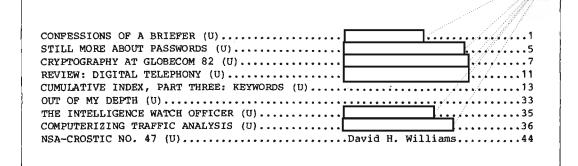


P.L. 86-36



THIS DOCUMENT CONTAINS CODEWORD MATERIAL

- CLACCIFIED BY NCA/COOM 123-2 - DECLACCIFY ON: Originating-- Agency's Determination Required



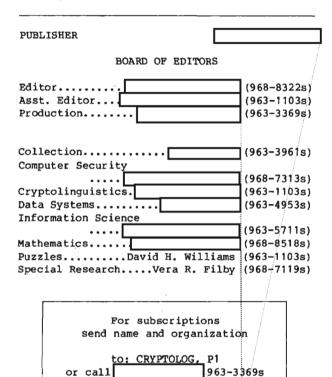
Declassified and Approved for Release by NSA on 10-12-2012 pursuant to E.O. 13526, MDR Case #54778

# CGVCTOLOG

#### Published by P1, Techniques and Standards

VOL. X, No. 5

MAY 1983



P.L. 86-36

#### To submit articles or letters via PLATFORM mail, send to

cryptolg at bar1cØ5
(bar-one-c-zero-five)
(note: no '0' in 'log')

Contents of <u>Cryptolog</u> should not be reproduced, or further disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

# Editorial

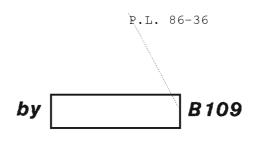
At my bank, having direct mail deposit qualifies me for certain privileges, but when I applied for them, I was told I was NOT a "direct mail depositor." I disagreed; my paycheck is sent directly to them, and has been for some time. Then, I discovered the key: my account is joint with my wife, and the computer lists her name FIRST. So when they retrieve data about MY accounts....

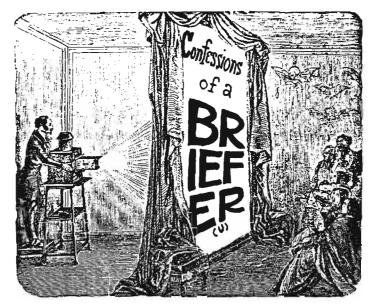
Some years ago, when I dabbled in real estate, I had several fat listing books, and kept them in order by area, price, and number of bedrooms. The listings were typed, and often contained errors. Some were easy to spot. If the tax district or the number of bedrooms was wrong, it was easy to make a pencil change on my copy and move the listing to the right place in the books.

I notice that real estate agents are computerized these days. They go to a terminal, key in a price range, number of bedrooms, geographic area, etc., and out comes a string of listings. Who makes the corrections? I doubt that anyone does. It wouldn't surprise me to hear that some real estate people "hide" new listings, when submitting them to "Multiple List" data bases, by putting typos into key data fields, to give their own agents "the first shot" at a new listing. Between accidental and intentional typos, I wonder how much of the existing data actually gets to the requestor.

Please don't write in and tell me about good programming practices. That's not my point. Both we and our targets are coming to rely more and more upon data retrieval for our information. Anybody who can read and type can call up data on most of these systems, but only the more innovative people will be able to squeeze out of the system the "hidden" data. Knowing how to do this could depend upon understanding how people behave when they use a data base, and also how the data base itself really works. It could, in fact, become a new cryptologic skill field.









ake up, Jim. The briefing's over."

"Huh, what did you say? Oh, I guess I must have drifted off. Sure is hard to stay awake in a dark briefing room after lunch. Say, Fred, did you get copies of that guy's slides for me to read back in the office so I can find out what Project RATTLECAN is all about?"

Does this exchange sound familiar? If not, then this article is not really for you. (Keep on reading though; you might learn something that will be useful later.) But if you are one of those who have been bored to sleep on numerous occasions as some well-meaning project officer or analyst read an endless succession of slides to you, perhaps this article will contain some thoughts that may help you avoid inflicting similar boredom on others. It may even make your briefings more effective.

One of the most basic causes of poor briefings here at NSA (and elsewhere as well, I am sure) is the mistaken view that briefings are a good, concise way to transfer information to people. Absolutely nothing could be further from the truth. Yet we constantly use briefings to "bring people up to speed" on a wide range of detailed and complex topics. The subtle deceit of briefings is particularly interesting when someone has received a "Good brief!" from his audience. Just ask the briefee afterwards how many tanks the Zendian Army has, or how many communications circuits are at Field Station Xapa, or some other detailed question on the topic and most likely you will get some answer like "Well, I don't recall exactly, but I'll call Tommy Talker who briefed me on it and he'll have the answer." In this case Mr. Briefee may not have the facts but he did get the message.

The fallacy of using briefings to bring people "up to speed" is that briefings are not a good medium for the presentation of a lot of objective, factual data. They are, however, an excellent medium for affecting people's attitudes and emotions. In our society we have so thoroughly suppressed our emotions (e.g., "Grown men don't cry") that we would tend to deny that we are even subject to a play on our emotions, especially in some intellectual palace like the National Security Agency. Unfortunately, this leaves us extremely vulnerable to approaches from a nonintellectual angle and the briefer who discovers this vulnerability, either by accident or as an active intellectual discovery, can use this approach to produce consistently "good briefs." This is a fact long known to Madison Avenue and it is equally true here at the Agency.

When you have had a good briefing, what are the things that you most readily recall? In all likelihood it will include items such as the command and presence of the briefer and the quality of the graphics. You will remember the organization that sponsored the briefing and those memories will be of a competent and professional outfit. You will know that the topic briefed is:

- very grave;
- [] requires immediate action by your organization;
- [] is in competent hands; or
- [] needs more resources in the out years.

But you will not recall specifically why you have those feelings.

All this having been said, then, how can we use this knowledge in building a "good brief"? The most basic step is to decide what emotional message, feeling, or attitude you want to inculcate in the listener. Generally, the attitude or emotion will be one favorable to the topic and organization presenting the brief. For instance, a project officer will generally want to leave listeners impressed with the importance of the project so that future requests for support will be favorably endorsed. In short, although briefings are generally thought of as being informational, most briefings are sales pitches. Once the basic message of the briefing is established, all other work should support that message.

In briefing there is no substitute for the competent briefer, a person who speaks with all the self-assurance of a Nobel Laureate but who at the same time compliments and involves the listeners; one who does not preach to them. For some people these qualities are natural, but for most they can be acquired. The secret is lots of practice and the knowledge that you know more about your topics than your listener.

Armed with this confidence, the briefer should never use a script. If you know what you are talking about, you don't need a script. If you don't know what you're talking about, you shouldn't be briefing. Bishop Fulton Sheen never used any notes on his very successful TV show during the 1950s. When asked about this once, he cited a remark he had heard as a child. An old woman walking out of church was complaining because the bishop had read bis sermon from notes. Her question, which impressed Sheen, was "How the devil can he expect us to remember what he's saying when he can't remember it himsel??" Freedom from the script allows the briefer to give the appearance of being extemporaneous as he or she responds to the quips, comments, and questions of the briefee(s). It also permits the briefer to tailor the brief readily to the background and interest of the listener. Finally, the freedom from the script allows the briefer to establish a pace or rhythm for the briefing that enhances the authority and assurance of the presentation.

With the script eliminated, the only tangible form left to the briefing is the graphics. These are as critical as the presence of the briefer and, in fact, can often make the briefer seem more professional and the briefing come across better. In the choice of graphics it is especially important to keep in mind the emotional appeal of the brief. The Chinese writer who said that one picture was worth a thousand words knew what he was talking about, and the proper choice of graphics can save a lot of talk and questions.

For example, consider the graphics in Figures 1 and 2. "Zendian Army Power" (Figure 1) is just a compilation of numbers. The briefee will read it rather than listen to the briefer--and you'd better hope that the briefee doesn't have some spurious knowledge or he might make some comment like "I thought the Zendians had Type Q tanks instead of Type Ys." This sort of question could well be enough to throw an inexperienced briefer off pace or, worse yet, lead to intellectual questioning of every statement.

Figure 1 has has yet another critical flaw: In column 1 the numbers don't add up to the total shown. If the listener notices this, he/she will spend the rest of the briefing adding up any numbers that appear, looking for other errors.

#### FIGURE 1: ZENDIAN ARMY POWER

	TROOPS	TANKS	HEAVY ARTY	MED ARTY	APC	HELOS
I CORPS	55,000	250	200	500	600	45
*						
III CORPS	58,000	300	212	550	600	43
IV CORPS	61,000	312	220	560	500	48
V CORPS	58,000	270	220	550	550	45
ABN CORPS	25,000	**		200		350
TOTAL	247,000	1132	632	2360	2250	531

\* There are no units in the Zendian Armed Forces with the designator 2 or II because the Zendians consider this number bad luck.

\*\* There are no tanks per se in the Airborne Corps but there are approximately 200 of the so-called "Y-type tanks" that are in reality a lightweight high-speed tracked anti-tank gun.

May 83 \* CRYPTOLOG \* Page 2



Figure 2



Figure 3 May 83 \* CRYPTOLOG \* Page 3 FOR OFFICIAL USE ONLY

Figures 2 and 3 (previous page) are good examples of effective graphics. Both of them evoke a strong emotional response. In fact, either of these pictures could well move the listener to a rendition of war stories about when he/she drove tanks, rode in helicopters, or had some related experience. This will imbue feelings of camaraderie between the briefer and briefee that will make the briefee much more amenable to the briefer's message.

These two pictures have some other practical advantages:

- [] they will serve to cue the briefer;
- [] they will not limit the remarks the briefer may wish to make
- [] they don't contain the intellectual snags
  that are found in Figure 1; and
- perhaps best of all, they will not have to be changed or updated unless the Zendians get rid of that tank or helicopter.

(When using slides like this, however, make certain that it is really a picture of what you say it is or it will be almost as bad as having numbers that don't add up.)

By concentrating on influencing emotions or feelings, we do not ignore the facts. We just use them in a different manner. Rather than being sort of inert things, the facts that we have to use are woven into the fabric of the brief in a way that supports the basic message. One way to do this is with "amazing facts." We all have a store of "amazing facts" but probably don't realize it. For example, the fact that the Zendian Navy has 89 operational submarines will probably mean very little to anyone but an avid naval buff, but the same fact cast in a different context becomes an "amazing fact": "The Zendian Navy has the largest submarine force in the third world!" Bar, pie, and line charts are all effective ways of presenting amazing facts such as this.

While you never want to read your slides to your listeners, there are times when you may want to let your listeners read the slides themselves. This provides a change of pace for both briefer and briefee. It's a quick way to slip over what otherwise may be a long narrative and it involves the briefee in the briefing process more actively. Such graphics should never be long textual passages. The proper form is short "bullets," ideally only one or two words each. (See Figure 4.)

#### UNITARY PLANNING I&W EMPHASIS SURVIVABLE COMMUNICATIONS COMPUTER INTEROPERABILITY PRODUCTION ENHANCEMENT COMBINED WORKFORCE

#### Figure 4

The briefer can introduce this type of graphic with some line such as "These are the characteristics of ..." (whatever the subject is). The briefer should watch the faces of his audience and move on to the next graphic as soon as the the expressions of the listeners show that they have read the graphic.

In summary, the key to effective briefing is to remember that briefings should be used to form attitudes or affect emotions, not only to transfer objective facts. The effective brief should have one central underlying attitudinal or emotional message that it is attempting to deliver and all aspects of the briefing must support this. The briefer should not use a script and the graphics should be simple and chosen with an eye to their emotional impact. Facts used in the briefing are much more effective when placed in some sort of comparative context. Slides to be read should be read by the briefee not the briefer.

Good luck! Good brief!

#### "Epilogue"

In closing, I believe it is necessary to comment on the ethics of briefing. It is evident that, armed with information about the weakness of our psyche, an unprincipled bureaucrat can take considerable advantage of his or her colleagues. At present the only sure counter to this is the individual integrity of the briefing organization which must use its power only for pure motives. Unfortunately, a full discussion of the ethics of briefing is beyond the scope of this article, but perhaps some reader may feel an urge to expand on that topic.



May 83 \* CRYPTOLOG \* Page 4



₽.L. 86-36

#### A USER VIEWPOINT

P13

The password controversy continues. On the one hand, and others have stressed the need for greater security to avoid potential compromise. On the other hand, and others have made a strong case for short, easy-to-type and memorable passwords to avoid needless errors and frustration on the part of the user. I am in sympathy with both causes, although I violently object to closing para-graph (CRYPTOLOG, Mar 83, p. 38): he states violently object to that an easily remembered password is easy to type regardless of length, and that he doubts that a non-typist (i.e., one who does NOT find a long, memorable password easy to type) will use a terminal for very long. I would argue just the opposite. The probability of error rises progressively with each additional character added to the password, especially since characters are not being echoed on the screen. Also, my personal observation has been that the majority of non-secretarial users-linguists, programmers, and managers among them--are in fact either non-typists or poorto-fair typists, myself included; yet terminal usage among these groups is increasing rather than decreasing, as more and more people become aware of the advantages which a computer terminal can provide to the professional user.

Having said this, let me state that I think the problem is easily solvable in a manner which should satisfy both viewpoints. Instead of viewing the problem theoretically--short passwords are good, but breakable; large alphabets, pass phrases, and "passcodes" are good, but will result in higher error rates-we should take the Agency environment into account. Many Agency computer systems have a feature which automatically "kicks out" anyone who unsuccessfully tries a user ID-password combination three or four times in a row. Those which do not can be easily modified to allow this capability. If the office security



manager is alerted to terminals on which three unsuccessful ID-password combinations have been tried, I doubt very much that a hostile entity would have any success in breaking even a five- or six-letter, single-case, mnemonic password before being apprehended. At the same time, a poor typist gets several chances at entering the combination correctly before setting off the alarm. This system thus provides the best of both worlds: a user-friendly password environment which is, for all intents and purposes, immune to exploitation.

P.S. A challenge to all UNIX users: how many of you can type "Low flying bees eat wax beans" (to use \_\_\_\_\_\_\_\_ example of a pass phrase) and get it right the first time? It's easy to find out: set terminal type to STTY -ECHO; type in the phrase enclosed in single quotes, i.e., 'Low flying bees eat wax beans' and hit <RETURN>. A system message will appear as follows:

> flying bees eat wax beans: not found (or whatever you REALLY typed)

After you're done experimenting, STTY ECHO will make your characters visible again. (At an informal testing in the KEPLER laboratory, I got the phrase right 3 out of 7 times; however, I fall under the "non-typist" category.)

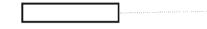
#### THREE GOOFS AND YOU'RE OUT

On [the system I use], a user signs on with user initials and then is required to type in a password. If the person "fails," they may try again and again and again.... To prevent exhaustive searches, why not flag to the systems operator any console that tries say three times? Or lock that terminal out?

P.L. 86-1

#### PASSWORDS: FRIEND OR FOE?

Speaking of passwords, what is an acceptable balance between security and convenience? I have found what I believe to be a rather comfortable and simple solution (but then I'm sure SOMEONE will disagree). I simply choose a word...such as walnut, then alter or mispell it (walllnut, wawlnut...etc.). Not enough to make it difficult to remember, but definitely making it more secure and harder to guess.



#### MORE ON PASSWORDS AND HUMAN FACTORS (from COMPSECNEWS, June 1983)

One of the frequently heard complaints from persons who changed to more clever passwords containing special symbols or mixtures of upper and lower case, was that when bringing some of the terminals up cold, and prior to loading the terminal emulator, they could not login. True that each keycap may not send the same character before an emulator load as it will after, but when those infrequent occasions arise, you can still prpbably login if you only knew what keys to press. For example, one system I know of uses the "back tab" key to produce the "/" prior to emulator load. Obviously an inconvenience, but most users do not regularly have to perform initial terminal loads.

Other systems that I have seen have accounts called "LOAD." These accounts do not require the person who logs in to enter a password, only to choose a desired emulator. After the selected emulator is loaded, the real user login is then required. If your system does not have this feature, complain to the system Guru. Incidentally, notice that an emulator load is all that the "LOAD" account can do.

Another comment had to do with the login-id being secret. The suggestion centered around doing away with initials as the login-id, and using a secret account name in addition to a secret password. Maybe a useful idea, but one point missed by this comment was that the current login algorithm used on most of the systems does not reveal what is wrong when the login fails. For example, notice of login failure only appears after the id and the password has already been given. Another problem with this suggestion is we already have a requirement to identify individual use of sensitive computers. Work is currently underway to assign each and every user of our computer systems a unique id that will be the same regardless of which computer system is used. The adopted format will follow first two initials followed by the first five

letters of the last name. A central registry is being established to resolve conflicts.

(June 1983)

P.L. 86-3

P.L. 86-3

Keep your comments coming! In particular, I would like to see more comments from users about the consequences for them of various access restrictions, password procedures, etc. How have some practices on the systems YOU use hindered or helped YOU in your work? I know that it is fun for a lot of you ingenious people out there to think up new password schemes and gimmicks, but the computer security experts are pretty inventive and ingenious too. What they need, more than new techniques and ideas, is some clear feedback from users about the COSTS and BENEFITS of different kinds of procedures currently in use. If they get a clear indication from users that certain methods of implementing access restrictions impose a relatively high cost on users, they will be motivated to use their ingenuity to find other and better methods that are just as secure but less costly to the user. I was interested to note, in the COMPSECNEWS item above, the assumptions that

- users rarely had to load terminals "cold"; and
- coping with keys that send different characters before and after emulator loading constituted a minor inconvenience at most.
   What do you think about those assumptions?

As a hunt-and-peck typist, I find odd-ball special characters are a MAJOR stumbling block, even when the keycaps agree with the character that gets sent. Even the shift key and "CTRL" key are frequent error-makers for me. Also, my impression is that users have to down-line-load Delta Data terminals more frequently, at least for some systems, than the COMPSECNEWS editor assumes. In fact, if I had to cope with that problem, even having to load a terminal once a week would be far too often for me! The "LOAD" account mentioned in the article seems to me a much more promising and user-friendly approach than "if you only knew which key to press."

