarters in Omsk had a radio set with a power of 30 kilowatts, which was used to set up communications along the lines: Omsk-Arkhangel'sk-London and Omsk-Nikolaev-Constantinople-Paris. The fixed radio sets had a power of 3-30 kilowatts, and the field and shipboard radio sets, respectively, 0.5 and 3 kilowatts; this made it possible, on medium and long waves, to cover rather considerable distances either directly or by way of intermediate radio sets. At the same time this allowed radio intelligence to monitor the enemy's radio transmissions from a considerable distance.

There was almost no observance of communications security or discipline among the White forces. Operational summaries concerning combat operations at the fronts, and sometimes even combat orders, were transmitted by radio in the clear. Sometimes the addresses in the radio messages were not encrypted, for example: "Urgent. Operational [summary] No. 3. Via Krinichnaya by radio to General Shkuro. . ." The radio data [callsigns, frequencies, etc.] of field radio sets were not changed for long periods of time. It was possible to determine who the radio sets belonged to by their callsigns, for example: PGL -- *p*oezd *g*enerala *V*rangelya (General Vrangel's train]; ALM -- cruiser *Al*maz; ZhA -- destroyer *Zha*rkij; ShI -- submarine *Shi*pka; GRV -- *Gur'ev*; etc. The grouping of enemy troops and the deployment and movements of headquarters could be learned from radio messages; from radio direction-finding information, from conversations in the clear between officials, or, indirectly, when the field radio set ceased operating and then started broadcasting again, but with reduced audibility.

Thus, the White and interventionist radio communications were a priceless source of information for the Red Army radio intelligence service concerning the enemy.

When, in the course of the civil war, Soviet Russia proved to be surrounded by a fiery ring of fronts, telegraphic communication with the Western European countries was cut off, and the delivery of foreign newspapers and magazines stopped, there was a sharp limitation in the amount of incoming information concerning international life. However, as during the years of World War I, the international radio stations (Paris, Lyon, Nauen, Carnarvon,

[1] [The RSVR was set up on 2 September 1918 to unify all military control at the fronts and in the rear during the civil war period.]

[2] Radio intelligence had sprung up and had received its organizational formulation during World War I.

[3] [It appears that the Soviet use of the term "Entente" includes all the non-Russian interventionist forces, rather than just the World War I Allies.]

Corsi, Rome) continued to transmit regularly (within the wave-length band of 600 to 1500 meters) newspaper reports concerning the international and military situation. The reports submitted by the foreign correspondents accredited to the headquarters of the White armies traveled along these channels. All this was of interest and enabled the RSVR, and the Red Army headquarters and troops, to intercept that information and to be informed concerning the international and military events, and to obtain valuable information about the enemy.

For the Petrograd Telegraph Agency (PTA) and subsequently the Russian Telegraph Agency (ROSTA), the interception of foreign reports was carried out at the Moscow, Tver', and Tsarskoe Selo radio stations, which had been constructed in 1914 for the purpose of linking the Russian Army's General Staff with the front-line staffs and with the Allies. In April 1918 these and other radio stations in the War Department were transfered, by decree of the Council of People's Commissars, to the People's Commissariat for Mail and Telegraph. In order to increase the amount of information, in the facilities occupied by ROSTA, its own radio station was set up in 1919; that radio station received reports from the correspondents at the civil war fronts, and also intercepted foreign telegrams. They were used in *Pravda* and *Izvestiya*, which regularly printed surveys of military operations at the fronts, and, in addition, provided special "pages for the Red Army man." A similar radio station was located at the People's Commissariat for Foreign Affairs.

The organization of a radio intelligence service in the Red Army dates from the beginning of 1919. However, attempts to carry out radio intelligence and to intercept enemy radio messages had been undertaken earlier by Red Army units. For example, during the second half of 1918, the interception of foreign reports was organized at radio stations 504, 600, 601, and 602 of the Western Sector of the screen detachments which had been intended for operational communications. This was carried out by radiotelegraph operators who were familiar with radio intelligence from having served in the old Russian army. During the period from July to October 1918, they intercepted 1576 radio messages. In July 1918, radio station 504 carried out surveillance and interception of the radio messages from the field radio stations of the Krasnov troops which were operating in the Don area. The necessity of organizing not only radio intelligence, but also radio counterintelligence, was recognized by the front headquarters. For example, the Board for the Administration of the Military Telegraph Communications of the Northern Front, in a report to the military commissar of the Northern Front in November 1918, noted, ". . . in order to detect and to provide warnings concerning the possible operation of enemy radio stations in the rear of our armies, and also in order to obtain information concerning the location and operation of radio stations attached to enemy military units, it is necessary to set up radio direction-finding stations and to organize radio monitoring on the front. . ."

