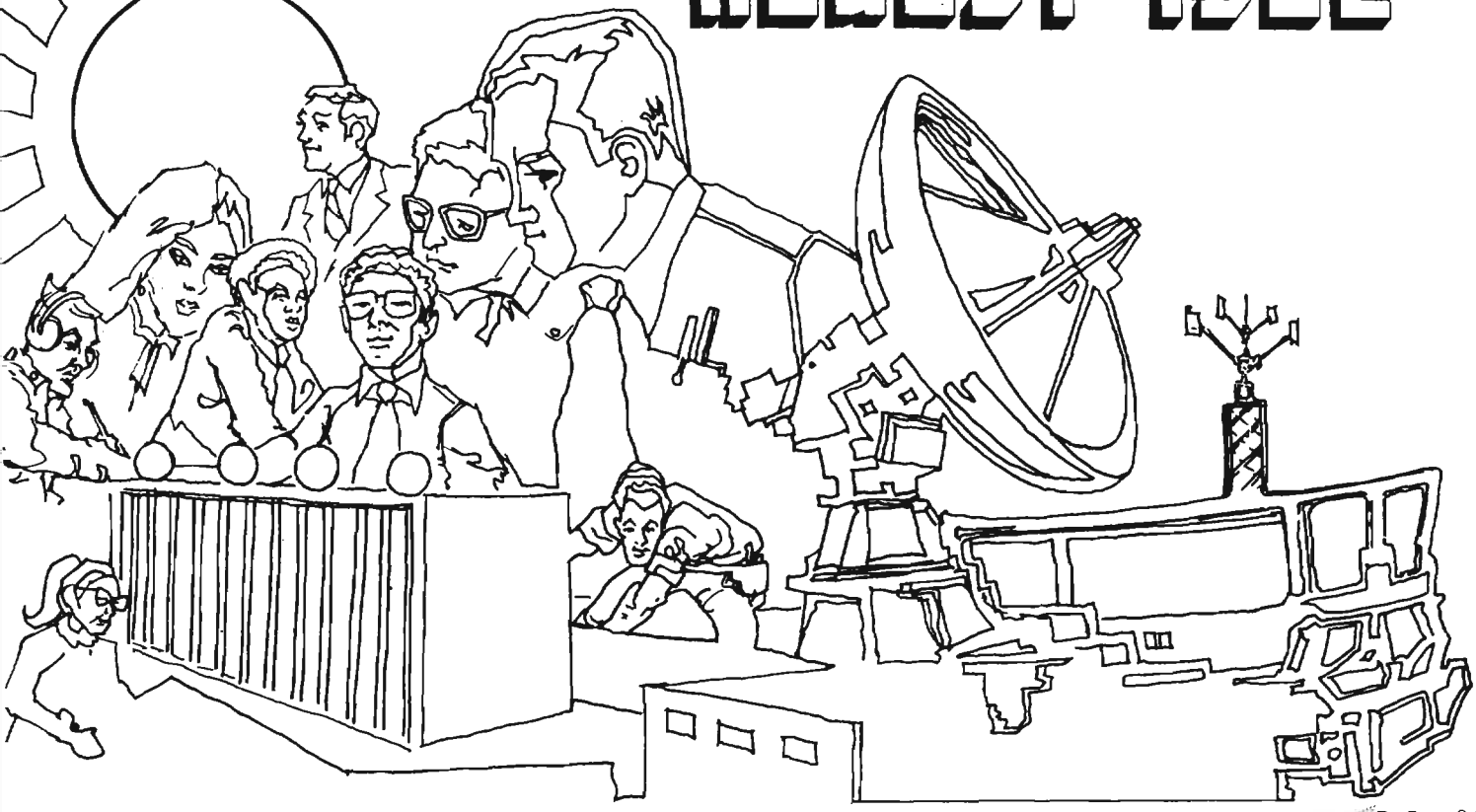
~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

AUGUST 1982



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~NOT Rreleasable TO CONTRACTORS~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~Declassify on: Originating Agency's Determination Required~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 8 AUGUST 1982

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlcØ5
(note: no 'O' in 'log')

Editorial

~~(FOUO)~~ Most people engaged in either managing or supporting analysts, and here I mean the analysts who produce the Agency's principal output, have the idea that they are helping the analysts in various ways. Theories about how to do this best are many and varied. Some people see the analytic process as a kind of production line, and therefore tend to think in terms of 'expediting' as a kind of helping. That is often the way I offer to 'help' my children do their homework.

~~(FOUO)~~ Some people, on the other hand, see the analytic process as an intellectual activity, rather like discovering the double helix, or deducing the presence of some new planet through the variations of the orbits of other planets. To them, the 'helping' tends to take the form of encouragement, or creating the proper environment so that this process of 'thinking' or 'discovering' can take place.