For a programmer, or someone thoroughly familiar with the terminal and software, perhaps keys that send different odd-ball sets of characters at different times may present only a minor annoyance; in fact, computer folk seem to thrive on and positively welcome such problems. Most others, however, are very unlikely to agree with them. Computer specialists, and computer security specialists in particular, need to be reminded that situations constituting brief nuisances or even amusing challenges for them can be stressful and exasperating for other kinds of users.

#### -M.E.D.

LOOKING AROUND with

# Cryptography at GLOBECOM 82

P.L. 86-36

# **Review:**

TOP SECRET UMBR

# Digital Telephony (U)



DES-type algorithm, using 800-bit vectors in place of the 48-bit vectors of DES, was proposed at GLOBE-COM 82 (the 1982 Global Communica-

(U) tions Conference) for the encipherment of medical records. The key would be 160,900-bits long. The Belgian author of the paper, Desmedt, claimed that this would protect medical records during the life of the person concerned. In reply to a question, he admitted that he did not know how to keep the 160,900-bit key itself secure and intact for the 100-year period.

(U) The Desmedt paper on super-DES was one of five papers on cryptography presented at GLOBECOM 82 in December. In addition, there were five other sessions on coding, primarily speech coding, which proposed reducing bit rates for video and voice and facsimile. Compression techniques and the ability to recover from channel errors are critical to the use of digital encryption techniques.

(U) One of the surprising papers was about a detailed experiment with analog encryption at Bell Labs. Apparently low bit rate encryption causes so much loss of voice quality, especially over low-quality lines which cannot support 9600-bps rates, that there is a growing demand for encryption which sends analog waveforms. The Bell Labs work has been done by computer processing, but they expect to develop a real-time circuit, after which their VLSI chip designers will examine the cost of single-chip analog encryption. That could have a revolutionary effect on secure voice and on cryptanalytic priorities. (U) Two other surprises were the sophisticated insight into the strengths and weaknesses of various public key schemes, especially the flaws of the Hellmann-Merkle algorithm, and the importance of the recent Racal-Milgo patent on finding large primes for the RSA public key algorithm. Several speakers stated that the RACAL-MILGO algorithm had made the integration of DES and the RSA algorithm feasible as the basis of a switched ad hoc public cryptographic network.

(U) This demonstrated interest in the feasibility of the RSA algorithm as a means of keying DES links is more interesting in the light of the Inman interview (<u>Science</u>, Dec 82), which identified RSA as a secure method.

(U) The leadoff paper by J. Michael Nye, a self-styled cryptographic "expert," described the methods and cost of intercepting telecommunications in the US and gave a list of 26 domestic cryptographic suppliers offering 104 products and 13 foreign vendors offering 81 products in the US market. The list of suppliers and products is growing, and the impact of Personal Computer encryption is yet to be felt. This is a very big change from ten years ago, when only a few companies supplied cipher equipment to the US market. Most of the products are for fixed telephone service, but as the new technology of cellular radio develops over the next decade, the market for voice encryption, to protect the 900-MHz mobile circuits from interception wi11 increase to millions of vehicle radios.

TOP SECRET UMBRA

(U) Cox, Jayant, and McDermott of Bell Labs gave a paper on a time-frequency segment permutation analog encryption which they believe is very secure against cryptanalytic attack, without loss of voice quality or syllable intelligibility. The delay for the scrambling and descrambling is no more than 256 to 512 milliseconds for 16-msec speech segments. Each 16-msec segment, sampled at 8000 Hz to give 128 samples, is converted to sub-bands by digital filtering, and the sub-band vectors are then permuted. The digital vectors are stored in a buffer with a memory capacity up to 512 msec. A cryptographic keystream decides on the segment permutation, and also decides which time segment will be sent. Any time segment can be delayed up to 256 msec. The input test data were voiced digits in random order, used to avoid the redundancies of normal conversational speech.

(U) The cryptographic scheme is to fill the buffer with 16-msec segments, then send all of them in some pseudorandom order until the buffer is transferred to the receiving end. Then the buffer is refilled and the scrambling and transmission begin on the next multisegment block of speech. It is not clear from the published paper whether the segment transposition key is the same or changes from block to block.

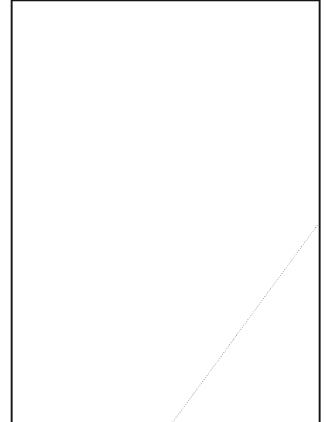
(U) The scrambler was implemented on the BTL Digital Signal Processor, and tests showed that it gave better intelligibility than simple frequency inversion scrambling. The scrambled signal envelope sounds like "birds chirping." To maintain synchronization, a series of pulses is sent down the channel whenever the scrambling buffer is reinitialized, and these high pitched pulses send like "cricket chirps" interleaved with the signal.

(U) Although the system is described as an "analog" scrambler, it is clearly a 5-stage analog-digital process, in which most of the processing at each end is digital, but the transmitted signal is an analog waveform. It has been tested over the Murray Hill phone system, with addition of simulated white noise and phase roll (a channel impairment).

(U) Because sample-to-sample fidelity is important to speech reconstruction, i.e., the sampled speech at the receiver must match the samples that are supplied to the digital-toanalog (D/A) converter at the transmitter, it is necessary to equalize the channel to compensate for channel distortions and to synchronize the instants of sampling at each end. The synchronization pulses (cricket chirps) are used to establish and maintain sample timing and are also used for channel equalization (since they give the impulse response of the channel).

(U) The main thrust of the designers' work was to get good intelligibility. They now want to reduce the software algorithm to a hardware device, and VLSI design can follow from there. The audience showed substantial interest in this scheme.

(U) Despite the rapid introduction of digital channels, for many years to come, most of the world's telephone connections will be made over copper circuits that will not support high bit rate digital speech. One of the driving forces behind the development of digital transmission and local loops is the desire for high-quality secure speech. If the hybrid analog-digital scrambling gives good enough speech quality, and no particular security weaknesses become known, the market pressure to develop digital services to the 64,000-bps level IDN ( = Integrated Digital Network) may reduce (since customers won't have to buy them) and this could affect an important part of the digitization of the telephone network.



May 83 \* CRYPTOLOG \* Page 8

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

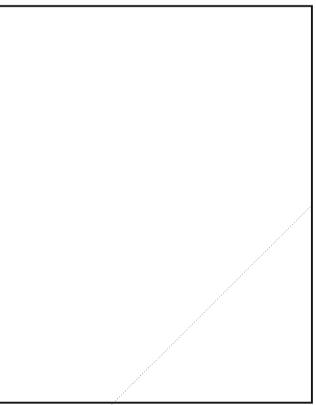
TOP SECRET UMBRA

(U) The Desmedt paper on Super-DES began with a critique of existing cryptographic methods, interleaved with some familiar commentary on NSA intervention in the DES design. A point of interest is the statement that the Geneva Management Group in 1981 concluded that DES was not adequately secure. Desmedt argues that encryption algorithms that iterate the basic operations many times provide higher security than the individual operations (e.g., substitution, transposition) but are impractical to implement on VLSI chips. He also argues that a DES-breaking special machine may be costly today, but in 20 years could be cheap enough to break messages enciphered on He also acknowledges that no DES now. "shortcut" solution to DES is known. Hellmann's insinuation that a "trapdoor" was built into DES by NSA is referred to. The problem of public key algorithms such as the Merkle-Hellmann scheme is described as either they have known weaknesses or they may have

This is undoubtedly a reflect Fon <sup>1</sup>of<sup>4</sup> the rapid transborder flow of technical information between academicians and the arrival of increasingly capable people into the arena of public cryptology. Without doubt, the technical quality of the work will increase and will threaten SIGINT.

(U) The particular cryptographic scheme that Desmedt et al propose is a version of DES in which blocks of data of 1,600 bits are enciphered, under the control of a 160,900-bit key. The S-boxes of DES are replaced by oneway knapsack functions. This revised "S box," instead of operating on eight bits, operates on 200 bits, and there are eight of them operating in parallel. Each of the new "S boxes" is initialized with 100 integers of 20 bits, so that it contains 20,000 bits. There are eight "S Boxes," which use up 160,000 bits of the key. Because of the trapdoor function, even if the 160,000 bits were known and all the S-box outputs were known, it would still be very difficult to compute the 800-bit input. However, the 160,000-bit key is not known. It is kept secret. That makes it even harder to compute the input from the output. The 200-bit outputs are expanded up to 208 bits and then hashed down to 100 bits to give the 800-bit output. This complicated process is iterated a number of times. A stream or block mode with this algorithm is possible.

unknown weaknesses. What is notable about all of this critique is that the authors are professors of mathematics in Belgium and they are very up-to-date in the state of cryptology in the public domain. (One of them spent 1978-79 at UCLA, Berkeley, doing pertinent research.)



EO 1.4.(c) May 83 \* CRYPTOLOG \* Page 9 P.L. 86-36

(U) Yiu and Peterson of Hewlett-Packard gave a paper on a single-chip VLSI Public Key algorithm. The algorithm is Hellmann's discrete exponential scheme using Galois Field arithmetic. The chip has 12,000 transistors and is designed for a 4-MHz clock rate. The Public Key algorithm would be used in conjunction with DES, to distribute keys for the DES algorithm. The purpose of the chip design was to give higher speed and lower cost for encryption. The use of Galois Field arithmetic eliminates the need for carry or borrow operations, and the arithmetic operations can be executed by linear feedback shift registers. The developers expect to use the chip in a computer network, but the company, according to Yiu, has no commitment to market it.

(U) Doctor Yiu mentioned the recent Racal Milgo patent for finding large prime numbers in a few seconds as an important breakthrough in implementing Public Key networks. The patent, No. 4,351,982, claims that it reduces microprocessor computation time to find a set of 200-bit primes from 1,200 hours to two hours. Desmedt stated in his talk that the RACAL MILGO datacryptor took only 17 seconds to distribute key (but it was not clear that it would find RSA primes in that short time). Hollander of BTL (Bell Telephone Labs) has a patent application that purports to find large primes very quickly. The Japanese are developing a chip that will do RSA encryption at 50,000 bps. The work is a joint project of NTT, NEC, Hitachi, Fujitsu, and Oki. Sandia has developed an algorithm that will do multiplication modulo C in log2(C) + 7 clock pulses, which is an improvement over the conventional modular multiplication, which takes N x N clock pulses for an N-bit modulus. The Sandia method would take only N + 7 clock pulses. It is aimed at RSA encryption using 512-bit prime numbers. At 20-MHz clock speed they expect to be able to encrypt at 25 Kbp/s. Now that the RSA Public Key algorithm has been publicly identified by a former NSA Director as secure, there will undoubtedly be intensified work to make it easier to use to set up DES links. The high utility of being able to dial up any other party and set up a secure link, without prior key distribution, is

irresistible from both intellectual and marketing viewpoints.

(U) A paper on the AMD DES chip was given by Brown, an AMD executive. This was followed by some discussion of the merits of DES. Both Yiu and Brown felt that DES was in fact secure, and that the criticism that Desmedt and other authors had raised were not supported by any facts. No one had been able to read or exploit DES, and it had the advantage of a standardized tested algorithm. The AMD DES chip was capable of 1.7 Mbytes/sec, so that it could be used for disc controllers. It cost \$75 for a single unit.

(U) Another paper at the cryptographic meeting was an Italian scheme by CSELT for a "robust" 4800-bps speech coder. Audio tapes showed it to be resonant and of low quality. The paper did not seem to offer any important new work. However, the topic of speech coding and other compression coding was treated at five other sessions. There were 31 papers on voice and image compression, of which 16 were by foreign authors. The sessions were:

- [] A8 : Low bit rate speech coding
- [] B6 : Image processing
- [] D4 : European videoconferencing
- [] E6 : Advances in speech coding
- [] F7 : Speech processing

(U) The interest in compressed speech in sessions A8, E6, and F7 was initially to allow narrowband encrypted voice signals. Now a number of other applications, including lowcost bandwidth conservation and interim storage of voice, have emerged from the capability to compress speech.

(U) The interest in compressed video is for both teleconferences and private TV broadcasts (e.g., Pay-TV, TV relay by satellite, and Direct Broadcast Satellites (DBS)). The common carriers and the broadcasters both see commercial advantages in being able to send TV signals that can be securely encrypted. Because bits/sec cost money, the customers want the pictures compressed.

(U) In Europe there is a multinational effort to develop a standardized videoconference system, with a standard video coder. Some of this is for satellite applications, to thwart interception, but most of it will

May 83 \* CRYPTOLOG \* Page 10

probably pass overland on radio relay and optical fibers. The compression allows cheaper conferences and security, and the standardization will allow the Europeans to intercommunicate and keep US companies out of the equipment market.

(U) There are now hundreds of papers published on vocoders, fax coders, encryption, video coding, etc. Many of the papers are foreign, but the Europeans in particular have been handicapped in the speech area, for example, by the lack of specialized journals which consolidate the work. As as result, they look to the US journals, especially the IEEE publications, as the focus of the current work. This also makes it difficult for US parties to keep up with the foreign work because it is spread across a number of journals and is often published in German, French, Italian, Swedish, Japanese, etc. However, the foreign literature is growing, and will become a more important source of new work in cryptography and coding.

(U) The Europeans, arriving on the scene after the US has identified the problems and paid for the basic research, will be able to converge on coding and encryption standards to serve many of their PTT plans, without the competition, confusion, public controversy, and divided purposes that have arisen in the US in both Government and civil coding and encryption. By the end of the decade, they may have passed the US in these fields, just as they have surpassed the US in a number of other selected technologies and industries.

#### References:

- 1. GLOBECOM 82 Conference Record
- 2. US Patent 4,351,982 (RACAL MILGO)
- 3. E.F. Brickell, <u>A</u> Fast Modular Algorithm with <u>Application</u> to <u>Two</u> Key Cryptography, Sandia National Labs. Re DE-AC04-76DP00789
- Simmons, G., and M. Norris, <u>How to Cipher</u> <u>Faster</u> <u>Using Redundant Number</u> <u>Systems</u>, Sandia National Laboratories, Aug 1980.
- 5. Miyaguchi, A., S. Mizuta, K. Furuie, T. Tsujiguchi, and H. Mizuta, <u>Combination</u> <u>Type</u> <u>Computer</u> <u>Circuits</u> for <u>Code</u> <u>Handling</u>, <u>NEC</u>, 1981.
- 6. NTIS Search Vocoders, V1,2, 1982.

- Inman, Bobby, <u>Science</u>, V218, 24 Dec 1982, p. 1290.
- NTIS PB-806860 Vocoders 1970-82, abstracts from the Engineering Index. Apr 82. Contains foreign vocoder abstracts. (In P1 library)
- NTIS PB-82-806852, Apr 82. Vocoders. Citations from NTIS data base. US literature (In P1 library)
- NTIS PB 82-863671, Mar 82, Facsimile Communications, Citations from INSPEC data base. (Contains many foreign literature references)

#### Digital Telephony by John C. Bellamy, Wiley, 1982.

-(2)- Is "plesiochronous"a familiar word? It soon will be, if you are concerned with international digital networks. A plesiochronous network does not synchronize the network, but merely uses clocks at each node that are accurate enough to keep the bit slip rate low enough not to interfere with operation. The US domestic digital network is synchronized, to save the cost of the node clocks, but the CCITT has established clock standards to interface different national networks by plesiochronous gateway connections. Because the national networks run at slightly different rates, and COMSEC will have to anticipate this plesiochronous structure.1.4.(c) P.L. 86-36

(U) Network synchronization schemes are just one small part of John Bellamy's new book on digital telephony. The author, who received his PhD in EE in 1971, worked as a manager at the Collins Division of Rockwell International in transmission systems, then as a member of the technical staff at Arthur A. Collins, Inc., the R&D firm that hived off from Collins Radio when Rockwell took them over. He is now an R&D manager at the Communications System Division of United Technologies, so he has substantial practical experience with modern telecommunications It is notable that Collins engineering. builds digital radio equipment so well that Western Electric dropped some of its own projects and buys from them. In addition to his industry experience, Dr. Bellamy has been an Adjunct Professor of Electrical Engineering and Computer Science at Southern Methodist University since 1976, so he is used to

#### TOP SECRET UMBRA

organizing,	simplifying,	and	teaching
engineering	technology.		

(U) His book is a well-written tutorial on telephony and digital telecommunication. Although digital transmission was developed with computer and data traffic in mind, the main traffic volume will be voice for a long time. Analog transmission and networks will also be around for a long time, but digital telephony is of particular interest where encryption is wanted (as he says on page 75) because of the paucity of good analog encryption.

(U) The book covers digital networks from a general overview of the analog network in the US, through voice digitization algorithms (PCM, DPCM, APC, vocoders, etc), fundamentals of digital transmission, switching and multiplexing, through digital modulation, network synchronization and control, to high-level descriptions of several digital networks and a discussion of the future of digital telephony. Among other things, the book has a 16-page glossary of pertinent terms, such as burst isochronous, Centrex service, despotic network, elastic store, HDB3 code, justification ratio, mesochronous, muldem, permanent virtual circuit, plesiochronous, robbed digit signaling, state store, transhybrid loss, traveling class mark, and waiting time jitter. These terms are indispensable refinements in educated discussions of networks. (This glossary will soon be in the NSA terminology base).

(U) Some points of interest in the book:

- [] One of the principal difficulties in making the large telephone network operate is the variety of signals and signaling func-'tions, all of which have to be translated by interfaces or made compatible.
- [] Common Channel signaling in the Bell System is highly centralized, making the entire network vulnerable to failures in the CCIS packet traffic.
- [] If a CCIS node fails to store and forward certain network information correctly, the network will gradually lock up because disconnects do not occur automatically.
- Digital microwave radio is cheaper than T-carrier for distances as short as eight miles, and the major impetus for digital radio has been the introduction of digital switches, not the demand for digital traffic, which can pass over the analog network.