The formation of radio intelligence subdivisions began in January 1919. Every front and army headquarters was supposed to have one intercept station *(priemo-informatsionnaya stantsiya)* and a radio direction-finding station. The former was intended for the reception of ROSTA summaries beginning with the words "to all Soviet deputies, to all editorial offices, to all propaganda points," and for the interception of of foreign newspaper reports and radio messages transmitted by the enemy's field radio sets. It was manned by eight persons and had one or two radio receivers with a vacuum-tube amplifier. The latter was supposed to detect enemy radio stations and get bearings on them. The staff at the radio direction-finding station consisted of 19 persons. In January 1919, for the purpose of supporting the Field Staff of the RVSR with intelligence information, a radio intercept station manned by 22 persons was set up at Serpukhovo.

Radio intelligence tasks were frequently assigned also to the field radio stations of troop staffs. But that was caused by an acute shortage of radio facilities and radiotelegraph operators working in the intelligence field.

The radio apparatus used for radio intelligence consisted of old models and was produced both by foreign companies and in the shops of the Navy Department. For the most part, they were detection receivers with a wave length range of 240 to 5100 meters. With the aid of changeable circuits, the limit of the range was extended to 15,000 meters. In order to increase the sensitivity of the radio receivers, three-cascade amplifiers operating on radio tubes were used.

Because of the shortage of radio direction-finding stations, an engineer at the Communications Directorate of the Red Army, V. I. Bazhenov, invented a special antenna. This antenna made it possible to adapt for purposes of direction-finding the ordinary field radio sets[4].

Organizationally speaking, the radio intercept and radio direction-finding stations were part of the radiotelegraph battalions of fronts and armies.

The overall management of the radio intelligence service was carried out by the radio

[4]See *Instruktsiya po prisposobleniyu polevykh radiostantsij k radiopelengovaniyu po sposobu inzhenera Bazhenova* (Instruction Manual for Adapting Field Radio Sets to Radio Direction-Finding by Engineer Bazhenov's Method), Moscow, 1922.

department of the Communications Directorate of the Red Army, and, at the fronts, by radio-communications and radio-intelligence sections of the communications directorates of the fronts and armies. The sections summarized the radio-intercept data, and drew up informational documents -- daily radio-intelligence summaries and diagrams showing enemy radio communications as they had reconstructed it. These materials were intended for the Field Headquarters of the RVSR and for the intelligence sections of the appropriate staffs. The most important information was immediately transmitted by telegraph to the Field Headquarters of the RSVR and to other interested headquarters.

It should, however, be noted that the possibility of organizing and making combat use of Red Army radio intelligence at the fronts was limited because of the shortage of radio equipment and specialists. As a result of this circumstance, on all fronts except the Caucasian Front it was impossible to carry out completely the radio direction-finding of enemy radio sets.

During the civil war years, the radio-intercept stations intercepted a large quantity of radio reports issued by foreign telegraph agencies. During 1919-1921, approximately 1000 intelligence summaries were issued solely on the basis of materials intercepted by just one radio station, attached to the RVSR (translated from English, French, German, and Italian). Summaries of radio-intercept materials from the foreign press were reported to V. I. Lenin. They were also regularly provided to members of the RVSR, People's Commissar for Foreign Affairs G. V. Chicherin, the Moscow Oblast' Committee of the RKP(b), the VChK[5], ROSTA, and the directorates and departments of the RVSR Field Headquarters on matters pertaining to their areas of responsibility.

The communiques transmitted by foreign radio stations contained important political, economic, and military information. For example, a radio message intercepted early in 1919 revealed Kolchak's overall strategic plan for the 1919 spring offensive. In a statement made by Kolchak in Omsk, it was stated, "We will attempt to establish contact with Arkhangel'sk, and as soon as we succeed in occupying a line on the Volga, we shall establish contact with the south and General Denikin, after which we will change over to the offensive and advance on Moscow. Seizing Moscow is our primary goal . . ."