~~(FOUO)~~ When we come to consider how modern technology will 'help' these same analysts, what we come up with will depend, in part, on what sort of theories we hold about 'helping' them. If we hold to the expediting school, then our technological planning will naturally take that shape. If we are encouragers, our futurizing will be full of strokes and hugs.

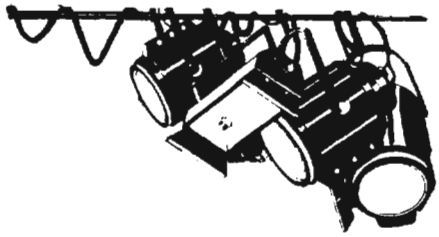
~~(FOUO)~~ I remember one job where my helping of my subordinates did not fit most of these patterns. When a particular kind of action message arrived, my instructions to everyone but the one taking action (and that included me) was to flatten themselves against the wall until the action was completed. It worked, as those of you who labored there know well. But I'm not sure that such a 'helping' philosophy will ever find itself into our technology.

P.L. 86-36

WED

~~FOR OFFICIAL USE ONLY~~

LOOKING AROUND with



P.L. 86-36

AFCEA 82 and ICC-82: NEW CRYPTO DEVICES(U)

(U) A number of new cryptographic devices were displayed at the AFCEA 82 Exhibition in June, 1982. The AFCEA show is known as the premier display of tactical communications equipment in the world, but in addition to the military cryptographic systems, some civil and police equipment was also on display. In general, there was almost no information about the actual encryption algorithms used, but key management, and nominal security factors were mentioned in brochures.

(U) MARCONI displayed their MINSTREL personal radio for police and military use. The military model uses a different encryption algorithm than the police model, and both algorithms have been tested by British cryptographic experts. The radio could be adapted to use a U.S. algorithm, according to MARCONI marketing representatives. The MINSTREL radio transmits a 16,000 bps stream of compressed voice in plain or cipher. Power output from the handheld unit is 0.5 W or 1.5 W. The radio weighs 500 grams. Dimensions are about 17 x 8 x 2 cm. For vehicle use, the handheld radio can be plugged unto a receptacle in the vehicle which switches it to vehicle power and antenna, then unplugged and taken out of the vehicle to protect the crypto unit. A special feature of the MINSTREL radio is the key control. The keys are not set up by thumbwheels, but are loaded by an optical device, so that the user never sees the key, and cannot change it. The key is about 160 bits, viz., 10^{38} different keys. Ten different radio channels are available, all on the same key. Because of the problem of terrorism and capture of the radios, channel 11 can be selected to clear the crypto variable so the radio is taken out of the secure net. The Fill Management Unit will generate random keys to load the radios directly, or to load them through a portable "fill gun" which uses an optical link. The radio and modulation system is compatible with the military CLANSMAN radios. Frequency coverage is 68-88 MHz, 146-156 MHz, and 420-470 Mhz. U.S. police and emergency frequency allocations are 150-173, 406-420, 450-500, with Federal as well as non-Federal allocations. There are also Federal allocations between 68-88 MHz. Therefore, the MINSTREL radio might be useful as a cipher radio for certain police and Federal applications in which there is no desire to expose U.S. cryptographic algorithms to loss or capture.

(U) MARCONI also displayed the MARACRYPT Mark II Key Management System, which improves the original MARACRYPT unit from 10^{10} bits to 2^{50} bits. The new MARACRYPT II units dispense with thumbwheel settings, and load keys from an optical fill gun, which stores and loads a 128 bit fill word. There is a facility for "stretching" a 10 character code of the type used in MARACRYPT Mk I to a 32 character fill word to provide interoperability between Mk I and Mk II updated equipments. The key is transferred as a 384 bit word, consisting of the 128 bit key variable in direct and inverted form, followed by 128 bits of control information.

(U) Both MINSTREL and MARACRYPT illustrate the new notion of keeping the key distribution under tight central control so that radios cannot be rekeyed in the field, unless a fill gun is available. MINSTREL will operate in the clear at 16 kbps, so that cross net traffic is possible in the clear mode. Flexibility as a base station, vehicle and handheld radio (with three different battery packs for the handheld model) make it useful for non military applications.