- [] Fifteen different types of digital central office switches are in service in the US, and more are expected as foreign suppliers enter the US market. The disadvantages of digital networks are increased bandwidth, A/D and D/A conversion, time synchronization, topologically restricted multiplexing, and incompatibility with the large analog plant.
- Voice digitization, nominally 64,000 bps, can be as great as 400,000 bps for specialized services such as broadcast transmission.
- [] About ten different speech coding schemes are described.

(U) In the chapter on digital switching, the advantage of time-domain switching is shown to be the ease of getting switches that don't suffer from blocking. There is guite a lot of information in the switching chapter. The chapter on network synchronization examines many of the timing problems and the solutions such as bit slips, elastic stores, pulse stuffing, and packetization. The chapter on digital networks leads from ARPANET to the ISDN (integrated services digital networks). Circuit-switched nets are shown to be more efficient for voice transmission than packetswitched nets, but digital speech interpolation can increase the effective number of channels on a trunk if the circuit switching is fast enough. Current circuit switching can operate fast enough so that even the beginnings of syllables are not lost. The final chapter is on traffic analysis, as the traffic engineers and designers do it.

(U) The book is well written and well illustrated, with references and exercises. Because of the integration of transmission and encryption, as well as the continuous growth and switchover into digital networks in every country, a knowledge of the engineering and technology of digital networks will be an essential part of a cryptologic repertoire. Bellamy's book is a good beginning to this knowledge. The enciphered speech cryptanalytic experts in R52 ordered desk copies after reviewing the book.

(U) Summing up, <u>Digital</u> <u>Telephony</u> is timely, gives good coverage of digital networks, and should be a useful text and reference for some years. It costs about \$50.



May 83 \* CRYPTOLOG \* Page 12

#### TOP SECRET UMBRA

SECRET

CUMULATIVE

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

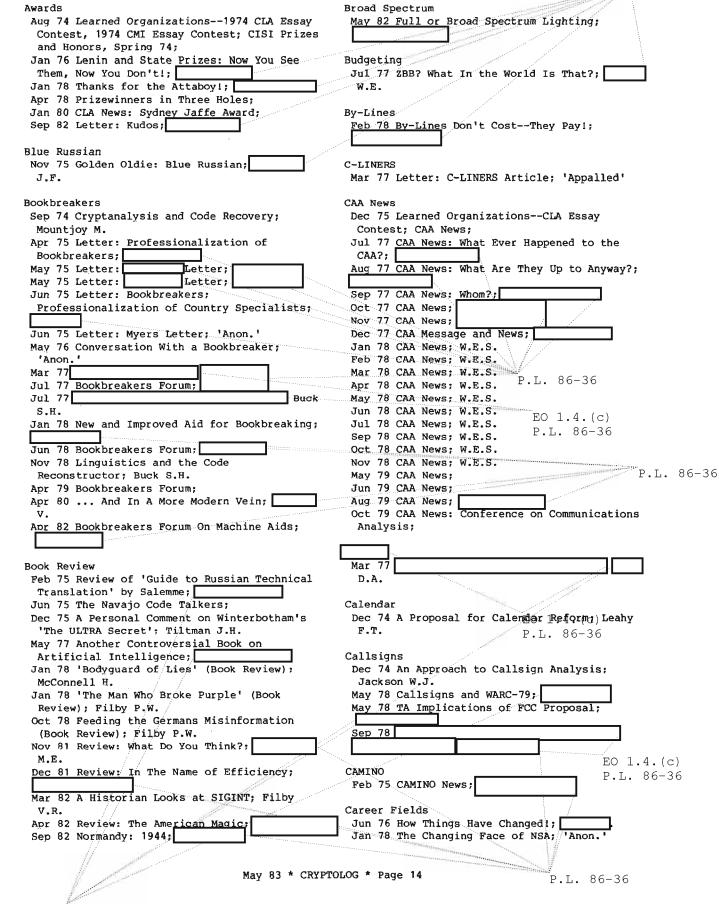
# Part Three: Keywords

.

The following cumulative index of CRYP-TOLOG (Vols. I through IX, 1974-1982) was produced using UNIX/PINSETTER tools on MYCROFT and BARDOLPH1. The index is in three parts, and is being published in three successive issues. Part one is an index by author; part two is an index by title; and part three is an index by title; and part three is an index by keyword. Items in multiple issues (February-March 1975, for example) are indicated by the first month (i.e., by Feb 75).

HANDLE VIA COMINT CHANNELS ONLY

and the second	P.L. 86-36
and the second	Amerind
AAAS	Sep 74 Language in the News;
Feb 82 Gayler - AAAS, 1982;	
Feb 82 Software - AAAS, 1982;	AOC News
	May 82 Is There An Old Crow In Your Future?;
ABNER	
Aug 77 Early Days in NSA Computing; Chauvenet	
L.R.	Appraisal System
Nov 77 Letter: Article; Snyder S.S.	Nov 78 Letter: Appraisal System: 'Anon.'
Jun 78 Equipment Maintenance on ABNER;	Nov 78 Letter: Appraisal System;
	· · · · ·
•	Arabic Sep 74 Language in the News;
Acronyms Apr 80 OH, K!;	Dec 74 Language in the News;
	Apr 75 Language in the News; Tetrault E.W.
Africa	Apr / J Danguage in the news, research
Nov 77 How Many African Countries Can You	
Spot?;	Sep 74 COMINT Analysis of
Afrikaans	Dec 74 Letter: Article; 'Anon.'
Sep 74 Language in the News;	
	Archives
AG-22/IATS	Jun 78 Never Againl: Gurin J. P.L. 86-36
Mar 76 Musings About the AG-22/IATS; Phillips	Nov 78 Never on My Watch;
May 76 What's Wrong with AG-22/IATS?;	Arms Control
	Feb 82 Gayler - AAAS, 1982;
Jun 76 Comments on AG-22/IATS;	·····
Jun 76 Comments on AG-22/IATS;	Artificial Intelligence May 77 Another Controversial Book on
Jun 76 Comments on AG-22/IATS; Jun 76 Comments on AG-22/IATS;	May 77 Another Controvers <u>ial Book on</u> Artificial Intelligence;
Jun 76 Comments on AG-22/IATS; Jun 76 Comments on AG-22/IATS;	Artificial Intelligence: Sep 77 The Doctor Is In(capable of
Jun 76 Comments on AG-22/IATS; Jun 76 Comments on AG-22/IATS;	Sep // The Doctor is in(capable of Diagnosing); Chauvenet L.R.
Jun 76 Comments on AG-22/IATS; Jun 76 Comments on AG-22/IATS;	Didynostny); Chauvenee D.K.
Jun 76 Comments on AG-22/IATS;	Asia
Sep 76 More Comments on the AG-22/IATS:	Aug 76 Integrated Analysts for Asia;
B.	W.D.
Oct 76 Another Word on AG-22/IATS;	
M.A.	Ask Art
Apr 77 The Last Word on IATS?; Phillips C.J.	Apr 79 Letter: Ask Art; 'Sue'
Jun 77 AG-22/IATS: A View From the Bridge;	P.L. 86-36
	Assignments
Sep 77 Another Last Word on IATS;	Jan 80 Coming Home;
P.A.	· · · · ·
Oct 77 Letter: AG-22 Page Print; 'Reader'	Automation Oct 75 Automation of a TA Process: Murnhy T
L /	Oct 75 Automation of a TA Process; Murphy T. Sep 77
American Mágic	Sep //
Apr 82 Review: The American Magic;	лана алана алан
May 83 * CRYPT	<b>COLOG * Page 150</b> 1.4. (c)
P.L. 86-36	P.L. 86-36



- SECRET

P.L. 86-36

HANDLE VIA COMINT CHANNELS ONLY

SECRET

R.L. 86-36

Jan 81 Why Do They Leave?; Ciphers; Nov 82 The Costs of Muddling Through; Gould Feb 76 What Is Cipher Text?; May 76 A Simple Cipher Story; R.E. Sep 76 Another Cipher by ...; Jun 77 Old Russian Manuscript Ciphers; Career Panels Aug 74 A Short Directory of Career Panels; Feb 79 Language Career Panel: Clarification of Nov 78 Item: Cipher Devices Apr 79 But, Mr. Boak, Did You Ever Try To Get CARRIAGE Rid of One in a Hurry?; D.H.W. Sep 74 Project CARRIAGE: Worldwide HFDF Modernization Plan; Webster J.B. Cipher Systems Oct 75 Computers, Comms, and Low-Grade Ciphers: Catalogs Oct 81 Technical Support Catalogs; K.J. EO 1.4.(c) CIRC Jan 80 CIRC: An Intelligence Data Base; Celtic Jun 78 Celtic Languages Today; CISI News Censorship Nov 75 When Censorship Backfires; Aug 74 Learned Organizations--1974 CLA Essay Contest, 1974 CMI Essay Contest; CISI Prizes and Honors, Spring 74; Central Information Dec 74 Learned Organizations--CISI Forms Apr 75 A Guide to Central Information, C5; Special Interest Group on Human Factors; Central Research Nov 82 Central Research and The Paper Blob: Jan 75 Learned Organizations--IAI News, CISI News; CLA is Ten Years Old1; CMI News; Mar 79 CISI News; Certification May 79 CISI News: Spring Conference; Mar 76 A Comparison of NSA and ATA Classic Cables Certification Standards; P.L. 86-36 Sep 76 Is There Life After Certification?: Mar 79 Classic Cables; Apr 79 Classic Cables; May 79 Classic Cables; Changing Environment Apr 81 Classic Cables: Jan 80 There's a New World Coming - Are You Classification Ready?; May 75 Codeword or COMINT Channels?; Chinese н. Jan 77 Letter: Use of Term 'Compartmented'; Sep 74 Language in the News; Oct 74 Character Building in the People's Jul 77 Classification Corner; Republic of China; Hamlett G., Reed M. Sep 77 Classification Corner: XGDS-2; Oct 74 Even a 5-year-old Child ...; Tetrault E.W. Oct 77 Classification Corner: A Bigger Picture; Oct 77 Classification Corner: Who Said?; Jun 76 An Evaluation of a Scientific Chinese Machine Translation; Kermisch H. Jun 76 Notes on Translation from the Chinese; Jan 79 It's Party Time!; . P.L. 86-Nov 77 Backing into Language Acquisition; CLA News Aug 74 Learned Organizations--1974 CLA Essay Contest, 1974 CMI Essay Contest; CISI Prizes Mar 78 and Honors, Spring 74; Jun 78 Jan 75 Learned Organizations--IAI News, CISI News; CLA is Ten Years Old!; CMI News; Jul 78 Letter: Article; Jul 78 Tell Me I'm Just a Sinobibliophobe; Apr 75 Language in the News; Tetrault E.W. May 75 Learned Organizations--CLA News; IAI News; Jul 75 Learned Organizations--CLA News; CMI Dec 82 News; Dec 75 Learned Organizations--CLA Essay Ciphers Codes and Contest; CAA News; Feb 75 Basic Patterns of P.L. 86-36 May 83 \* CRYPTOLOG \* Page 15 EO 1.4.(c) P.L. 86-36 BECRET HANDLE VIA COMINE CHANNELS ONLY

P.L. 86-36 SECRET

Sep 76 Learned Organizations--1976 CLA Essay Garofalo C.A. Contest; 1976 CMI Essay Contest; Mar 78 CLA News; Comic Strip Sep 78 CLA News; Sep 77 Al Balloni, Editor; A.J.S. EO 1.4.(c) Feb 79 CLA News: Russian Institute; Jan 79 Al Balloni, Editor; A.J.S. P.L. 86-36 Oct 79 CLA News; Jan 80 CLA News: Sydney Jaffe Award: COMINT Sep 74 COMINT Analysis of Jan 81 NCS-CLA Symposium; Jan 75 The Case for COMINT Readers; Clustering Apr 78 A Little PEP Talk; H.G. Apr 76 Golden Oldie: Hidden Losses in COMINT CMI News Production; Gould R.E. May 76 COMINT in the Russian Navy, WWII; Aug 74 Learned Organizations--1974 CLA Essay Contest, 1974 CMI Essay Contest; CISI Prizes and Honors, Spring 74; Jan 78 COMINT, COMSEC, and Hilbert's Tenth; Jan 75 Learned Organizations--IAI News, CISI News; CLA is Ten Years Old!; CMI News; Feb 79 The COMINT Chain 'Gang'; Jul 75 Learned Organizations--CLA News; CMI News; Communications Sep 76 Learned Organizations--1976 CLA Essay Oct 75 Computers, Comms, and Low-Grade EO 1.4.(c) Contest; 1976 CMI Essay Contest; Ciphers: P.L. 86-36 Jan 79 CMI News; Aug 79 CMI News; Apr 80 EO 1.4.(c) P.L. 86-36 Communications Changes Codes P.L. 86-36 Sep 74 Cryptanalysis and Code Recovery; Apr 75 A Comm Change at Ramasun Station; Mountjoy M. Oct 82 Golden Oldie: The Reality of Feb 75 Basic Patterns of Codes and Communications Changes; Ciphers; Jun 75 The Navajo Code Talkers; Jun 76 The Marquis and the Medium; Computers Nov 78 Linguistics and the Code Aug 74 Right-to-Left Text Sorts Are Not Reconstructor; Buck S.H. Impossible; Dec 74 Flag-Waving Programmer; John G. Mar 82 Jan 75 The Yawn of the Computer Age or When EO 1.4.(c) **Collection**  $P_{L}$  86-36 Your Terminal is Terminal; Aug 74 What Is a Collector?; Jun 75 Professionalizing in Computer Systems; Dec 74 The New Collection Criteria; Aug 75 Computer Network Resources In C5; Aug 75 Abdul and His 40 Tanks; Mason F.O. System; Oct 75 Computers, Comms, and Low-Grade Feb 76 The Ciphers: The Southeast Asian Exploitable May 76 Some Principles of Cover and Message Processing System; P.L. 86-36 Deception: Jun 76 The Collection System; Murphy Apr 76 What's the Best Location for the т. Computer Applications Function?; Aug 76 NSA Cryptologic Collection; C.E. Jun 76 Computers In The ELINT and Telemetry 1.4.(c) Oct 76 Another Word on AG-22/IATS; M.A. Business; 86-36 Mar 77 A View of the Central Computer Complex Jan 77 Where Were We?; Mason F.O. Nov 77 Director's Memorandum: in the Late 1970s and Early 1980s; Phillips Guidance'; Inman B.R. C.J. Nov 77 Objective Satisfaction Score: Mar 77 An <u>Overview of Proj</u>ect Collection Performance; Coyle J., Jan 78 An Early NSA Proposal for Satellite Apr 77 Contemplating Computing; Remoting; Nolte W.M. May 77 Universes, Galaxies, Stars, Bars, and Jan 78 What Ever Happened to COPES?; Other Concepts; Phillips C.J. W.E. Aug 77 Early Days in NSA Computing; Chauvenet Feb 78 Collection-Support TA is Not for L.R. Apr 78 Remedial Software Engineering; Everyone; Jun 78 J.F. Jan 81 KITTIWAKE; May 78 The Joys of UNIX; Oct 78 Data Security and Human Error; Color Code J.M. Sep 74 Gary's Colors; Garofalo C.A. Jun 79 Teaching Computer Science To Feb 82 Golden Oldie: Simplicity in Color; Linguists; P.L. 86-36 May 83 \* CRYPTOLOG \* Page 16 EO 1.4.(c) P.L. 86-36

EO 1.4.(c		EO 1.4.(c)
O <b>ĠIÐ :</b> 86 <b>-4</b> 0	009861	P.L. 86-36 P.L. 86-36
	Jan 80 Analysts of NSA, Arise!:	
	Nov 81 How to Create A User-Unfriendly	Jul 77 Which Tape Has the Intelligence?
	System: Nov 81 The PPC Is Coming!;	Project Gurin J.
	Dec 81 In Pursuit of: Faster Horses, Younge	CRITIC
	Women, Older Whiskey and More Money;	Nov 78 Wedding Bells and That Old Gang of
	D.L. Dec 81 PLATFORM: How Did You Say That Works	Mine; Sawyer E.L.
		CRT
	Feb 82 Human Factors Corner: Some Advice to Users of Unfriendly System;	Mar 78 A Linguist Looks at the Tube;
	Feb 82 Software - AAAS, 1982;	Mar 78 The Hand Is Not Quicker Than the Eye;
	Mar 82 A Personal Computer: A Current	
	Cryptanalysis Support Tool: Mar 82 Human Factors <u>Corner: Consume</u> r vs.	Aug 82 Human Factors Corner: Video Display Terminals and Vision of Workers;
	Computer: A Review;	м.е.
	Apr 82 Personal Computer Application;	Cryptanalysis
4 A A A A A A A A A A A A A A A A A A A	Apr 82 Word Processing In A4;	Sep 74 Cryptanalysis and Code Recovery;
	Sep 82 TSS Revolution;	Mountjoy M.
	Oct 82 Human Factors Corner: Text Editors;	Oct 74 An October Overlap; Nov 74 Answer to An October Overla :
	Oct 82 What's The Good (Pass)Word?;	J.E.
	Dec 82 Going On-Line With Information Aids; Gurin J.	
	Gurin J. P.L. 8	6-36 Dec 74 Puzzle: Secret Messages, 'Military
	Computer Aids	Cryptanalytics':
	Apr 76 Computer-Aided Transcription of	May 75 TA, Handmaiden of CA; Mason F.O. Jul 75 Re-psychling the Code Clerk;
		Jul 75 Too Many Garbles
	Computer Security Mar 79 Computer Operating System	Aug 75 Twenty Years of Transposition;
	Vulnerabilities:	Aug 75 Typewriter Random A New Look;
P.L. 86-36	Jun 82 Some Reflections On The Reality of	Oct 75_Letter: Typewriter Keyboard;
	Computer Security; Hanyok R.J. Oct 82 What's The <u>Good (Pass)Word</u> ?;	Oct 75
	Dec 82 Passwords;	F.
	Computer TA P.L.	Feb 76 What Is Cipher Text?; 36-36 May 76 A Simple Cipher Story;
	Apr 80 A Traffic Analyst Looks at Computers	; Aug 76 The Hierarchical Clustering of
		Cryptanalytic Data; Nov 76 Teacher Learns a Lesson;
	COMSEC	Aug 77 Want to Play with a Pickfair Square?;
	Jun 75 COMSEC Familiarization: Do You Need	Dec 77
	It?; Jan 78 'Bodyguard of Lies' (Book Review);	Jan 78 'The Man Who Broke Purple' (Book
		L. 86-34eview); Filby P.W.
	Jan 78 COMINT, COMSEC, and Hilbert's Tenth;	Apr 78 Looking at Mr.
	Apr 79 COMSEC/SIGINT Relations: Boak D.G.	May 78 The Future of Cryptanalysis; Lutwiniak
	Nov 82 COMSEC Challenges;	Jun 78
	EO 1.4.( P.L. 86-	
	Nov 76 Check Your Morse Front-End Alignment	; Jan 82 Letter: Cryptanalysis Article;
	'Anon.' Jan 78 What Ever Happened to COPES?;	Mar 82
	W.E.	Dec 82 Does Anybody Here Remember PURPLE?;
	Jun 78 Letter: Article; Gilbertson E.A.	
	Sep 78 Letter: Gilbertson Letter;	Cryptanalysts
	Coverterms	Aug 74 What Should You Expect? or, The Analysis of Cryptanalysts;
	Apr 75 Coverterms; Filby V.R.	Jun 76 Row Things Have Changed1;
	Care and the second sec	
P -	L. 86-36	EO 1.4.(c)
2		P.L. 86-36
	May 83 * C	RYPTOLOG * Page 17