In his article "How the Bourgeoisie Uses Renegades," V. I. Lenin emphasized the value of foreign radio communiques. "Our radio stations," he wrote, "intercept radio messages from Carnarvon (England), Paris, and other European centers. Paris is now the center of the worldwide alliance of imperialists, and therefore its radio messages are frequently of particular interest."[6]

The radio waves were the first to carry across the front line the information that the Entente was preparing a new campaign against Soviet Russia (the chief reliance being placed on bourgeois Poland and Vrangel').

During the period of Red Army combat operations against Kolchak in 1918-1919, the radio intelligence service on the Eastern Front successfully monitored the radio communications of Kolchak's Siberian, Western, and Urals White Cossack armies, was well as White Guard radio stations in the Astrakhan', Gur'ev, Krasnovodsk, and Baku areas. Kolchak's radio contact with the Entente was also established. Radio messages and radio conversations in the clear made it possible to establish the location of the headquarters of Kolchak, Denikin, the Caspian Front, the Caucasian and Don Armies, the Astrakhan' Detachment, and the group of forces in the Northern Caucasus.

In the summer of 1919, in combat engagements against the White Cossack Urals Army, the enemy's radio communications were monitored not only by the radio-intercept stations at the headquarters of the Turkestan Front and the I and IV Armies, but also by radio station 529 at the headquarters of the 3rd Cavalry Division, 596 at the 24th Rifle Division, and 530 at the 25th Rifle Division.

On the Southern and Southeastern Fronts in 1919, radio stations 504, 522, 518, and others monitored the field radio stations of Denikin's army and the fixed stations situated on the coast of the Black Sea (Nikolaev, Odessa, Sevastopol'). On the basis of radio messages and radio conversations in the clear, the radio intelligence service on the Southern Front in May 1919 succeeded in revealing rather precisely a grouping of Denikin troops in the south and in noting a concentration of the Volunteer Army in the Azov-Donetsk sector, the III Don Army in the Lugansk sector, the II Don Army on the Northern Donets, the I Don Army to the south of the Don, in the Tsaritsyn sector, and General Vrangel's Caucasian Army in the Northern Caucasus, and also succeeded in establishing the deployment of many of the White Guard troop headquarters.

On 5 October 1919 a radio intercept station at the IX Army headquarters intercepted and decrypted radiogram 04118, which contained a a combat order issued by the Commander of the Voronezh Group, General-Lieutenant Shkuro. The order assigned tasks to the units of Shkuro's cavalry corps after its seizure of Voronezh. The information received was immediately transmitted to the headquarters of the Southeastern Front.

The radio intelligence service of the Red Army operated more successfully against

[5] [Secret police; predecessor of KGB.]

[6] V. I. Lenin, *Poln. sobr. soch.* (Complete Collected Works), Vol. 39, p. 182.

Vrangel' in the concluding phase of the civil war. Factors that contributed to this were the experience that had been accumulated in the combat use of radio facilities for purposes of intelligence, and the improvement in the supplying of technical equipment to radio battalions.

During the Red Army's combat actions against the Vrangel' forces, many of the intercepted radio messages dealt with enemy groupings, the redeployment of headquarters, and the headlong flight of the White Guardists from the Crimea. For example, in one radio intelligence summary issued by the headquarters of the Southern Front it was indicated, "From radio messages intercepted by the chief front [station] from radio stations 6ZhT, 7ZY, and 5PY, one can make the following conclusion: radio station 5PY, attached to the 2nd Don Cavalry Division, approximately between 29 September and 1 October, was transferred, together with the division, to the area to the north of Volkovakha; previously that radio station had been in the Aleksandrovka area." The data obtained was subsequently confirmed by tactical reconnaissance.

Beginning on 8 August 1920 the radio stations on the Caucasian Front noted an exceptionally large amount of radio traffic in the Sea of Azov area. The possibility of a landing operation was raised. And, indeed, on 14 August, under the command of General Ulagay, a landing was made in the Akhtarsk area. Frontline radio intelligence continuously monitored the enemy's radio communications, intercepting radio messages and official conversations. The information thus received contributed to the defeat of this landing.

On 16 October a radio intercept station of the Caucasian Front headquarters intercepted an order from the Commander of the II Army, General Abramov, which had been sent in the clear. That order concerned the changeover on 17 October to the offensive against the Red Army units on the Kakhovka bridgehead. Knowledge of the enemy's plan of operations helped the headquarters of the Southern Front -- to whom the intercepted White order was forwarded -- to destroy the Vrangel' forces at Kakhovka.