SECRET

P.L. 86-36 Crypto-TA Jun 75 More on Squaring the Page (A Crypto-TA Function); Mason F.O. Data Flow Apr 79 A Somewhat Larger Problem; Apr 80 Data Flow--Challenge of the 1980s; W.E. Phillips C.J. Aug 82 An Old Problem; Oct 82 Answer: An Old Problem; Data Security Oct 78 Data Security and Human Error; Cryptograms J.M. Sep 74 Secrets of the Altars--The Moustier Cryptograms; Data Sorting Aug 74 Right-to-Left Text Sorts Are Not Cryptographic Impossible; Apr 75 Psyching the Code Clerk: Data Standards Nov 74 Data and Definitions: Calling Things Callimahos L.D. EO 1.4.(c) by Their Rightful Names; P.L. 86-36 CRYPTOLOG Nov 78 Data Standards Center; Pattie M.T. Aug 74 CRYPTOLOG A Letter of Introduction; Dec 78 a/k/a Sam; Wolff H.E. Feb 79 Data Standards Without Tears; Dec 74 CRYPTOLOG Index for 1974; P.Q. Jan 75 CRYPTOLOG Index for 1974; Feb 79 Well, Maybe a Sniffle or Two...; Dec 75 CRYPTOLOG Index for 1974-1975; Pattie M.T. Mar 79 Data Standards Without Tears: A Nov 76 Letter: Cumulative Index; Bostick C.W. Dec 77 CRYPTOLOG Index for 1977; P.L. 86-3 Comment; Mar 78 An Idea for an Article; Miller D.E. Mar 79 Letter: Data Standards; Dec 78 CRYPTOLOG Index for 1978; Jun 79 ... Mr. Pattie Replies; Pattie M.T. Jan 79 Letter From the Publisher; Lutwiniak Jun 79 Data Standards Without Teeth; P.Q. ω. Mar 79 Readers' Survey; D.H.W. Aug 79 An August Baudy; May 82 CRYPTOLOG Numbering; Jan 82 Data Field Naming/Coding Conventions at NSA; Aug 82 All I Ever Wanted To Know About DES; Cryptologic Mission Feb 79 Let's Not Forget Our Cryptologic Mission: Gurin J. Apr 79 Letter: Gurin Article (Feb 79); Dates Jul 77 Dating Game; Williams D.H. Aug 77 Postscript to 'Dating Game'; Cryptology Jan 76 Football and Cryptology; P.L. 86-3 Feb 78 First Lady of Navy Cryptology Deception Feb 76 How Do We Know It's True?; Filby V.R. R.P. May 76 Some Principles of Cover and Cryptosystems Deception; Oct 75 The Do Xa Pads; Wiley E Jun 76 'Right On, Veral'; Sep 78 Jun 79 M.R. EO 1.4.(c) Crypto Devices Aug 82 AFCEA 82 and ICC-82: New Crypto 86-36 Degarbling Devices; Sep 77 D.L. CSI News Dec 77 Letter: Article; Dec 75 Establishment of CSI Newsletter; DESKPAD Cyrillic Nov 75 DESKPAD: A Programmers's Tool; Jun 76 Transliteration or Cyrillic?; н. G. DIALOG Data Bases Aug 77 DIALOG Available at NSA; Jan 75 How Clean Does a Data Base Need to Feb 79 Literature Search On-Line; Miller M.E. Be?: Feb 79 Literature Search On-Line; Miller M.E. Dictionaries Jan 80 CIRC: An Intelligence Data Base; Feb 75 Glossaries versus Dictionaries: Which Should It Be?; Gurin J. Nov 82 Central Research and The Paper Blob; Feb 75 The Devil's Dictionary: May 83 \* CRYPTOLOG \* Page 18 P.L. 86-36

BECRET

SECRET

P.L. 86-36 Aug 76 Note on FRANCOPHONEGLOS; s. May 78 Project UTENSIL: The DDO Data May 79 More Fairbanks On English; Fairbanks Dictionary/Directory; S Jun 79 How Are Your Stamina?; Fairbanks S. Jul 79 Wilt Thou, Angelina ...?; Fairbanks S. Documentation Sep 77 Is There a Doctor in the House?; Equipment Jan 80 System Acquisition Document Review; Jun 78 Equipment Maintenance on ABNER; Bernard R. Jun 82 Human Factors: Responsible Oct 78 Will It Really Do the Job?: Documentation; Apr 79 But, Mr. Boak, Did You Ever Try To Get Rid of One in a Hurry?; D.H.W. Economic Intelligence Oct 79 Another Source; Oct 81 Economic Intelligence: Problems and Oct 79 Snowballs On The Roof; Filby V.R. Aug 82 AFCEA 82 and ICC-82: New Crypto Prospects; Devices; Editor's Note May 76 Scraps from the Editor's Desk; Salemme Equivalency Tests EO 1.4.(c) Nov 75 NCS Offers Course-Equivalency Tests; A.J. P.L. 86-36 and a Little Bit of Luck; Apr 76 NCS Offers Course-Equivalency Tests, Feb 79 Williams D.H. Clarification: Editorial Comment Evaluation Feb 78 No, Winnie, You've Got It Upside Down Oct 7/7 K1: SCA Field Management and Too!; A.J.S. Evaluation: Jun 82 Letter: Editorial Comment; Jul 79 EXPERT; P.L. 86-36 P.A. EW Jun 75 The Role of the Electronic Warfare Efficiency Advisory Element (EWAE) of NSA; Dec 81 Review: In The Name of Efficiency; Oct 76 Russian SIGINT and Electronic Warfare; EO 1.4.(c) P.L. 86-36 ELINT Nov 74 What? Where? Why?; EXPERT Jul 79 EXPERT; G.A. Apr 75 The Uses of ELINT; May 75 Letter: Bloom Article; Exploitation Apr 76 Will the Real ELINT Please Stand Up; Feb 78 Schlauch R.H. EO 1.4.(c) Jul 79 EXPERT; Jun 76 Computers In The ELINT and Telemetry P.L. 86-36 P.L. 86-36 Business; Aug 76 Yes, Don, There is an ELINT!; Field Stations Apr 75 A Comm Change at Ramasun Station; W.L. Nov 76 Letter From Canada; Reese J.C. Oct 75 The Danang Processing Center; Emitter Identification Α. Jan 76 Leo in October; Murphy A.I. May 79 Emitter Identification Techniques; Apr 76 One Day in Danang; Jun 76 Letter: Article: Murphy A.I. Jan 77 Where Were We?; Mason F.O. English Dec 74 Language in the News; Jun 75 Where Does 'Does' Come From?; Tetrault Forms Sep 77 Speaking of Logging ...; E.W. Aug 75 Language in the News; FRANCOPHONEGLOS Nov 76 The Uses of Elegant English: P.L. 86-36 Aug 76 Note on FRANCOPHONEGLOS; J.R. May 77 Choose Ye!; May 77 Plain English; French Aug 74 Nice Busman's Holiday for One NSA Jun 77 Vich Iss R-r-right?; A.J.S. Nov 77 What Ever Does 'However' Mean?: Employee; Sep 74 Language in the News; Jan 78 The Joys and Frustrations of Plural-Aug 76 Language in the News; EO 1.4.(c) Dropping; A.J.S. Mar 79 Fairbanks on English; Fairbanks S. P.L. 86-36 Apr 79 More Fairbanks on English; Fairbanks P.L. 86-36 May 83 \* CRYPTOLOG \* Page 19

- SECRET

# COCID: 4009861

	P.L. 86-36
French Connection	HF
Dec 76 The French(fried) Connection: Gino the Genie;	Jan 79 The Return to HF; Jan 82 HF The Rebirth;
Frequencies	HFDF
Jan 79 The Return to HF;	Sep 74 Project CARRIAGE: Worldwide HFDF
Jan 82 HF - The Rebirth;	Modernization Plan; Webster J.B.
Jun 82 Amateur Spread Spectrum;	Nov 74 What? Where? Why?;
	G.A. EO 1.4.(c)
	P.L. 86-36
Feb 76 The System;	Hiring
Oct 77 Update on	Oct 74 News from NCSAgency Resumes Hiring
	of LICs; NCS Offers Course in 'SIGINT
Games	Appreciation
Oct 76 A Vexing Agency-Wide Problem; Mason	Dec 75 Linguists From The Melting Pot; Gould
F.O.	R.E.
Nov 76 Answer to 'Vexing Problem'; Mason F.O. EO 1.4.(c)	P.L. 86-36
P.L. 86-36	History Feb 75 The Gulf of Tonkin Incident;
Geography	W.D.
Dec 74 Maps in MindA Photoessay;	May 76 COMINT in the Russian Navy, WWII;
Dec 74 Puzzle: Citizens of the World;	May / o control in the muserian wavy / mail,
Nov 77 How Many African Countries Can You	Sep 78 Soviet COMINT and the Civil War;
Spot?;	
Apr 78 +Conoces Bien la Geografia?:	Nov 78 Cast a Double Shadow: The Trojan Horse
Oct 78 Know Your Geography;	of SIGINT;
Dec 78 How Do You Spell Peking?:	Jan 79 W.W.II Japanese Translation at
Feb 79 Know Your Geography;	Arlington Hall Station;
Apr 80 Geographic Trivia;	Mar 79 Pursuit of the
	E.L. EO 1.4.(c)
German	Sep 82 Normandy: 1944; P.L. 86-36
Sep 76 Language in the News;	Dec 82 Does Anybody Here Remember PURPLE?;
Nov 77 Backing into Language Acquisition;	STREET STREET
	Human Restore
Glossaries /P.L. 86-36	Human Factors
Aug 74 The New Traffic Analysis Glossary;	Jun 77 Human Factors and <u>Systems Design</u> : An Estranged Relationship?;
Oct 74 Golden Oldie: An Unofficial Glossary	Oct 77 Human Factors and the Use of
of Weasel Words:	Microfiche Readers at NSA; Snow D.
Feb 75 Glossaries versus Dictionaries: Which	Jan 79 Human Factors Newsletter;
Should It Be?; Gurin J.	Jan 82 Human Factors Corner: Information
Feb 76 Expletives Deleted: Glossing Over a	System;
Glossary;	Feb 82 Human Factors Corner: But What Do I Do
Aug 77 Expletives Deleted?; Salemme A.J.	With My Papers?;
EO 1.4.(c)	Feb 82 Human Factors Corner: Some Advice to
P.L. 86-36	Users of Unfriendly System;
	Mar 82 Human Factors Corner: Consumer vs.
	Computer: A Review;
Oct 76 Letter: Article	May 82 Human Factors Corner: Data Gathering,
Craphics	How Do We Spend Our Day?;
Graphics Dec 75 Graphic Analysis of Linear Recursive	Aug 82 Human Factors Corner: Video Display Terminals and Vision of Workers
Sequences;	M.E.
Dec 76 Graphic Names;	Oct 82 Human Factors Corner: Text Editors:
GUPPY	Nov 82 Human Factors Corner: How Do People
Feb 75 Replacement of the GUPPY Library;	Organize Cooperative Work?;
and an and a second sec	Dec 82 Passwords;
and an and a second second second	
Hebrew	IAI News
Sep 74 Language in the News;	Jan 75 Learned OrganizationsIAI News, CISI
	News; CLA is Ten Years Old1; CMI News;
HELIPAD	May 75 Learned OrganizationsCLA News; IAI
May 79 Project HELIPAD: An Epitaph;	News;
M.L.	P.L. 86-36

May 83 \* CRYPTOLOG \* Page 20

-SECRET

-SECRET

	<b>7</b>	P.L. 86-36
	Indicators	Japanese Nov 76 Toujours La Politesse (Japanese); Buck
	Dec 82 Development and Correlation of	
	Indicators;	S.H. Tul 37 The Manageriation Chille Contents and
	Information	Jul 77 The Transcription Skill: Concepts and Teaching Methodologies;
	Jan 82 Human Factors Corner: Information	Jan 79 W.W.II Japanese Translation at
	System	Arlington Hall Station;
	May 82 The NSA Information Desk: 'No	Allington dall Station,
	Comment';	JPRS
		Sep 77 JPRS Language Reference Aids;
í l	INKSTAND	
	Jun 77 SIGINT Welcomes INKSTAND;	
		Keyword Spotting
	Intelligence	Mar 77 Letter: Keyword Spotting; Gurin J.
	Dec 75 What Are We Ab <u>out? (Fragments</u> ,	EQ 1.4.(c)
	Figments, or What?);	KITTIWAKE P\L, 86-36
	Apr 76 Letter: Comments on Letter	Jan 81 KITTIWAKE;
	on What Are We About?;	
- ACCEPTION OF THE OWNER OF THE O	Apr 76 Letter: What Are We About? Article;	
P.L. 86-36		Dec 78
	Intelligence Community	Dec 78
	Aug 77 New Directions for the U.S.	
	Intelligence Community; Gaddy D.W.	anne ann
	Incollegence community, duddy bins and	KRYPTOS News
	Intern Program	Feb 82 KRYPTOS: A New Society;
	Sep 74 A Long Hard Look at the Intern	Dec 82 KRYPTOS News;
	ProgramProgram Philosophy; Recruitment	
	(Part One); 'Exinterne'	Language
•	Oct 74 A Long Hard Look at the Intern	Aug 74 Nice Busman's Holiday for One NSA
	ProgramSelection and Orientation (Part	Employee; Dudley B.
	Two); 'Exinterne'	Aug 74 The Language of Beisbol in Everyday
	Nov 74 A Long Hard Look at the Intern	Talk; , Santiago-Ortiz R.A.
	ProgramMotivation and Morale (Part Three); 'Exinterne'	Sep 74 Language in the News; Oct 74 Character Building in the People's
	Dec 74 A Long Hard Look at the Intern	Republic of China:
	ProgramWhat Happens to the Graduate? (Part	Oct 74 Even a 5-year-old Child; Tetrault
	Four); 'Exinterne'	E.W. P.L. 86-36
	Feb 75 Letter: Exinterne Articles; Tetrault	Nov 74 Purity of the Russian Language-
	E.W.	Slavophiles vs. Westernizers;
	Apr 75 Letter: Exinterne Articles;	Dec 74 Language in the News;
EO 1.4.(c)		Dec 74 The Old Section;
P.L. 86-36	Interpreters	Jan 75 The Case for COMINT Readers;
	Feb 75 The Faithful EchoThe Role of the	H.G.
	State Department Interpreter;	Feb 75 The Faithful EchoThe Role of the
	Oct 77 The Perils of Being a State Department	State Department Interpreter;
	Interpreter; Feb 78 The Unseen Go-Between; Gurin J.	Apr 75 Language in the News; Tetrault E.W. Jun 75 The Navajo Code Talkers;
	red /o the onseen do-between; durin 5.	Jun 75 Where Does 'Does' Come From?: Tetrault
	IRA	E.W. P.L. 86-36
	Aug 77 What Is an Information Research	Aug 75 A Fix for the Language Problem?;
EO 1.4.(c)	Analyst?;	
And the second sec		Aug 75 Language in the News:
	d Strengthere and the second	Oct 75 Language Lessons Learned: A Personal
	Oct 79	Memoir;
		Oct 75 Tactical Language Exploitation: A
	IRONHORSE	Lesson Learned?;
	Oct 75 IRONHORSE: A Tactical SIGINT System;	Nov 75 Golden Oldie: Blue Russian;
		J.F.
	Oct 76 Letter: IRONHORSE Article;	Feb 76 Expletives Deleted: Glossing Over a Glossary:
	ISHTAR	GIOSSATY: Mar 76 1976 Language Meetings and
	Jan 75 The SIGINT Users' Handbook or: What's	Conferences;
	an ISHTAR?;	Mar 76 A Comparison of NSA and ATA
		Certification Standards;
	May 83 * CRYP	TOLOG * Page 21 P.L. 86-36