In the final stage of the Red Army's combat actions in the fight for the Crimea, the White Guardists did not have enough time to encrypt their combat documents, and the radio traffic was sent in the clear. The radio messages contained information concerning the withdrawal of units, their evacuation from the Crimea. For example, changes in the enemy's groupings were mentioned in the 25 October 1920 radio-intelligence summary issued by the Southern Front: ". . . radio station OCh, attached to I Army headquarters, was removed, for transfer to a new location. Apparently the enemy has begun evacuating Melitopol'. Radio station 81T, which serves the headquarters of the troops operating in the Nikolaev area, also has been removed for transfer to a new location. During the past few days we have observed almost no activity by the enemy's field radio stations. One can assume that the headquarters of the divisions and corps to which the field stations are attached are being redeployed."

Radio communications also provided information about the course of the evacuation of Vrangel's troops from the Crimea. For example, General Kutepov reported to the fleet commander that he had 6500 officers and men on board a steamship, and there was absolutely no water or bread. He also reported that "the LAZAR, which was being towed by it," had sunk as a result of a leak. The KRONSHTADT reported to Constantinople that it had absolutely no coal or food supplies, it had 5000 passengers on board, and was towing the ZVONKIJ.

On the basis of the radio intercept information, the Commander of the Southern Front, M. V. Frunze, in an order dated 15 November 1920, demanded the "development of the most energetic efforts on the part of submarines and the liquidation of the enemy's attempts to use the sea to escape the blows being dealt by our armies."[7]

Thus, it follows from what has been stated that during the years of the civil war the Red Army's radio facilities were used successfully for intelligence purposes against the enemy.

At a conference of front-level chiefs of communications troops that was held in 1921, the activities of radio intelligence were rated highly. The radio intelligence service that had been created in our Armed Forces "completely justified its purpose and provided the Red Army with valuable material concerning the enemy, thus helping the Red Army to achieve victory." The role and importance of communications troops, including the role and importance of the radio facilities, were also given their proper credit by the Revolutionary Military Council of the Republic, which, in recognition of the valorous and extremely valuable work for the benefit of Soviet Russia, expressed its appreciation to the entire complement of commissars, commanders, and Red Army men in the Red Army communications troops.

The combat experience of using radio equipment for intelligence purposes during the years of the civil war was used for the further development of the radio intelligence service in the Red Army.

[7] *M. V. Frunze na frontakh grazhdanskoj vojny* (M. V. Frunze on the Civil War Fronts). Collection of articles, Moscow, 1941, p. 448. Unfortunately, the submarine forces could not execute this order. The two submarines in the Black Sea -- the AG-23 and the AG-24 -- were not ready for operations in the open sea.

G95 P.L. 86-36

GRAPHIC (?) LINGUIST

FORMERLY NON-VOICE LINGUIST

For some unknown reason, it seems that persons writing or talking about language skills, functions, and work loads have been unable to find an appropriate descriptive or general heading for the world of the translator. In contrast, the world of the transcriber presents no apparent difficulty, for it is neatly and effectively packaged and labeled as "voice." We speak, hear, read, and write about the "voice problem," a "voice linguist" (can this be a transcriber?), "voice traffic," "voice skills," the "voice language technician," and the "voice language analyst." As for that other world, however, no such overall descriptive has been discovered or devised.

At some point, someone decided to adopt a binary approach in resolving this problem. In our daily routine, we are constantly involved in situations where we are faced with a choice or condition of two alternatives, such as on-off, yes-no, 0-1. It follows, therefore, that if the one world is "voice," what can be more simple than to call the other world "non-voice"? This term has gained acceptability and respectability and is now virtually official NSAese.

When one carefully examines the word "non-voice," one can only conclude that it is a "nonword." It is vague and imprecise. The rejoinder to this might be, "Well, you know what it means from context." True enough. Yet, one could also understand the connotation of the term "non-transcriber" if it were used as a substitute for "translator" in the proper context. Fortunately, no one has suggested the use of the expression "non-voice language analyst" or "non-voice language technician" as career occupational titles, although such an eventuality is not unreasonable to imagine.