-SECRET-

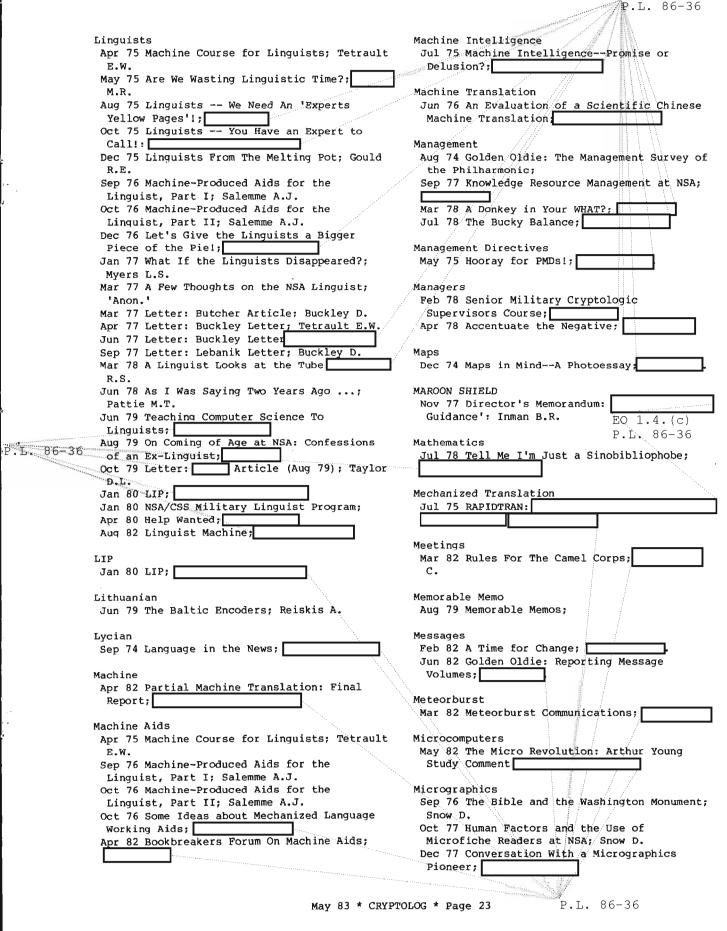
-



1.40(0,9001	P.L.	86-36
P.L. 86-36		
Mar 76 To Pull a 'Ponyal';	Jan 79 Golden Oldie: On First Opening	
Apr 76 Computer-Aided Transcription of	Kenney's 'Statistics'; Mountjoy M.	
	Jan 79 Henry Cement and other Phantoms of the	
Apr 76 How Do Adults Learn Language?;	Opera(tions);	•
and the second	Feb 79 Language Career Panel: Clarification	
Apr 76 Language in the News: Language Rule;	of Nov 78 Item;	
May 76 Hypnosis and Self-Hypnosis in Language	Mar 79 VORD is a Better Idea;	
Learning; Buckley D.	May 79 Run This Through Your Transcription	
May 76 What Language Problem?; Pattie M.T.	Machine;	
Jun 76 An Evaluation of a Scientific Chinese Machine Translation;	May 79 Where Do Good Transcribers Come From?;	
Jun 76 Notes on Translation from the Chinese;	Jun 79 Letter: 'Sixth Language';	
	P.A.	
Aug 76 Language in the News;	Jun 79 Sign Language; /	
Aug 76 Research in Speech Perception (Dr.	Jun 79 The Baltic Encoders;	
Ruth Day); Tetrault E.W.	Jul 79 Gears of the Mouth;	
Sep 76 Language in the News;	Jul 79 Letter: Article (Apr 79);	
Oct 76 Language Skill File;		
Mooney K.	Jul 79 Wilt Thou, Angelina?; Fairbanks S.	
Oct 76 Some Ideas about Mechanized Language Working Aids;	Aug 79 Language Proficiency Certificates for Military Personnel	
Nov 76 Golden Oldie: The Things They Say;	Oct 79 NCS Summer Language Program;	
Miller D.E.	Apr 80 LIME-A, OHIO; LEEM-A, Peru; Salemme	
Nov 76 The Uses of Elegant English;	A.J.	
J.R.	Apr 80 P16 Language and Cryptologic Library;	
Nov 76 Toujours La Politesse (Japanese); Buck		
S.H.	Jan 81 Why Do They Leave?;	
Dec 76 What's In a Name?;	Apr 81 Grading The Russian PQE;	
Jan 77 Letter Article; Kenny	Jan 82 Letter: Article; Chauvenet L.R.	
M.M. Apr 77 'It's Got to Get Out Today!'; Blank F.	Feb 82 Native Scripting of Languages;	
$Jul 77 \underbrace{EO 1}_{EO 1} Hick (C)$		
S H S H	Apr 82 Partial Machine Translation: Final	
Jul 77 Tool Languages; P.L. 86-36	Report; Pratt D.L.,	
Aug 77 Expletives Deleted?; Salemme A.J.	Nov 82 The Costs of Muddling Through; Gould	
Sep 77	<b>R.E.</b> EO 1.4. (c)	
D.L.	P.L. 86-36	
Sep 77 JPRS Language Reference Aids;	Language Identification Jan 80 LIP;	
Sep 77 The Seminar Program;		
W.L.	Leadership	
Nov 77 Backing into Language Acquisition;	Oct 82 Leadership: A Personal Philosophy;	
	P.	.L. 86-36
Nov 77 Language Processing Forum;		
	Lexicography	
Nov 77 Letter: Salemme Article;	Sep 74 Some Thoughts on Lexicography; Buck	
Nov 77 Letter: Salemme Article;	S.H. Feb 75 Glossaries versus Dictionaries: Which	
Dec 77 What Made Them Do It? (Language Self- Study);	Feb 75 Glossaries versus Dictionaries: Which Should It Be?; Gurin J.	
Jan 78 Thanks for the Attaboy!;	Jul 77 Buck	
Feb 78	S H	
	EU 1.4.(	
Feb 78 The Unseen Go-Between; Gurin J.	Library P.L. 86-	30
May 78 Uncle-a Sam Wantsa You!:	Feb 75 Replacement of the GUPPY Library;	
Jun 78 Celtic Languages Today;		
Jul 78 Is A Translator a Professional?;	Aug 76 NSA Cryptologic Collection;	
Sep 78 Letter: Pattie Article; Buckley D.	Jun 79 Letter: Library Changes; Jun 79 Letter: Library Changes;	
Sep 78 Soviet COMINT and the Civil War;	Apr 80 P16 Language and Cryptologic Library;	
	The second secon	
Sep 78 What's In a Non-Name?;		
Oct 78 And-a You Betta Have Moti-vaysh!;	Linguistics	
	Nov 78 Linguistics and the Code	
Dec 78 Agency Summer Language Study; Buckley	Reconstructor: Buck S.H.	
D,		
May 83 * CRYPTO	LOG * Page 22	
May 05 Chillon		

-SECRET-

#### SECRET



-GEORDT

#### OCID: 4009861 -SECRET P.L. 86-36 Oct 79 Snowballs On The Roof; Filby V.R. Oct 78 Back to Square One!; Oct 78 Reduction Ratios in Micrographics; Apr 80 What To Do About 'FANX'; Snow D. May 82 The NSA Information Desk: 'No Comment'; Military Oct 82 Not Secret Anymore; Jul 78 The Soviet General Staff; On-Line Aids Dec 82 Going On-Line With Information Aids; Minicomputers Gurin J. Jun 78 A Computer Scratch Pad at Home or at On-Line Data Work?; Jun 78 Minnie's Mini: Kenny M.M. Aug 77 DIALOG Available at NSA; EO 1.4.(c) Feb 79 Literature Search On-Line; Missiles P.L. 86-36 Nov 77 OPELINT Nov 81 OPELINT Is Alive and Well In B Group; P.L. 86-36 Molecule Superseries Feb 75 Golden Oldie: Establishment of. (c) Order of Battle Molecule Superseries; P.L. 86-36 Dec 77 Mar 78 Letter: Rosenbluh Article; MORETOWN K.E. Mar 78 Jul 78 Letter: Article: Organizations Dec 78 To Whom It May Concern; Grant L.G. Feb 79 Letter: Grant Article (Dec 78); Pattie MOSES Jun 79 The Story of MOSES; Gardner D.G. M.T. P.L. 86-3 Apr 81 Middle-Age Spread; MSI Dec 75 The Great Soviet Shipbuilding Mystery; Organize Work Nov 82 Human Factors Corner: How Do People Williams D.H. Organize Cooperative Work?; Multichannel Oct 78 Overheard Oct 78 Overheard in the Burnbag Line; Apr 82 Overheard While Standing in the Multivariate Techniques. Burnbag Line; Mar 77 D.A. EO 1.4.(c) Pattern Recognition P.L. 86-36 Dec 77 What Is Pattern Recognition?; Navv Feb 78 Soviet Navy Command Post System; D.A. PEP Apr 78 A Little PEP Talk; NCS Oct 74 News from NCS--Agency Resumes Hiring of LICs; NCS Offers Course in 'SIGINT PERCIVAL Nov 76 Check Your Morse Front-End Alignment; Appreciation'; Apr 75 Language in the News; Tetrault E.W. 'Anon.' Nov 75 NCS Offers Course-Equivalency Tests; Apr 76 NCS Offers Course-Equivalency Tests, Performance Clarification: Feb 82 The Internal Performance Evaluation: Oct 79 NCS Summer Language Program; Friend or Foe?; Jan 81 NCS-CLA Symposium; Performance Appraisals Negative Intelligence Jan 80 Between The Lines of Your Performance Appraisal; Oct 78 A Method for Measuring Negative Intelligence; Personalities Jul 77 Match Them Up!; Network Aug 75 Computer Network Resources In C5; Jan 79 Golden Oldie: On First Opening Kenney's 'Statistics'; Mountjoy M. Jan 79 Henry Cement and other Phantoms of the NSA May 76 A Soviet View of NSA; Opera(tions); Dec 78 A VIP Tour through the Attic of NSOC; Oct 79 The Roads Around Us; Chauvenet L.R.

May 83 \* CRYPTOLOG \* Page 24

P.L. 86-36

SECRET

Personality

GRONDT

₽.L. 86-36

Dec 82 Questions In Search of a PQE;

Sep 77 Tribute to the Guru; 'Class 32' Personal Computers Mar 82 A Personal Computer: A Current Cryptanalysis Support Tool; R. Apr 82 Personal Computer Application: Jun 82 Letter: Personal Computer/Article; Personnel Feb 78 First Lady of Navy Cryptology; R.P. Jan 79 How do You Tell These Two Clowns Apart?; Plaintext May 82 Letter: Plaintext; PLATFORM Mar 77 An Overview of Project Dec 81 PLATFORM: How Did You Say That Works?; PL1 Nov 78 Formatting PL/1 Source Code; K.J. PMD May 75 Hooray for PMDs!: PMT Apr 82 Partial Machine Translation: Final Report; Poems Jan 77 Executive Order 11652; 'Leiner' Jan 81 Some Things Never Change; Feb 82 A Wail, A Complaint, and a Melange; Snyder S.S. Polyhedrons May 77 The Polyhedral War; Aug 77 Letter: Article; 'Weeson' Portuguese Sep 74 Language in the News; Jan 78 Thanks for the Attaboy!; POE Jan 75 The Case for COMINT Readers; H.G. Dec 76 Why Can't They Design a Good SR Test?; Biorklund K. Apr 77 Some Thoughts on the Russian PQE; Jun 77 Letter: Clark Article; Feb 79 In Defense of The Indefensible: Notes on the Russian PQE; Tetrault E.W. Apr 81 Grading The Russian PQE; Jan 82 Letter: Article; Chauvenet L.R.

'Schmedlapp' Predictions Feb 76 The Prebendary and the Prophet; Dec 76 But It Looks Like the Real Thing; Mar 77 Letter: Interview; H.L. Production Apr 76 Golden Oldie: Hidden Losses in COMINT Production; Gould R.E. Professionalization Dec 74 The New Collection Criteria; Apr 75 Letter: Professionalization of Bookbreakers; Jun 75 Letter: Bookbreakers; Professionalization of Country Specialists; Jun 75 Professionalizing in Computer Systems; Apr 77 Some Thoughts on the Russian PQE; Oct 78 Continuing Professionalization; Apr 79 Fear of Testing, and What To Do About It; Proficiency Aug 79 Language Proficiency Certificates for Military Personnel; Promotions Nov 77 A Proposed Cure for the Time-in-Grade Syndrome; Mar 78 A Proposed Cure for the 'Performance Syndrome'; Dec 78 Some Tips on Getting Promoted; v.c. Feb 79 Letter: Article (Dec 78); Bostick C.W. Aug 79 ... But On The Other Hand; Aug 79 NSA Promotion Boards: How They Work; Jan 81 How to Improve Your Promotion Potential; Jun 82 Who Wants A Promotion, Anyway?; Aug 82 What Promotion Boards Want; Publications Jan 75 The SIGINT Users' Handbook or: What's an ISHTAR?; May 76 About the NSA SIGINT Summary; Hunt W. Sep 76 Foreign Publications Procurement Program; Mar 77 Revised Technical SIGINT Manual in Preparation; Filby V.R. May 78 Project UTENSIL: The DDO Data Dictionary/Directory; Dec 78 'No, No, Nanette!' Means Yes?; A.J.S. Jan 79 Human Factors Newsletter;

May 83 \* CRYPTOLOG \* Page 25

SECRET

Jul 79 Russian Handbook of Spoken Usage, Oct 78 Letter: NSA-Crostic; Filby V.R. Vol 3: Oct 78 NSA-Crostic No. 18; Williams D.H. Jan 80 System Acquisition Document Review; Oct 78 Puzzle: Who and Whom?; Nov 78 NSA-Crostic No. 19; Williams D.H. Dec 78 NSA-Crostic No. 20; Williams D.H. Mar 82 Old Phone Books Never Die; Nolte W.M. Jan 79 NSA-Crostic No. 21; Williams D.H. Feb 79 Know Your Geography; Punctuation Nov 74 The Apostrophe: Some Thought's; Feb 79 NSA-Crostic No. 22; D.H.W. Oct 76 The Winnah: Kid Apostrophe!; Mar 79 NSA-Crostic No. 23; Salemme A.J. Aug 79 Punctuation: More Than Meets The Eye; Apr 79 NSA-Crostic No. 24; D.H.W. May 79 NSA-Crostic No. 25; D.H.W. Jun 79 NSA-Crostic No. 26; D.H.W. PURPLE Jul 79 NSA-Crostic No. 27; D.H.W. Dec 82 Does Anybody Here Remember PURPLE?; Aug 79 NSA-Crostic No. 28; D.H.W. Oct 79 NSA-Crostic No. 29; D.H.W. Jan 80 NSA-Crostic No. 30; D.H.W. Apr 80 NSA-Crostic No. 31; D.H.W. Puzzle Aug 74 Puzzle: Stinky Pinky; Jan 81 NSA-Crostic No. 32; D.H.W. Apr 81 NSA-Crostic No. 33; D.H.W. Aug 74 Puzzle: Telephone Directory; Oct 74 An October Overlap; Oct 81 NSA-Crostic No. 35; D.H.W. Oct 74 Puzzle: Telephone Recall; Nov 81 Cryptic Crossword; Nov 74 Answer to An October Overla ; Dec 81 NSA-Crostic No. 36; D.H.W. Jan 82 NSA-Crostic No. 37; D.H.W. J.E. Feb 82 NSA-Crostic No. 38; D.H.W. Dec 74 Puzzle: Citizens of the World; Dec 74 Puzzle: Secret Messages, 'Military Mar 82 Cryptic Crossword; Mar 82 Letter: Strangest Bust of the Month; Cryptanalytics'; P.L. 86-36 Jan 75 Puzzle: Crossed Codewords; Dibben A. Feb 75 Letter: Citizens of World Puzzle; Apr 82 NSA-Crostic No. 39; D.H.W. G.P. May 82 Bust Answer; Feb 75 Puzzle: Can You Make Out the Name?; May 82 NSA-Crostic No. 40; D.H.W. Jun 82 NSA-Crostic No. 41; D.H.W. Apr 75 Answer to Can You Make Out the Name!; Aug 82 NSA-Crostic No. 42; D.H.W. Oct 82 NSA-Crostic No. 43; D.H.W. EO 1.4.(c) May 75 Puzzle: How Many Words in 'CRYPTOLOG'; Nov 82 NSA-Crostic No. 44; D.H.W. P.L. 86-36 Jun 75 Puzzle: Dec 82 NSA-Crostic No. 45; P.L. 86-36 Aug 75 Puzzle: CRY-PTO-LOGrolling; Qualifiers Nov 76 Clarity, Thy Name is Qualifier; Oct 75 NSA-Crostic No. 1; A.J.S. EO 1.4.(c) Jan 76 NSA-Crostic No. 2; A.J.S. Mollick J.J. Apr 76 NSA-Crostic No. 3; A.J.S. P.L. 86-36 Jun 76 NSA-Crostic No. 4; A.J.S. Radio Electronic Oct 76 NSA-Crostic No. 5; A.J.S. Jun 79 Nov 76 TEXTA 'Word Seek'; M.R. Jan 77 NSA-Crostic No. 6; A.J.S. Apr 77 NSA-Crostic No. 7; Chauvenet L.R. Radio Fingerprinting P.L. 86-36 Jul 77 NSA-Crostic No. 8; A.J.S. Apr 80 AIT; Jul 77 Puzzle: Match Them Up!: Sep 77 NSA-Crostic No. 9; Williams D.H. RAGPIE Nov 77 How Many African Countries Can You Jan 78 But Why Do We Do It?; Spot?; Nov 77 NSA-Crostic No. 10; A.J.S. RAPIDTRAN Jul 75 RAPIDTRAN: Jan 78 NSA-Crostic No. 11; Williams D.H. Feb 78 Puzzle: Three Holes; Mar 78 Answer to Three Holes: Mar 78 NSA-Crostic No. 12; A.J.S. Readiness Mar 78 Word Seek; Jul 79 Naval Readiness: A Basis for Apr 78 +Conoces Bien la Geografia?; Comparison; Apr 78 NSA-Crostic No. 13; Williams D.H. Apr 78 Prizewinners in Three Holes; Reference Aids May 78 NSA-Crostic No. 14; 'Sardonyx' Sep 77 JPRS Language Reference Aids; Jun 78 NSA-Crostic No. 15; A.J.S. Spiegelthal E.S. Jul 78 NSA-Crostic No. 16; Williams D.H. Sep 78 NSA-Crostic No. 17; A.J.S. Reflections Oct 78 Know Your Geography; Nov 74 Reflections on a Translator's Oct 78 Letter: NSA-Crostic; Conference; May 83 \* CRYPTOLOG \* Page 26 P.L. 86-36

-SECRET

R.L. 86-36

DOCID:	4009861 <sub>EO</sub>	0 1. <del>Asctat</del>
·	ЦU	L. 86-36 P.L. 86-36
	L •	$\mathbf{N}$
		$\Delta$ $\sim$
	Jan 79 Reflections and Recommendations; 1	
	V.R.	Apr 81 Grading The Russian PQE;
	Peminisaenaas	Jan 82 Letter: Delaney Article; Chauvenet
	Reminiscences Mar 77 A View of the Central Computer Cor	L.R.
	in the Late 1970s and Early 1980s; Phil.	
	C.J.	Nov 75
	Apr 81 The Poet's Corner;	
	Aug 82 I Remember;	W.L.
	Nov 82 An Old Timer Is One Who;	Jan 78 An Early NSA Proposal for Satellite Remoting; , Nolte W.M. P.L. 86-36
	Reporters	
	Aug 74 Calling All SRAs! SRA Symposium	
		Aug 79 Letter: Screening Radiation;
	Reporting	W.E. Aug 79 Letter: Letter (Aug 79);
	Reporting Aug 74 A Spot by Any Other Name; Filby V	
	Oct 74 Letter: Article:	
	Apr 7 <u>5 Oral Reporting: A New Challenge for</u>	or SCREENWRITER
	NSA;	Mar 78 A Linguist Looks at the Tube;
EO 1.4.(c)	Jun 75 Letter: Volenick Article;	
P.L. 86-36		Apr 78 Letter:Article; 'Fennwatcher'
	Jan 78 Letter: Article;	SDO
	Sep 78 A Matter of Style; Jan 79 Reflections and Recommendations; 1	SDO Filby Dec 81 Sleep Well: Your SDO Is On Duty;
	Jan 79 Reflections and Recommendations; 1 V.R.	Filby Dec. 81 Sleep Well: Your SDO Is On Duty; Sawyer E.L.
	V.K. Nov 81 Futuristic Reporting;	
		Secure Communications
	Resources	Jun 75 The Navajo Code Talkers;
	Sep 77 Knowledge Resource Management at 1	
		- Committee
	Apr 78 Accentuate the Negative;	Security
	Reutilization	Apr 77 The 'Ice Age' and International Security;
	Oct 79 Another Source;	Jul 77 Letter: Westwood Article;
		Jul 79 Source Protection: Our Agency's
	Russian	Insurance Policy;
	Sep 74 Language in the News;	Dec 81 Sleep Well: Your SDO Is On Duty;
30 1.4.(c)	Oct 74 The Exercise: A Case S	Study Sawyer E.L.
P.L. 86-36	in Special Research Analysis; Filby V.R.	
	Nov 74 Purity of the Russian Language	Self-Paced Instruction
	Slavophiles vs. Westernizers;	Aug 74 Self-Paced Instruction: The Future is
	Feb 75 Review of 'Guide to Russian Techn Translation' by Salemme;	
	Mar 76 To Pull a 'Ponyal';	P.L. 86-36
	Mar 76 TO Pull a Ponyal ; May 76 COMINT in the Russian Navy, WWII;	
		Apr 76 On Being Truthful; Gaddy D.W.
	Apr 77 Some Thoughts on the Russian PQE;	Oct 76 More Thoughts on 'Questionable'
		SIGINT;
	May 77 Why Are These People Smiling?;	Oct 76 Russian SIGINT and Electronic Warfare;
	Jun 77 Letter: Clark Article; Jun 77 Old Russian Manuscript Ciphers;	Jun 77 SIGINT Welcomes INKSTAND; Oct 77 Partners in the Exciting Future of
	oun // Oru Russian manuscript Cipners;	SIGINT: Rosenblum H.E.
0 1.4.(c)	Sep 77	Nov 78 Cast a Double Shadow: The Trojan Horse
.L. 86-36	D.L.	of SIGINT;
	Nov 77 Backing into Language Acquisition	
		Dec 81 Exercise Support;
	Dec 77 Letter: Article	Mar 82 A Historian Looks at SIGINT; Filby
	Jul 78 I Remember SPELLMAN; Salemme A.J.	v.R. //
	Feb 79 In Defense of The Indefensible: No	lotes
	on the Russian PQE; Tetrault E.W.	SIGINT 1990
	Jul 79 Gears of the Mouth;	Sep 82 SIGINT: 1990, Part One; Oct 82 SIGINT: 1990, Part Two:
	Jul 79 Russian Handbook of Spoken Usage,	Oct 82 SIGINT: 1990, Part Two; Nov 82 SIGINT: 1990, Part Three;
	Vol 3;	MON OS DIGINI: (330, LALC TUTGE!

May 83 \* CRYPTOLOG \* Page 27 P.L. 86-36

and the second

	EO 1.4.(c)
D: 4009861 EQ 1.4.(c) SEC P.L. 86-36	P.L. 86-36
F.H. 00 50	P.L. 86-36
SIGINT 80s	J.
Jan 81 SIGINT In The 80s: Two Views;	May 76 A Soviet View of NSA;
Lutwiniak W.	Oct 76 Russian SIGINT and Electronic Warfare;
SIGINT Alert	Oct 76 Work Quotas for Soviet Translators;
Dec 78	
P.L. 86-36	Nov 77
SIGINT Exploitation	Feb 78 Soviet Navy Command Post System; P.L. 86-36
Apr 78 SIGINT Exploitation, 1990; Jul 78 Letter: Article; Gurin J.	Jul 78 The Soviet General Staff;,
SIGINT Handbook Jan 75 The SIGINT Users' Handbook or: What's	Sep 78 EO 1.4.(c)
an ISHTAR?;	Sep 78 Soviet COMINT and the Civil War; P.L. 86-36
SIGINT Reporting	Apr 80
<u>Auq 76 Initiatives in SIGINT Reporting;</u>	EO 1.4.(c)
P.L. 86-36	Space Program P. L. 86-3 Jan 76 63 DaysThe Soviets in Space;
SIGINT Summary	Jan 76 63 DaysThe Soviets in Space;
Mar 77 More about the NSA SIGINT Summary;	Dec 76 Apollo-Soyuz Test Project;
Jun 77 More about More about the NSA SIGINT	J.E
Summary; Boucher M.J.	EO 1.4.(c) P.L. 86-36
Signals Processing	Spanish F.H. 80-30
Oct 74 The Mission of the Signals Processing	Aug 74 The Language of Beisbol in Everyday
Requirements Panel;	Talk; Santiago-Ortiz R.A. Sep 74 Language in the News;
Signs	Jan 75 The Case for COMINT Readers;
Jun 79 Sign Language;	H.G. Aug 77 Telling It Like It Is; Santiago-Ortiz
SIMP	R.A.
Jun 75 Golden Oldie: SIMP Tables;	Special Research
Software	Special Research Dec 76 Why Can't They Design a Good SR Test?;
Nov 75 DESKPAD: A Programmers's Tool;	Bjorklund K. EO 1.4. (c)
H. May 78 The Joys of UNIX; D'Imperio M.E.	Spelling P.L. 86-36
Nov 78 Formatting PL/1 Source Code:	Jun 77 Vich Iss R-r-right?; A.J.S.
K.J. Feb 82 Software - AAAS, 1982;	Dec 78 How Do You Spell Peking?;
SOLIS Dec 78 How Do You Spell Peking?;	May 82 Letter: Plaintext; P.L. 8
Dec 78	SPELLMAN EO 1.4.(c)
Jan 79 SOLIS: A Vehicle in Search of an	Jun 78 Never Again!; Gurin J. P.L. 86-36 Jul 78 I Remember SPELLMAN; Salemme A.J.
Engine;	Sep 78 Letter: Salemme Article; Williams D.H.
May 79 Chapenko, Shapenko: What Difference Does It Make?;	Oct 78 More B.S. (Before Spellman);
	Feb 79 P.S.; P.L. 86-
SOLITS Nov 75 In Praise of SOLITS; Grant L.G.	Jul 79 Shootout at the SIGINT Corral;
EO 1.4.(c)	
Soviet	Spread Spectrum
Aug 75 Processing Communications;	Jun 82 Amateur Spread Spectrum;
Nov 75	SRA P.L. 86-36
W.L. /	Aug 74 Calling All SRAs! SRA Symposium;
Dec 75 The Great Soviet Shipbuilding Mystery;	Oct 74 Letter: Sapp Article:
Williams D.H. Jan 76 63 Days-The Soviets in Space;	Oct 74 The Exercise: A Case Study in Special Research Analysis; Filby V.R.
	IN Special Research Analysis, LITAN A.W.
.4.(c) P.L. 86-36	EO 1.4.(c)
86-36 May 83 <sub>P* LCRY 878</sub>	<b>BOLGG * Page 28</b> P.L. 86-36

CECDER

		P.L. 86-36
5ap 77	Whither the CD82.	Malamatan
Sep //	Whither the SRA?;	Telemetry
SRI		Jun 76 Computers In The ELINT and Telemetry
	Flash! 115th SRI Located!; Salemme	Business;
A.J.	Fidshi (15th BAI Located), Satenine	
A.U.		P.L. 86-36
		Telephone P.L. 80-30
EO 1.4.(c) Feb 78		Apr 78 Telephone Problem Here;
P.L. 86-36		Mar 82 A Brief Treatise on Five Laws of
		Telephonic Communications; Nolte W.M.
Swahili		
Sep 74	Language in the News;	Telex
		Jan 75 UNNA,
SYMBIOS	IS	EO 1.4.(c)
Jun 75	Project SYMBIOSIS; 'Anon.'	Manning January
		Aug 74 A Spot by Any Other Name; Filby V.R.
System	-	Nov 74 Data and Definitions: Calling Things
	Human Factors and Systems Design: An	by Their Rightful Names;
Estrar	nged Relationship?;	Aug 79 An August Baudy;
Sustan	Development	Nov 81 Say What You Mean; Gaddy D.W. Jan 82 D <u>ata Field Naming</u> /Coding Conventions
	Towards Better System Development;	at NSA;
		TEXTA P.L. 86-36
T-Visior	1	Aug 74 TDB: The TEXTA Data Base; Jackson W.J.
Jan 79	T-Vision: The R <u>eference Ana</u> lyst's	Nov 76 TEXTA 'Word Seek';
Medium	of the Future;	Jul 78 Ye Gads! Another Country Trigraph
		System;
Tale		Oct 78 Letter:Article; Pattie M.T.
•	Golden Oldie: King Eusyb and Queen	Dec 81 TEXTA: What Is It? Where Is It Going?;
Deodi;	The Stairwell Society;	
	Letter: Stairwell Society Article;	
	Detter, dealtwell bottety Article,	Sep 77 The Seminar Program;
		W.L.
Target I	location	
Jun 78	Golden Oldie: Unidentified Unit at	Third Party
Unknow	m Location;	Apr 81 Third Party Relationships;
TDY	1) The 11/ store breath on Grant	
Jan 82 Shirts	All The Alligators Aren't On Sport	Jul 77 Buck
501108	5 F	EO 1.4.(c)
Teaching	Methodolgies	TIDE P.L. 86-36
	The Transcription Skill: Concepts and	Dec 81 TIDE: A Brief History;
	ng Methodologies;	
		Time Usage
	l Exercises	May 82 Human Factors Corner: Data Gathering,
Sep 77	'Simonoff Says!'; A.J.S.	How Do We Spend Our Day?;
<b>Masha</b> ina	1 Information	TIPS
	The Story of MOSES;	Sep 76 TIPS is Still Alive and Well;
6dit 73		
Technica	l Manual	
Nov 74	Guidesmanshipor How to Write	Traffic Analysis
Techni	cal Manuals Without Actually Giving	Aug 74 The New Traffic Analysis Glossary;
	.ng Away;	Sep 74 Gary's Colors; Garofalo C.A.
	Revised Technical SIGINT Manual in	Dec 74 An Approach to Callsign Analysis;
Prepar	ation; Filby V.R.	
	1. 0	Apr 75 A Comm Change at Ramasun Station;
	al Support	May 75 The Handmaiden of Che Magon P.O.
Oct 81 K.J.	Technical Support Catalogs	May 75 TA, Handmaiden of CA; Mason/F.O. Jun 75 More on Squaring the Page (A Crypto-TA
		Function) 7 Mason P.O.
		Aug 75 Abdul and His 40 Tanks; Mason F.O.
1	*	-
8		P.L. 86-36

May 83 \* CRYPTOLOG \* Page 29

SECRET

octof<sup>E0</sup>: 84009861

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

Aug 75 Processing	Apr 81 Traffic Analysis: Specialty Without Portfolio; Portfolio: Portfolio: P.L. 86-36
Oct 75 Automation of a TA Process; Murphy T.	
Nov 76 How to Make a Railroad Disappear;	Training
	Aug 74 Self-Paced Instruction: The Future is
Jan 77 Letter: Mason Article;	Now!;
Apr 77 Letter: Mason Article: Boucher M.J.	Nov 74 New Trends in the Teaching Of
Apr 77 Letter: Mason Article;	Cryptanalysis;
Apr 77 Letter: Mason Article; McGrillies J.R.	Apr 76 How Do Adults Learn Language?;
May 77 A Story With a Moral;	
Jun 77 Letter: Mason Article;	May 76 Hypnosis and Self-Hypnosis in Language
Oct 77 Which Numbering System Should We Use?;	Learning;
'Asken'	Nov 77 Backing into Language Acquisition;
Nov 77 A Little TA Problem;	
Dec 77	Dec 77 What Made Them Do It? (Language Self-
Feb 78 Collection-Support TA is Not for	Study);
Everyone;	Dec 78 Agency Summer Language Study:
Apr 78 Telephone Problem Here;	
May 78 TA Implications of FCC Proposal:	Jun 79 Teaching Computer Science To P.L. 86-36
May 78 IN IMPIICATIONS OF FCC FIODOSAT:	
	Linguists; EO 1.4.(c)
Sep 78	ool is noo canaci sangaage riogram,
	P.L. 86-36
Nov 78 A Small Problem;	Transcriber Analyst
Jan 79 Second Sighting; 'Donym'	May 79 Transcriber-Analyst Relations; Miller
Mar 79 Let's Not Lose Our TA Skills;	D.E. 86-36
G	
Apr 79 A Somewhat Larger Problem:	Transcription
W.E.	Mar 76 To Pull a 'Ponyal';
Jun 79 Letter: Article; Bjorklund K.	Apr 76 Computer-Aided Transcription of
Jun 79 Traffic Analysis of the Future;	
	May 77 Why Are These People Smiling?; EO 1.4.(c)
Jul 79 Letter: Bjorklund Letter (Jun 79);	P.L. 86-36
Broglie E.F.	Jul 77 Which Tape Has the Intelligence?
Jul 79 Letter: Bjorklund Letter (Jun 79);	Project Gurin J.
Buckley D.	Aug 77 Telling It Like It Is; Santiago-Ortiz
Aug 79 Letter: Buckley a (Jul 79);	R.A.
Aug / J Deccer: Buckley a (our /s);	
Two 00 mbass is a Maximum la Contine Ana May	Jul 78 I Remember SPELLMAN; Salemme A.J.
Jan 80 There's a New World Coming - Are You	Oct 78 You Can't Tell the Wheat from the
Ready?;	Chaff Without a Program; Gurin J.
Feb 82 Golden Oldie: Simplicity in Color;	May 79 Run This Through Your Transcription
Garofalo C.A.	Machine:
Mar 82 Letter: A Toy Problem; Tiren D.J.	May 79 Where Do Good Transcribers Come From?;
Apr 82 Golden Oldie: Tracks in the Sands of	
Time; Mason F.O.	Oct 79 The 2000-Year-Old Transcriber; P.L. 86-36
May 82 A History Lesson;	
May 82 True Base: Two Tales	
Jun 82 A Personal Footnote;	Translation
Jun 82 Golden Oldie: Reporting Message	Feb 75 Review of 'Guide t <u>o Russian Tech</u> nical
Volumes;	Translation' by Salemme;
Oct 82 Answer: An Old Problem;	Jul 75 RAPIDTRAN:
	EO 1.4.(c)
Traffic Analysts	Mar 76 A Comparison of NSA and ATA P.L. 86-36
Aug 76 Integrated Analysts for Asia;	Certification Standards;
W.D.	Jun 76 Notes on Translation from the Chinese;
	Sun ve Noces on Transfactor from the Chinese,
Jan 77 Letter: 'Firebrand' Letter on	Can 76 Companyin Voider, Denilt Chapt the
Article;	Sep 76 Semantic Voids: Don't Shoot the
Apr 77 Letter: Article;	Translator; Mason D.
Apr 77 Letter: Article;	Nov 76 How to Make a Railroad Disappear;
Jul 77 Letter: Article;	
Jul 77 Letter:Article;	Apr 77 'It's Got to Get Out Today!'; Blank F.
Oct 77 Golden Oldie: Analyzation of Data;	Nov 77 What Ever Does 'However' Mean?;
Curtin R.	
Mar 79 Attention Military Traffic Analysts;	Apr 78 ATA Letter to President Carter;
Apr 80 A Traffic Analyst Looks at Computers;	Tinsley R.L.
	May 78 Uncle-a Sam Wantsa You!;
May 83 * CRYPTO	LOG * Page 30
···- <b>·</b>	P.L. 86-36

SECRET

₽.L. 86-36 Jul 78 Has It Ever Been Translated Before?: Dec 75 Mum's Still the Word! ('The ULTRA Secret'); Nov 78 Letter: Dec 75 Weapon That Helped Defeat Nazis Article; (Winterbotham's 'The ULTRA Secret'); Filby Jul 79 Gears of the Mouth; Lasley D. Jul 79 Seminar on Translation Problems; P.W. Jan 81 Translator In Your Pocket; Feb 78 More Beans; Filby V.R. Aug 82 Linguist Machine; Oct 78 Feeding the Germans Misinformation (Book Review); Filby P.W. Translation Grading UNIX Mar 76 An Objective Approach to Scoring May 78 The Joys of UNIX; Translations; Aug 76 NSA's System for Grading Translations; Nov 81 How to Create A User-Unfriendly System: Dec 81 In Pursuit of: Faster Horses, Younger Women, Older Whiskey and More Money Translator Aug 74 Nice Busman's Holiday for One NSA D.L. Employee; Dudley B. Feb 82 Human Factors Corner: Some Advice to Nov 74 Reflections on a Translator's Users of Unfriendly System; Conference; Feb 82 Letter: UNIX Article; Oct 76 Work Quotas for Soviet Translators; Oct 82 Human Factors Corner: Text Editors; Oct 82 What's The Good (Pass)Word?: Nov 76 Golden Oldie: The Things They Say; Miller D.E. Jul 78 Is A Translator a Professional?; UNIX How To Mar 82 But Life Is Supposed To Be Hard; Jan 79 W.W.II Japanese Translation at J., Arlington Hall Station; May 82 Letter: Article Transliteration Sep 82 More Free Goodies: Jun 76 Transliteration or Cyrillic?; UNIX Shell G. Apr 82 Shell Game; May 79 Chapenko, Shapenko: What Difference Does It Make?; May 82 Letter: Shell Game Article; Jun 82 Letter: Shell Game Article J.W. Trigraph Jul 78 Ye Gads! Another Country Trigraph Jun 82 Letter: Shell Game Article: P.A. System; Jun 82 Loooong Shell; Aug 82 Shell Game; Trivia Jun 79 Letter: 'Sixth Language'; Nov 82 Letter: Shell Game Article; P.A. Dec 82 Shell Game: AJSQUE; Jul 79 Letter: Linguatrivia; Dec 82 Shell Game: Counter; W.E.S. Apr 80 Geographic Trivia; Dec 82 Shell Game: PWB WHEN; UNNA True Base Jan 75 UNNA, May 82 True Base: Two Tales; URST TSS Dec 81 The 1981 URSI XX General Assembly; Apr 82 Word Processing In A4; Sep 82 TSS Revolution; EO 1.4.(c) UTENSTI. Typewriter P.L. 86-36 May 78 Project UTENSIL: The DDO Data Aug 75 Typewriter Random -- A New Look; Dictionary/Directory; Oct 75 Letter: Typewriter Keyboard; Validitv T Organization Dec 75 What Are We About? (Fragments, Mar 78 Some Background on the C/T Merger; Figments, or What?); Feb 76 How Do We Know It's True?; Filby V.R. Smith F. Apr 76 Letter: Comments or Sep 78 T Establishes Human Resource Letter Development Panel; on What Are We About?; Apr 76 Letter: What Are We About? Article; ULTRA Apr 76 On Being Truthful; Gaddy D.W. Dec 75 A Personal Comment on Winterbotham's May 76 Some Principles of Cover and 'The ULTRA Secret'; Tiltman J.H. P.L. 86-36

May 83 \* CRYPTOLOG \* Page 31

GECRET

# CID: 4009861

Deception;

Mollick J.J.