In seeking an alternative to "non-voice," I thought it would be helpful to scan the NSA Basic Cryptologic Glossary of June 1971, which the Director in his foreword urged all of us "to consult and be guided by . . . in the preparation of briefings, technical reports, and other documents." I was in for quite a surprise! If a linguist wants to give his or her tender sensibilities a real working over, he or she should review the 20 main categories of cryptology listed on page 47 of the glossary. Neither "language" nor "linguistics" nor "cryptolinguistics" made the honor roll (although "cryptolinguistics does appear as an entry). It is interesting to note that the entries "transcript" and "transcription" appear under the category "Collection (Interception)"! It is evident that the compilers must have wrestled with the placement of the entry "cryptolinguistics" because it is listed -- along with "scanning," "gist," "kana," "Cyrillic alphabet" -- under the category "General"! In effect, although this glossary represents the codification of the highly specialized vocabulary of cryptology, the few terms from the world of the linguist are lumped together as "General."

As for the cryptologic dramatis personae, a "traffic analyst" is defined as "a person versed in the art of traffic analysis," and a "cryptanalyst" is, of course, "a person versed in the art of cryptanalysis or the science of cryptanalytics." A "bookbreaker" is "a cryptanalyst who specializes in the recovery of plain text values in a code." One can only assume that the compilers of the glossary would have referred those who inquired about the definition of a linguist to Webster's dictionary. The Webster's *Third International Dictionary* defines a linguist as "1: a person accomplished in languages and especially in living languages: one who is facile in several languages. 2: a student of or expert in linguistics." The merits and demerits or validity of this definition in the cryptologic context could undoubtedly provide a stimulating subject for discussion among the practitioners of the linguistic art.

The next official source I consulted was the textbook "Radio Traffic Analysis," vintage 1964, which contains a "Glossary of Traffic Analysis Terminology." Although "transcription" and "voice" appear in this glossary, my search for other language-related terms was in vain. And then the trail led to the earlier edition (1955) of "Radio Traffic Analysis" and its glossary. There, for all the world to see, is the entry "linguist." Instead of providing a definition at that point, the glossary advises one to "See LINGUISTIC PERSONNEL." For "linguistic personnel," the glossary explains, "In cryptology, those persons skilled in language." The glossary adds what it calls "the specific categories of linguistic personnel engaged in cryptologic work." Would you believe 11 categories? They are:

- identifier,
- interpreter,
- language specialist,
- linguist ("one who has expert knowledge of a foreign language"),
- listener,
- reader (for those who may be puzzled by this, a reader is "a language specialist who deals with a foreign language in its written form"),
- scanner,
- spotter (not one who locates enemy targets or a civilian who watches for approaching airplanes or one who removes spots, but rather "a reader who sorts traffic by means of key terms"),
- transcriber,
- translator, and
- voice translator ("a listener who translates recorded language voice transmissions into written English).

How did the compilers of this glossary overlook the "non-voice translator"?

From the context in which "non-voice" is used, it presumably refers to a foreign language in its written or printed form, although one may make a good case for including Morse code, semaphore, smoke signals, or even intelligible drumbeats. If this presumption is correct, then why not use the term "graphic," defined by Webster's as "of or relating to the written or printed word or the symbols or devices used in writing or printing to represent sound or convey meaning"? In combination forms it may even offer some euphonious possibilities -- "graphic traffic," anyone? In fact, "paper linguist" has been occasionally used as a synonym for translator. However, it comes too close to "paper tiger" and our local humorists have enough material already.

I have been using the term "graphic" in the language context for some time now without having elicited any noticeable confusion, discomfort, or demurral on the part of readers or listeners. Notwithstanding the fact that the "age of verbal permissiveness" is upon us and almost anything goes, I offer it as an effective substitute for "non-voice."

Years ago there was a popular song, written by the late Johnny Mercer, that contained some relevant sound advice in its opening lines: "You got to accentuate the positive, eliminate the negative, latch on to the affirmative, don't mess with Mr. In-between." ~~(C CCO)~~

[redacted]

LETTERS TO THE EDITOR

To the Editor, CRYPTOLOG:

This letter is in response to two articles by Mr. Mark Pattie, "What Language Problem?" (CRYPTOLOG, May 1976) and "As I Was Saying Two Years Ago..." (CRYPTOLOG, June 1978).

You were wrong in 1976, Mr. Pattie, and you are wrong again. Worse, your attempt, or any attempt, to prove that there is a high-level Agency-wide conspiracy against linguists is doomed to failure because no such conspiracy exists. Nor has it ever existed. Individual inequities -- probably, but no more in the ranks of linguists than in any other cryptologic area.