Video Encryption

Videocasette

81;

Nov 76 Clarity, Thy Name is Qualifier;

Jan 82 Video Encryption: A Report From EASCON

Apr 81 DIA Videocasette Program;

P.L. 86-36

EQ 1.4.(c) P.L. 86-36 P.L. 86-36 Waveguide Analysis May 76 Waveguide Analysis; Weasel Words Oct. 74 Colden Oldie: An Unofficial Closser

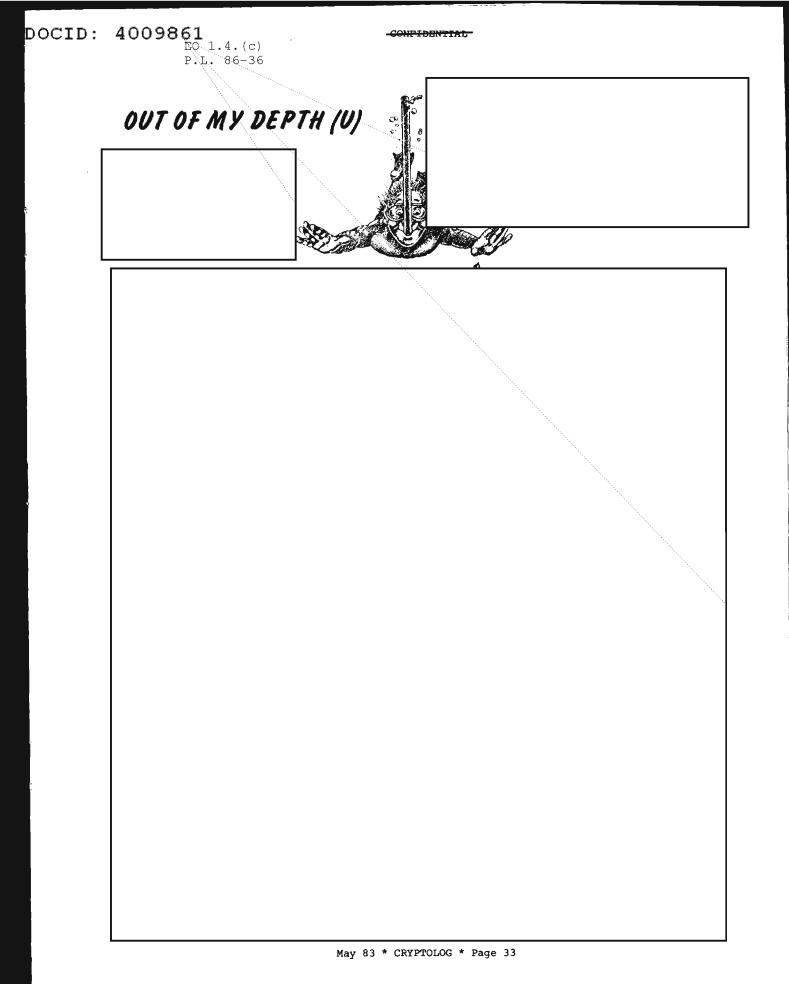
Oct 74 Golden Oldie: An Unofficial Glossary of Weasel Words;

Working Aids Jan 75 The Case for COMINT Readers;

Vietnam	H.G.	
Feb 75 The Gulf of Tonkin Incident;		
W.D.	Writing	
Jul 75 Re-psychling the Code Clerk;	Nov 74 Guidesmanshipor How to Wr	1+0
Aug 75 Twenty Years of Transposition;	Technical Manuals Without Actually	y GIVING
J.E.	Anything Away; Thal W.E.	
Oct 75 1972-1973: A Vietnam Odyssey $EO_1.4.(c)$	May 77 Plain English;	
Stepp L.C.,	Aug 77 Let Me RepeatAnd Make Mys	elf
Oct 75 Computers, Comms, and Low-Grade	Perfectly Clear: Jenks P.	
Ciphers:	Jan 78 The Joys and Frustrations o	f Plural-
Surger State	Dropping; A.J.S.	
Oct 75 NSA in Vietnam: Proud and Bitter	Dec 78 'No, No, Nanette!' Means Ye	s?; A.J.S.
Memories;	Mar 79 Fairbanks on English; Fairb	
Oct 75 One Chance in Three-But It Worked;	Apr 79 More Fairbanks on English;	
	S.	
Oct 75 The Danang Processing Center;	May 79 More Fairbanks On English;	Pairbanko
		nationen antification f \$4
	S.	P.L. 86-36
Oct 75 The Do Xa Pads; Wiley E.	May 79 More Than Words Can Say; Gu	
Oct 75	Jun 79 How Are Your Stamina?; Fair	
F. EO 1.4.(c)	Jan 82 The Literary Bends; Murphy	
Jan 76 Leo in October; Murphy A.I.	Feb 82 Native Scripting of Languag	
Mar 76 Letter: Proud and Bitter Memories		P.L. 86-36
Article;	Mar 82 Letter: The Literary Bends	Article;
Mar 76 Letter: Proud and Bitter Memories	Murphy A.I.	
Article:	and the second	
Apr 76 One Day in Danang;	N	
Jun 76 Letter: Cameron's Article; Murphy A.I.	Apr 78 Looking at Mr.	<u> </u>
Mar 79 Pursuit of the		,
E.L.	Nov 78 A Dialogue Between Ms. User	and Dr.
	Analysis	und br.
May 79 Project HELIPAD: An Epitaph;	Analysis	
M.L. EO 1.4.(c)		
PT 86-36		
VORD	EO 1.4.	
Mar 79 VORD is a Better Idea;	P.L. 86	5-36
Voynich Manuscript		
Aug 75 The Voynich Manuscript-Third Theory;	the second secon	
Miller D.E.	and the second s	
Apr 76 The Voynich Manuscript Revisited;	Contraction in the second s	
P.L. 86-36	From: fma at stept03	
WARC-79	Subject: SHELL	
May 78 Callsigns and WARC-79;	Reference: CRYPTOLOG, March 83, pag	ie 32
	Kererender entriched, naren os, pag	0.01
Warningo		
Warnings Dec 76 But It Looks Like the Real Thing;		
Dec 76 Buc IC LOOKS LIKE CHE Real Thing;		
Mar 77 Letter: Bunker Interview;		
R.L.		
Dec 82 Development and Correlation of		and the second
Indicators;		and the second
		a state of the second se
WARSAW Pact		and the second se
Jul 75 The Warsaw Pact	т441, 963-555	<b>35</b> 0 1.4.(c)
D		P.L. 86-36
	н. 00-00	
May 83 * CRYPTO	LOG * Page 32	
EO 1.4.(c)	-	

SECRET

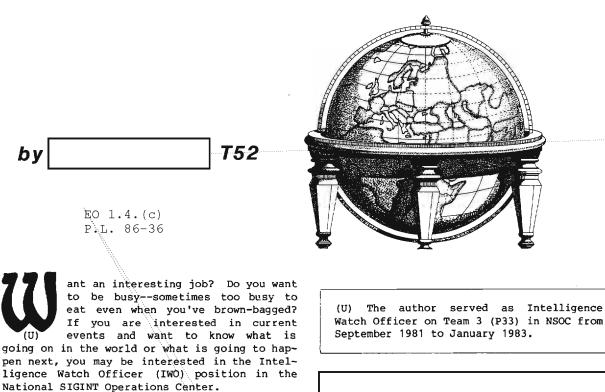
P.L. 86-36



by

(ບ)

# The Intelligence Watch Officer (U)

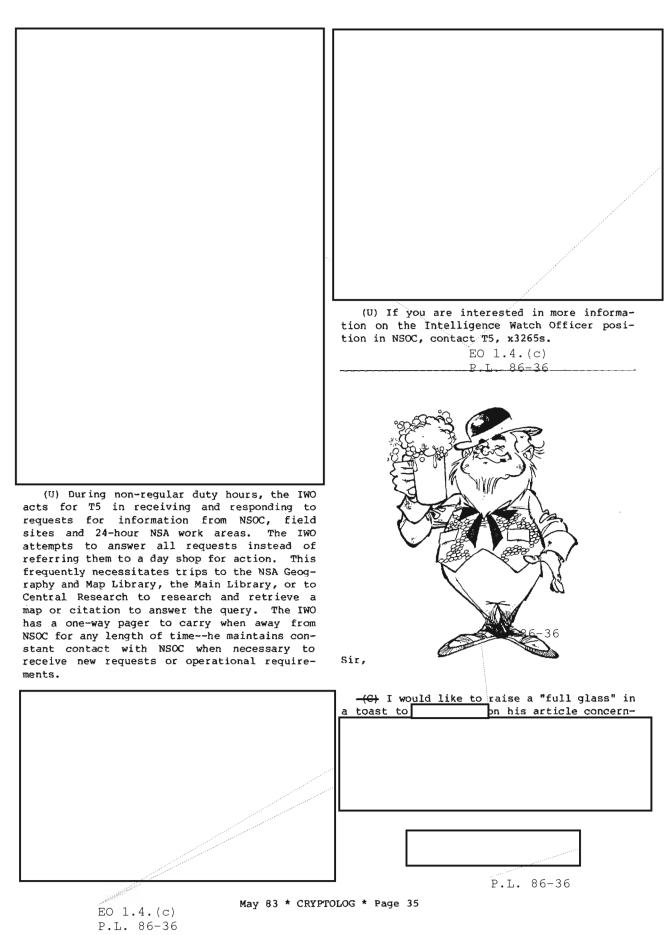


P.L. 86-3

May 83 \* CRYPTOLOG \* Page 34

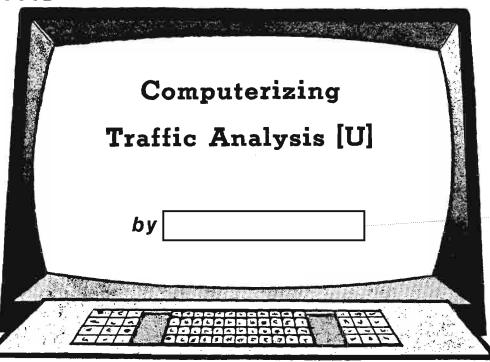
# DOCID: 4009861

-GECRET



SECRET

#### SECRET SPOKE



P.L. 86-3

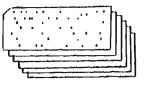
he traffic analyst finds himself turning to data systems because he often has mountains of data to examine, because the people who receive
 (U) TA results usually want their information very rapidly, and because almost all the data the traffic analyst wants to see is already inside a computer somewhere.

(U) Most traffic analysts who try to look at data systems develop a kind of schizophrenia. On the one hand, the TA data that comes in today has to be processed and analyzed today because there will be another batch of data coming in tomorrow. This means that the traffic analyst has to use today's data system to handle today's data. On the other hand, it does seem to us traffic analysts that data systems people would much rather talk about tomorrow's system--the one that isn't here yet, the one that won't have all these glitches and problems that today's system has.

(U) The traffic analyst who is in the trenches on a current operational problem would easily trade all the glowing promises of some brighter tomorrow for a quick fix on some of the glitches in today's system that will keep him from bleeding to death right now. That isn't my subject today--I really want to talk about the future. But as I thought about standing up here in front of all you data systems people, I couldn't resist putting in a plug for the working traffic analyst; he needs your help, both today and tomorrow. This paper was presented at the November 1982 Meeting of CISI.

THE PROLOGUE IS PAST

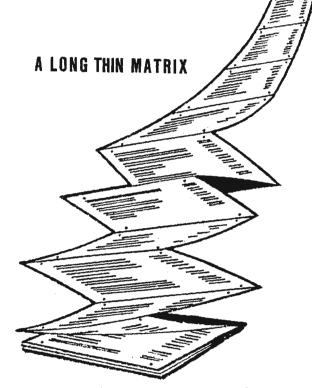
(U) I might be well to begin with a little history, or at least history as I remember it. My first recollection of what we now call data systems was a lot of 80-column cards and a card sorter. That was about 35 years ago. Watching those cards go through that sorter was rather hypnotic. The possibilities seemed limitless then--if we could only find a cheap and easy way to get the data onto the cards. I think the equipment was called Electronic Accounting Machines (EAM), and the people who supported the traffic analysts were called Methods Analysts (in the 1940s and early 50s).



(U) Since our data consisted of a matrix with 80 columns and many rows (one row for each card), our output consisted of that same matrix with its columns and rows transposed in some way. Later, we added the ability to look up words or strings in a dictionary and insert the result back into the matrix. SECRET SPOKE

(U) Many years and computer systems later, in the mid-1960s, this was still the primary data systems support to traffic analysts: a transposed matrix (now often wider than 80 columns) with a dictionary lookup. There were attempts to go beyond this. Most of the things we tried were made to fit one specific problem, and never developed into general TA We developed ponderous, monolithic tools. record formats whose structure provided a special place for each variety of data we thought we would find in the traffic. What I remember most vividly are long, soporific meetings where all we ever seemed to talk about was what format the data was going to be in. We spent untold amounts of energy and resources getting all of our data into these unyielding, user-murky systems, and there was often little energy and resources left over to develop any user-friendly output.

(U) The result of this, in many areas, was that the output received by the traffic analyst was not much more than his original raw traffic, transposed both horizontally and vertically, and with some information added through dictionary lookup processes.



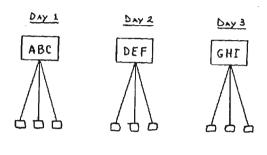
The form in which the output was delivered to the analyst was often decreed by someone remote from the analyst--someone who never had to actually live with the output--and it was rarely if ever changed to fit the current needs of the local problem or individual analyst. (U) It is still possible, even today, to see analysts sitting down with computer output and handlogging data from that computer output onto a form for their own personal use. In at least two areas, one might then see that same handwritten log being used a little later to punch cards for further computer processing!

# WHAT IS THE TRAFFIC ANALYST TRYING TO DO?

(U) The traffic analyst is trying to draw a picture of his communications target. He usually wants this picture to show how his target looks when it is operating normally. Once he knows what his target's normal behavior is, then he is in a position to detect variations, and report them to intelligence consumers.

# CONTINUITY

(U) Traffic analysts are usually looking for something they call continuity. When faced with a target that has daily-changing callsigns, the traffic analyst seeks to learn which of today's callsigns matches what callsign used yesterday.



# CONTINUITY

DATE: <u>1</u> <u>2</u> <u>3</u> <u>4</u> STN 1: ABC DEF GHI ... STN 2: ...

If I can say that the station that used callsign ABC on the first day is the same station that used callsign DEF on the second, then I can say that DEF (on the 2nd day) is continuity of ABC (on the 1st). On the third day, if I can say that GHI was used by that same station, then I can add GHI (on day 3) as another link in a growing chain of continuity. Many of our TA targets do change their callsigns, frequencies, addresses, and other features on a regular basis. They do it to

development.

make collection and identification more difficult, and it is the job of the traffic analyst to defeat these changes by the development of continuity.

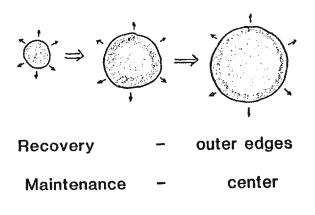
# TWO KINDS OF TRAFFIC ANALYSIS

(U) There are two forms of traffic analysis on most problems: development and maintenance. To borrow an example from cryptanalysis, the attack against a cipher system often goes through two phases:

- [] first, diagnosing and recovering of the general cipher system, and
- second, exploiting and processing the recovered system, which often involves solving daily keys or settings.

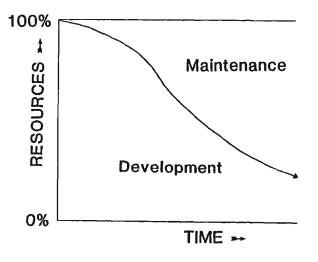
So too, in traffic analysis, one can consider that there is a <u>development</u> (or recovery) phase and a <u>maintenance</u> (or exploitation) phase, which may or may not include product reporting. However, in traffic analysis, the two phases often occur at the same time.