There are some fatal flaws in your articles that ought not to be there, if for no other reason than because of your cryptanalytic background. For example, the current group of GG-15s in the SR, Language, CA, and TA fields breaks down to one SRA, nine "linguists," 11 CA, and one TA. Using your analytic methodology the "linguists" are in pretty good shape in the cryptologic skills area. In fact, we might deduce that they don't do badly when measured against the CA field, and that they are 9 times better off than the SRAs and TAs.

We might make that deduction, but we had better not because those numbers don't tell us anything at all except that there are a certain number of people at a certain grade in a particular group of COSCs. In short, they don't tell us any more than your numbers did. If we took a further look, we would find that the nine "linguists" are in fact almost all division chiefs, research linguists, or language coordinators rather than language analysts or voice language analysts. And that is who we are talking about, isn't it? We must get that straight at the beginning. If we are going to talk about language analysts and voice language analysts at the 13 or higher grade levels, we are not talking about language people at the technician level. Your second fatal flaw, then, I believe, was to put all language people into the same pot. Surely you are aware that the terminal grade for language techs is GG-12 and since that job has requirement for only a level-2 language proficiency, GG-12 seems quite generous to me. I should point out that in the technician arena, in grades GG-5 through GG-12, language people enjoy a promotion rate and an attrition rate that is nearly identical to that of the other cryptologic skills.

But I digress. We are not supposed to be talking about technician-level language people, but rather professionals. You made a big thing out of the statistic that said linguists got 4 percent of promotions in the 13-18 range, while engineers captured 19 percent of the total. That rate is just not strange when you also consider that all professional-level language jobs throughout the Agency constitute only 3 percent of the authorized work force while engineer and computer scientist professional-level jobs constitute 17 percent of that same work force. Now if you want to argue that there should be more professional-level jobs in the language field, that's a different ballgame. But you would probably get a lot of argument there too. The fact is that an awful lot of our current authorized level-3 (professional) jobs are being done by level-2 (technician) people. In some areas the professionalization rate is under 25 percent, meaning that 75 percent and more of the people on the job are not even qualified for consideration to promotion beyond grade 12.

But aside from all of this, I recognize that the gut issue, in your mind, is that we get what we pay for. Not always, Mr. Pattie, not always. Sometimes we have to pay for what we get, though, and we do not operate in a vacuum. We know what professional engineers (and linguists) are paid outside the Agency, so we must be competitive. If that means extra pay and more rapid advancement for engineers and computer scientists at the professional level, then it is so because of a real-world situation -- that is, it is so because it is what we must do to accomplish the mission. You ought not to confuse ideological truths with reality: everybody has an opportunity to become Deputy Director, but not everyone will. The career structure allows for movement in the language field up to GG-18, but there are no real jobs at that level. That's the way it is.

Whoever told you that hiring high school kids was "*the* latest solution to the language problem" lied. Nobody associated with the program that I know believes that. The facts are that we are hiring very sharp high school kids as trainees (in Russian only at this point) because that's where the requirement is. We are also hiring Russian majors, other language majors as trainees, ex-military (many of whom were high schoolers, incidentally), and anybody else who can qualify as a language technician or trainee. The point is that we are hiring people against requirements as trainees only when we cannot get already trained people. We are doing it in language, collection, signals conversion, and soon we will do it in the computer field.

You asked, "Why don't we hire high school graduates to be trained as engineers or mathematicians?" I know you were once assigned to the National Cryptologic School so I expect that you know we aren't equipped to train either from scratch. We are, however, well equipped to train language people from the ground up with one of the best damn language teaching staffs and faculties anywhere in the world. The attrition in those classes is under 10 percent, and that would be a miracle, except that it has been accomplished by outstanding recruiting, teaching, staffing, supporting, and plain hard work by the students themselves.

Another mistake I suspect is that you are confusing the importance of the mission with the difficulty of accomplishing it. We cannot realistically use "job importance" to set pay scales -- who's going to decide whether it is more critical to collect, decrypt, translate, transcribe, analyze, or transmit?

Finally, solutions that cannot be carried out are not solutions. About $20 million and 1000 more people would probably solve all our problems, but neither the $20 million nor the 1000 people are available. If you can figure a way around that, you should immediately pass it on to the "senior managers" you think are involved in the conspiracy. I am sure you would enjoy their unending gratitude.

Dan Buckley, M03

~~(C CCO)~~

Mr. Pattie replies:

My goodness! I must certainly have struck a nerve in Mr. Buckley. His letter flays me up, down, and sideways. Could it be that his role in the high school program has made him a bit sensitive to any criticism?