(U) In some ways, the traffic analysis process resembles a spreading oil blot. Out on the edges, new target territory is being conquered; new target communications structures are being discovered and cataloged; new methods of identifying and distinguishing various communications are being developed. But back in the central part of the oil blot, the territories previously conquered must be kept track of; the continuity of target communications structures previously recovered must be maintained.



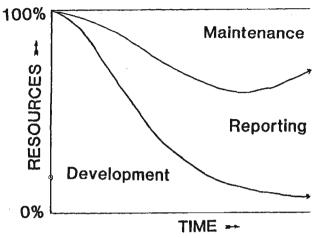
**OIL BLOT** 

(U) The more territory one conquers, the thinner the center of the oil blot becomes. The more communications structures one recovers, the more continuities there are that now must be kept track of. As the maintenance effort grows, it will use more of the available resources, draining them away from the recovery part of the effort, and at some point it will have absorbed enough of the resources so that a point of "no growth" is reached and, for all practical purposes, recovery of new structures stops. If expansion doesn't stop, the center of the oil blot will break; if development doesn't stop, the maintenance effort will fall behind and begin to lose track of continuities, which will then have to be discovered and developed all over again. This tension over resources between maintenance and development is similar to the one between software maintenance and software



(U) Sometimes the personality of the manager plays a part in just where this point of "no growth" takes place. Some managers are more at home in the settled, stable atmosphere of the center, where things don't change much from day to day. These managers tend to concentrate their attention on building a smooth-running system at the center, and may put a larger proportion of their resources into that area, so that the "no growth" point is reached more quickly. Other managers thrive in the rough and tumble frontier atmosphere out on the edges of the problem, where each day is likely to bring some new and different challenge. These managers tend to concentrate their attention on the recovery effort, sometimes at the expense of the more humdrum maintenance.

May 83 \* CRYPTOLOG \* Page 38



# REPORTING

(U) Some traffic analysis problems have a lot of potential for reporting--for providing the intelligence consumer with a blow by blow account of what the target is doing. Targets that involve ships and aircraft often have this potential because they move around from place to place, and the analysts often find much of their time taken up with reporting which ships and aircraft were active today, in what areas and performing what missions. Where this reporting potential is high, it tends to draw off resources from both development and maintenance. Managers whose problems have a strong reporting emphasis (especially, time-sensitive reporting) will generally try to pull resources from development rather than from maintenance, because losing the continuities means losing the raw material for the reporting effort. Losing the development effort is generally seen as the lesser of two evils.

(U) As an aside, I should say here that the reporting side of traffic analysis is generally well ahead of the technical side in the use of computers. Since my primary interest in this paper is the working-level traffic analyst, I will be concentrating on the technical side, and I do not propose to discuss the reporting aspects of TA except as they touch on the technical side.

## TRAFFIC ANALYSIS GOALS

(U) From the standpoint of the two kinds of traffic analysis--development and maintenance --we can express the general goals in the following ways:

# TA DEVELOPMENT GOALS

(U) We rarely collect or analyze all of the communications of any given target. We are almost always working on a sample of the target. At any given time, there is some residue of the target that we do not maintain continuity on, and bits and pieces of that residue find their way into our unidentified or search pile--the file of incoming traffic which looks as if it belongs to our target but doesn't exactly fit any of our known continuities. Development TA concentrates on that pile, trying to dig out new target nets and continuities. This unidentified pile is almost like "background noise"; it is always there, whether we talk about it or not. If we are still growing (if the oil blot is still expanding), then our development goal is to dig more of the target out of the unidentified pile. If we have reached the "no growth" point, then our development goal is to be able to recognize and develop any new communications that the target might put on the air-communications that ought to stand out against the "normal noise" in the unidentified pile.

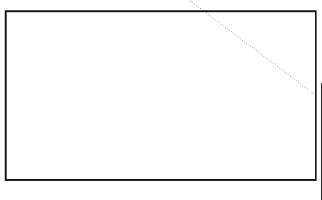
# TA MAINTENANCE GOALS

(U) During the maintenance phase, we want to be able to hang on to the continuity that we have already recovered. We want to do this:

- [] to support whatever analysis efforts are currently engaged on the target (such as cryptanalysis, language, reporting, etc.), and
- [] to support whatever collection effort is working against the target.

(U) To do the first support requirement properly, we need to be able to correctly distinguish and identify each of our continuities as the traffic arrives at the point of analysis, i.e., after it has been collected. OCID: 4009861

form to the other.



P.L. 86-36

# HOW CAN COMPUTER POWER BE APPLIED TO THE TA PROBLEM?

(3-CCO) In order to consider how the power of the modern computer might be applied to traffic analysis, we need to look at the model of TA that emerges from these two phases: development TA and maintenance TA. Although I have described them as if they were distinct and separate, they really ought to be thought of as a conjugate pair, because they tend to occur together on most problems. It is also possible for certain problems to be best described as a hybrid of these two forms: during the war in Vietnam, one out of every three pieces of intercepted traffic was unidentified, largely because of the rapidly-changing nature of the target. The point I want to leave with you today is that any attempt to provide the traffic analyst, either here in this building or anywhere in the world, with a Traffic Analysis Workbench System must reckon , with the fact that the problem he is working

will always be some mixture of these two forms of traffic analysis. We also need to consider that a TA problem can quickly change from one

(C) We decided to see if we couldn't find a way for computers to help us with the more stable maintenance problem. I remember spending several weeks laying out the logic and processes on the problem. And I remember being told, at the end of the project, that there wasn't nearly enough memory available to do what I needed.

DEVELOPMENT

# MAINTENANCE

#### Problem type: continuity-keeping continuity-seeking bookkeeping pattern searching "Anything changed?" "What's new?" slowly changing rapidly changing How dynamic? Foreknowledge: high low ~solved State of solution: ~unsolved Control: semi-automatic hands-on Interaction: human-efficient human-intensive Techniques: target specific human specific "mix-n-match" knowledge-based? "below the salt" start from scratch Worst case:

A COMPARISON OF TWO FORMS OF TA

May 83 \* CRYPTOLOG \* Page 40

SECRET SPOKE

# A COMPARISON OF TWO FORMS OF TA

(U) Let's look at these two forms of TA a little more closely. How do they compare when we look at them from the viewpoint of providing today's (and tomorrow's) traffic analyst with a computer support toolkit, while using a terminal workstation in an NSA worldwide networking environment?

(U) In development TA (the garrison communications in our example), we have a bookkeeping problem,

- where the emphasis is clearly on keeping track of a lot of known continuities;
- where we expect the changes in the target characteristics to be relatively modest;
- [] where the technical means of keeping up with the target (i.e., callsign and frequency systems, address tables, etc.) are largely solved or understood; and
- [] where we have good prospects of being able to project the appearance and behavior of the target from day to day.

(U) In development TA (the training communications in our example), we have a patternsearching problem,

- where the emphasis is on sifting through masses of low-yield ore, looking for something that forms a continuity;
- where the next success may look nothing like the last one; and
- [] where the chances of finding that needle in the haystack may depend as much on the personality of the searcher as on the content of the haystack.

If we can't <u>keep</u> continuities, (i.e., are not able to), then the target stays in the development phase, no matter how much we know about it. Someone once said that TA continuities take either 95% of our resources, or 5%. That number may not be right, but the idea is. Being able to keep track of the continuities is the key to whether the problem is development or maintenance in nature. A dailychanging callsign system <u>looks</u> to us as if it is rapidly changing if we haven't solved the system, but once the system is solved, we then perceive it to be slowly changing. It is a matter of viewpoint. (U) In maintenance TA, we work largely with what the target gives us. A package of techniques to grapple with a callsign system may work well enough on a problem where the callsigns are the key to our keeping track of continuity, but may be almost useless on another problem where the callsign system isn't solved and we must rely on other things, such as serial numbers or addresses.

(U) In development TA, on the other hand, a particular technique may pull one new structure out of the search pile and then never again find anything. The development analyst may need to continually devise new attacks and new methods; to him, the search pile is a featureless mass and it is his job to sort out the various pieces and find ways to distinguish one piece from another with some reliability.

(U) The maintenance TA problem probably needs a package that will

- [] look over the incoming material for the day;
- [] make reasonable guesses about continuities (including garbles);
- [] flash a warning light at the traffic analyst when things look very wrong or when it is confused by something; and
- [] provide a clean and readable summary of its results to the analyst for review.

It ought to keep up with both short-term and long-term trends, and should be especially attentive about "missing persons," portions of the target which haven't been seen for a while.

(U) The development TA problem, on the other hand, needs a toolkit that will provide the analyst with a range of diagnostic, computational, and pattern-searching techniques that can be brought to bear on the problem, in whatever mix the analyst needs at the moment.

# WORST CASE

(U) I have shown what might be called the "worst case" for each of these forms of traffic analysis.

(U) In maintenance TA, one sometimes finds that a problem must somehow be worked, but that it has no real resources and not enough clout to get any. Now, in the best of all worlds, where everything is done right and for the right reasons, such problems should not exist. If a problem is worth working on at

May 83 \* CRYPTOLOG \* Page 41

all, it is worth the resources needed to get the job done. However, in the real world, those problems that are "below the salt" will always be working with whatever support they can beg, borrow, or scrounge. Providing a general package for such problems would pay for itself a hundredfold in the first few years. At the minimum, package needs to be able to "ring an alarm bell" when the target starts to disappear, or becomes more active, or changes in some other way.

(S-CCO) In development TA, the worst case might be the situation where nothing is known. That is not as uncommon as some people might think.

When we pull together an analysis effort for a sudden war or brushfire, the analysts are usually drawn from other problems around the building; it would be nice if they didn't have to add "learning a new system" to all the other problems they will face on the new target. Therefore, the toolkit for such situations must be quite general and all-purpose.

#### TWO SYSTEMS OR ONE?

(U) What I have been describing so far may sound like two different systems, but what I am proposing is <u>one</u> system, with two parts. I have already said that these two phases or aspects of TA occur together, and I should add that on more than one problem, they are frequently done by the same people. New continuities are recovered by the development TA process, and then handed over to the maintenance TA effort to be kept track of. Information is often derived by the maintenance effort that will help the development effort. What the traffic analyst needs is one system that has enough flexibility for him to move whichever way his TA problem takes him. It would also be useful if the language we use is one that isn't going to change every few years because some equipment in the basement is being upgraded.

## PINSETTER

(U) Several years ago, we began to work on the concept of a Traffic Analysis Workbench System, with the covername PINSETTER. Some of what I have described here comes out of that experience. PINSETTER has been described elsewhere, so I will not spend time on it here. However, I will share with you some of my personal conclusions about PINSETTER, especially those which seem to be pertinent to the future. (U) There are aspects of traffic analysis which resemble word processing, and a good screen editor seems to go a long way toward putting the analyst in contact with his traffic, letting him rearrange it and touch up the rough edges and garbles the way he (the owner) wants them. It lets him look at the data <u>before</u> he decides what processing to apply to it. It also puts him in a good position to generate reports about his problem, especially the technical reports with technical data embedded in narrative text.

(U) A good toolkit, similar to UNIX and the PINSETTER extensions, is invaluable in providing the traffic analyst with the ability to tailor-make his own flexible processes for 1.4.(c)large scale manipulation of his traffic. P.L. 86-36

(U) Many of the practical results of PIN-SETTER, results that found their way into daily applications on specific targets, were not limited to traffic analysis. It became a regular occurrence to hear people from other cryptologic disciplines tell us that much of the UNIX/PINSETTER package for traffic analysts was what they needed, too.

# PROBLEMS THAT NEED SOLVING

(U) Among the many problems that need to be solved, I would like to mention two. Both of these are areas that are critical to the future TA Workbench System.

#### ARCHIVES

(U) Some of our continuities form chains that stretch back to the end of World War II. One of the things that Data Systems people don't like to hear is that we need storage for data whose lifetime must be measured in years, and perhaps decades. Some years ago, there came a time when all of our incoming data went solely into the computers in the basement. It was the culmination of the dreams of a number of people: to take the raw traffic away from the analyst! I don't challenge that decision. It is history. But I must say that on many TA problems around the agency, there are no good records on our known continuities from that date forward, unless there were analysts still keeping some sort of hand records. The philosophy on most computer hosts is that any records not accessed within some period (usually a year or less) are taken off the system.

(U) Even if the data is put onto tape, the medium will deteriorate. Once on tape, the data is "out of sight and out of mind." The software that understands that data will sooner or later disappear or be "improved." Nevertheless, the analysts on that problem are still responsible for that period of time, and may still have to field questions about their targets for that time period. So far, we have | Dear Editor: dodged this bullet, but sooner or later we | will have to face the need for long term archives.

# INFREQUENT USE OF PROCESSES

tion of software that is only infrequently | 2A be christened--at least informally--"The used. For example, suppose that one of our | Tower of Babel"! larger targets has a major communications ! change every five or six years. The effect of | this change is so great that it interrupts | intelligence reporting on that target until | [Editor's Note: In keeping with the tradition the new communications structures are under- | of naming the streets, auditoriums, etc., in stood and recovered. Each time the change | the NSA complex after outstanding individuals, occurs, an intensive effort is therefore | we could always claim that the building mounted to recover our continuities in the | had been named after the late, lamented Mabel shortest possible time.

(U) In the old days, when the special effort was over, everything was bundled up and packed away for retrieval when the next change came along. But how do we handle this now that we have modern data systems support? After five or six years, how much of the software is still useful? Chances are that | the data base has been changed, as well as the host on which it resides.

(U) Another example might be the diagnostic techniques to attack a particular kind of callsign system. Once the system in question is solved, how should we preserve the software so that it doesn't need to be reinvented the next time such a system is encountered? Suppose we don't find a similar system for five, or six, or even ten years?

# CONCLUSION

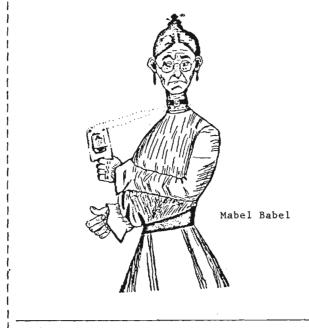
(U) I don't offer either my observations or my experiences as criticisms, but rather as areas of traffic analysis support which need to be solved. I have tried to avoid mentioning specific hardware or software, except as examples. A man named Bob Biles taught me long ago that users should never tell computer people what equipment to use.

(U) Perhaps traffic analysis has lagged behind other cryptologic disciplines in making full use of modern data systems. But that is changing, thanks to the patience, ingenuity, and hard work of many of you here today. I still keep a supply of pencils around, and I still have a pencil sharpener on my desk--but I have noticed that I don't really use them very much any more.

(U) In sympathy with countless NSAers who, through the years have been antagonized, baffled, challenged, demoralized, etc., by count-L lless forms of human and machine language (not I to mention the devil's own creation, govern-(U) The second problem involves the ques- | mentese), I propose that our new OPS Bulding

# JOHN J. MOLLICK, B41

Babel (19??-1979), one of the Agency's foremost linguists, who spoke fluent govern-I mentese as her native tongue. Her classic work, A Governmentese-English, English-1 Governmentese Dictionary (now out of print), is still the classic work in the field.]



# P.L. 86-36

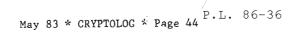
# SOLUTION TO NSA-CROSTIC No. 46

Memo from the Editor (of CRYPTO-[ LOG to CRYPTOLOG's Puzzle Editor]

"Our Jan-Feb issue will be devoted to the CISI Essay Contest. It would be useful to have a puzzle that has data systems as a base, if you I can find a suitable text. Also, I have been contemplating running an April Fool issue. | You might be thinking about that ... "

NSA-Crostic 47 by DH W

N.S. Norway (1889-1960) was an aeronautical engineer, active during the pioneer days of British aviation. He was also a prolific novelist. Many of his best works are set in the country which became his post-WWII home. Mr. Norway is Word V in this puzzle.



# DOCID: 4009861

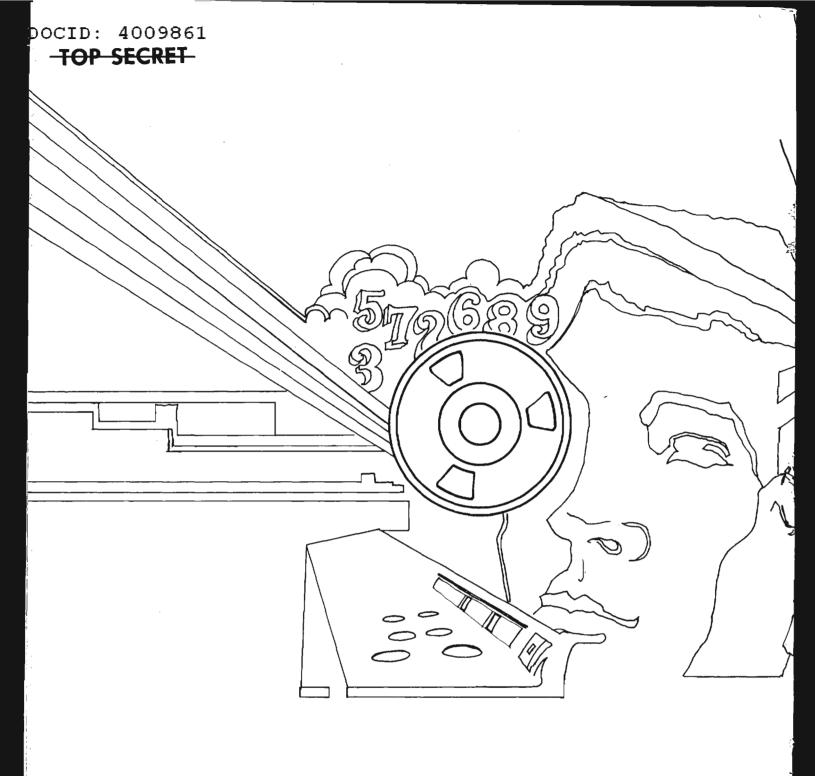
-2

a'

FOR OFFICIAL USE ONLY

May 83 \* CRYPTOLOG \* Page 4586-36

FOR OFFICIAL USE ONLY



THIS DOCUMENT CONTAINS CODEWORD MATERIAL

TOP SECRET