After reading his scathing letter I thought I had better reread my articles to see if I had said anything about a "high-level Agency-wide conspiracy against linguists." I never brought up the possibility of such a "conspiracy," but since he did, maybe it does exist. Methinks he doth protest too much.

I suppose someone could construe my comments about senior officials and their attitudes toward language work as implying "conspiracy." If anyone took it that way, I apologize. However, I do stick by my statements about individual seniors and their attitudes. Although I suspect that there would be staunch denials, some have definitely expressed low opinions about linguists and language work.

Mr. Buckley uses flamboyant language in castigating me and I feel reasonably sure that if he had thought about it a bit more he might well have toned down his letter. For one thing, I believe he could have made his first "fatal flaws" paragraph more comprehensible. I don't know what he meant by "current group of GG-15s" and I don't really care, for I thought I was comparing linguist *promotions* with those of engineers.

Then, to take me to task for not recognizing that there is a language-technician level is raising another "fatal flaw" to no purpose. Did any other reader believe I was talking about nonprofessional linguists? All of that particular argument is a red herring having nothing to do with the issue I tried to raise.

As for professionalization itself, there is no question in my mind that it is far easier to become professionalized as an electronic engineer than as a linguist. Can you deny that, Mr. Buckley? This is so because the Agency has determined that to be a professional linguist one must pass a series of very difficult tests, along with other requirements. That in itself goes a long way towards explaining why so many level-3 language jobs are being handled by level-2 people. Engineers have a far less stringent professionalization program.

The tone of Mr. Buckley's letter is most unfortunate, for he seems determined to read the riot act to me even when he states what I have already said in my articles. Of course I recognize that the Agency must compete with the outside world in hiring. The difference is that the Agency is willing to pay more to hire engineers than linguists. Since he is so close to all of the facts and figures, perhaps Mr. Buckley could tell us how many engineers and how many linguists have been hired directly at the GGD-13 level or higher over the past few years or so.

And, of course, the statement that there are no real jobs in the language field at the higher grades is a fact that we all recognize. But isn't that one of the things I was complaining about? His "That's the way it is" implies that that is the way it will always be, and I fear he is right.

Then, there is the matter of the high school program, for which he berates me so soundly. I would still like to hear someone give facts and figures on the retention rate of the previous high school program. If his office cannot find this data, I suspect that some of the operational areas would be able to fill in the gap.

Incidentally, this "one of the best damn language teaching staffs and faculties" he refers to is composed of contract instructors (many of whom have not had a raise in years) and people on loan from operational elements, in addition to those who are assigned to billets in the NCS. It is a real hodgepodge. I do not have access to any pay records but my best guess would be that the Agency is getting this instruction at bargain rates. It should also be noted that the contract instructors, being only partially cleared, can only carry the students so far before their lack of knowledge about our business brings a halt to their usefulness.

I do not understand the accusation that I am "confusing the importance of the mission with the difficulty of accomplishing it." What does that really mean?

Then, finally, the statement that "we cannot realistically use 'job importance' to set pay scales" does not ring true. Someone does, or should look at Agency mission and function statements when determining hiring needs and tables of distribution. The statement runs contrary to his previous points about hiring and career structure. Yes, someone has decided that pay scales for engineers are higher than those for linguists. Is that a conspiracy? I'll let you decide.

I'll end with one final point -- all the best engineers in the world cannot issue one piece of end product. Linguists can and they ought to be paid well for it.

Mark T. Pattie, Jr., P13D

~~(FOUO)~~

Do you HATE TO WAIT?

Do you hate it when only one or two copies of CRYPTOLOG are circulating in your work area and you have to wait and wait to read the latest issue until after everyone else has read and discussed the provocative ideas expressed in it? Worse yet, do you hate to wait to see the latest CRYPTOLOG, only to find that all the puzzles have already been done? -- *and in ink!* Well, then, why don't you just ask to be put on the distribution list to receive your own personal copy of CRYPTOLOG? Just send your name and organizational designation to: CRYPTOLOG, P1. You don't have to type up a fancy-looking memo -- a scrap of paper will do it. Or you could telephone the editor, on 5236s. That's riskier, however -- while he's got you on the phone, he might try to coax you into writing one of those discussion-provoking articles yourself.

(U)

T ANNOUNCES ESTABLISHMENT OF HUMAN RESOURCE DEVELOPMENT PANEL

Telecommunications and Computer Services (T) announces the establishment of a Human Resource Development Panel. The Panel's two primary functions are to assist T employees in career planning and to advise DDT in areas of human resources development, career planning, and utilization. Information about the operation of the Panel may be obtained from the Chairman, Mrs. [redacted] T432, Room 6A126, x3091s.

P.L. 86-36

(U)

NSA-crostic No. 17

by A.J.S.

The quotation on the next page was taken from the published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

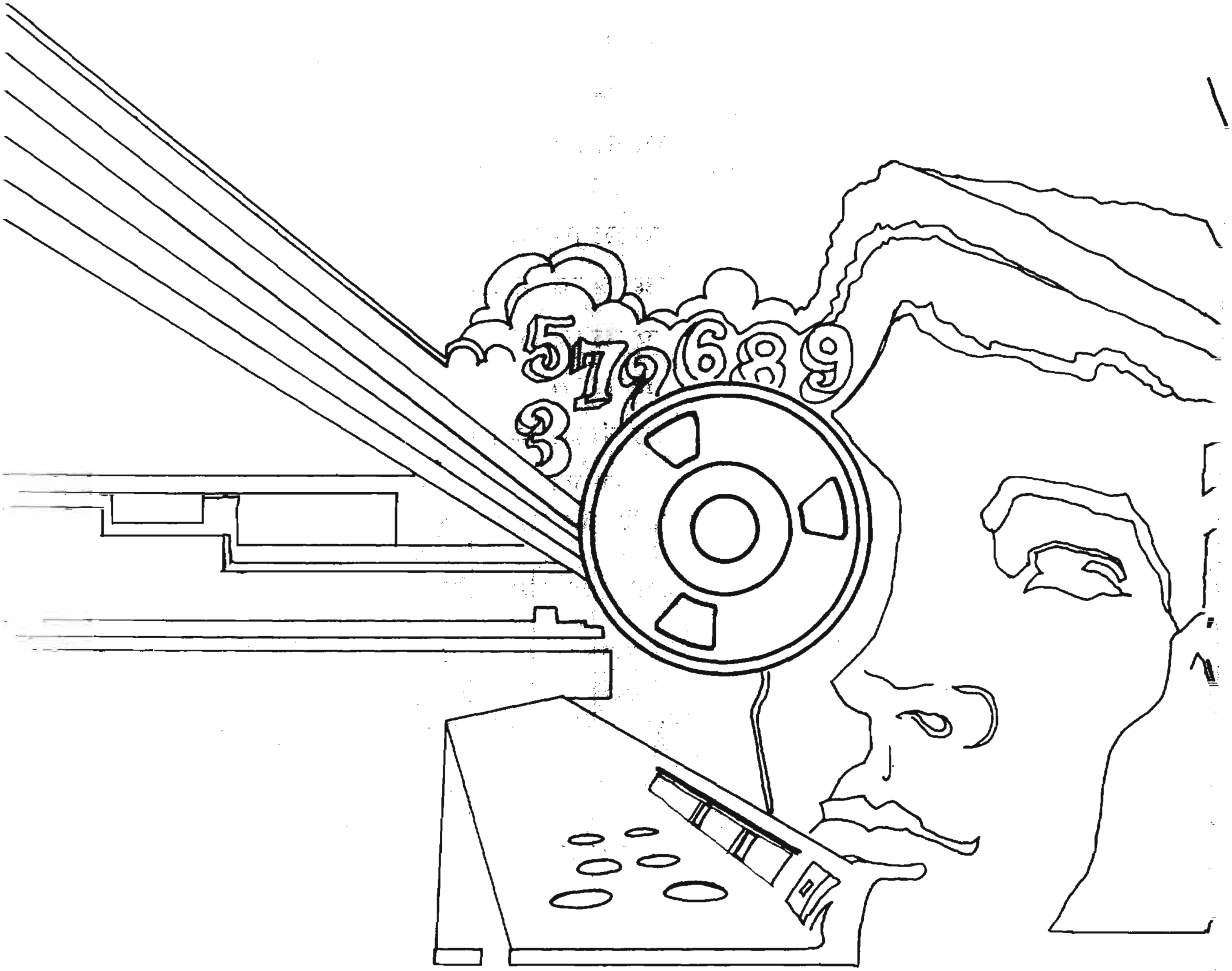
DEFINITIONS *WORDS*

(Solution next month)

P.L. 86-36

DOCID: 4019726

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~