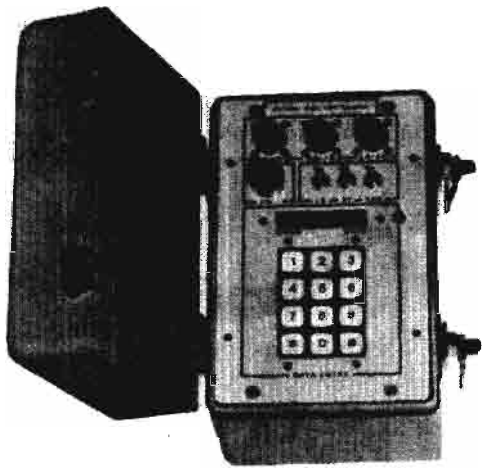
(U) PLESSEY displayed some similar radios, viz., the PTR 1851D VHF pouch radio which used the "Smalltalk" 16 Kbps speech encipherment. The PTR 2451 VHF vehicle radio operated at 50 watts. PTR 349 VHF squad radio transmits at 1 W and 3 W power levels. In addition, a PTR 3411 Groundsat terminal was displayed. The DMT (Digital Message Terminal) stores and receives or transmits messages at different rates, and has a 3500 character storage. On a radio channel, the DMT sends speech or stored data at 16,000 bps; over a telephone or 3 KHz ssb channel, the DMT can send at 100 or 600 bauds. The keyboards and output display present English or Arabic characters.

~~(NC)~~ PLESSEY is also developing a new line of equipment in a bid for a major Australian military communication project called RAVEN. The Australians have not modernized their military radios in some time, and wish to go directly to modern digital systems. For this, PLESSEY has developed new "brassboard" circuits to demonstrate the combined frequency hopping plus in-band spread spectrum technology to meet the RAVEN specifications. The equipment will hop at a 100 to 500 Hz rate, and will transmit data or voice. It will interface with the DMT, hence probably has a 16,000 bps data rate, using some spread spectrum coding.

(U) THOMPSON CSF displayed the TRC 773 tactical digital ciphony equipment for VHF and UHF operation. The speech is coded as adaptive delta modulation at 16,000 bps. The user is allowed more than 2.3×10^{18} different combinations, of which 65,536 are used for a fixed internal key. The radio is supported by a CRY 103 key processing and control unit, and a key injector CRY 104 unit. The TRC 773 will operate in the clear or cipher mode. There are protection devices to ensure perfect and secure operation, and a pushbutton erases the memory contacts in an emergency. Possible enciphered relay can be done by the CRY 105 device. The TRC 773 can be connected directly to the TRC 550 family, and connects to the TR.PP13 family by a broadband connector. The TRC 773 weighs 1.6 Kg as a handheld unit, and can be attached to a TRC 751 VHF/FM vehicle mounted transmitter.

(U) ROCKWELL presented the COLLINS VP-110 voice encryption unit for airborne application. This analog scrambler uses a proprietary algorithm to control the time and frequency scrambling. The encryption unit will accept 10^{19} key variables, which can be inserted at the unit through a 16 key input. They claim the algorithm is cryptographically secure, and that voice quality is excellent. There is an in-band digital controller for FSK synchronization to synchronize the crypto units during operation. Once a key or set of keys is set up, the device is locked with a metal key and the crypto keys cannot be changed. A special feature of the VP-110 is that it has a "public key" algorithm which can be exercised by pushing a button. Any two VP-110 units can exchange a key generated by a PK algorithm, so that every two party conversation can be secure from all other authority. This will make it possible for any two VP-110 users to exchange secret voice traffic even if they are on opposite sides in a war. This should present some interesting administrative problems in controlling the flow of secret traffic, and the arrangements that can be made in secret between consenting parties.

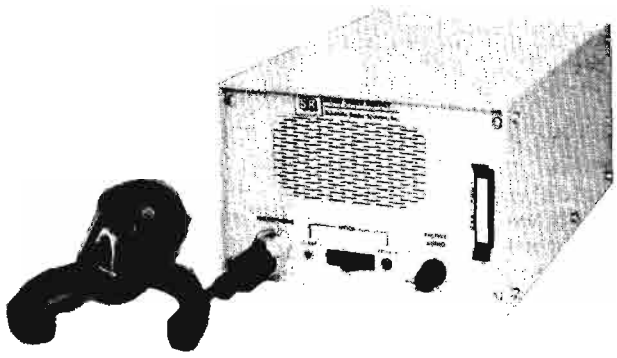
(U) ROCKWELL also presented the DDC-575 Digital Data Cipher, and the DDL-104 Digital Data Loader. The DDC-575 is used for encipherment of full duplex data channels at 576 Kbps. Other models in the DDC series operate from 128 Kbps to 2.048 Mbps (the CCITT standard). The key generator is a COLLINS high security proprietary nonlinear device with more than 10^{70} possible codes. Random start of the code generators (approximately one billion selections) is used to prevent attack in depth, according to the brochure. 80 octal characters can be used to input a key. Key generator and data path have check circuits to prevent faulty output. The DDL-104 is used to load keys in any of the DDC series. A TTL logic interface is used to connect the loader to the cipher device.



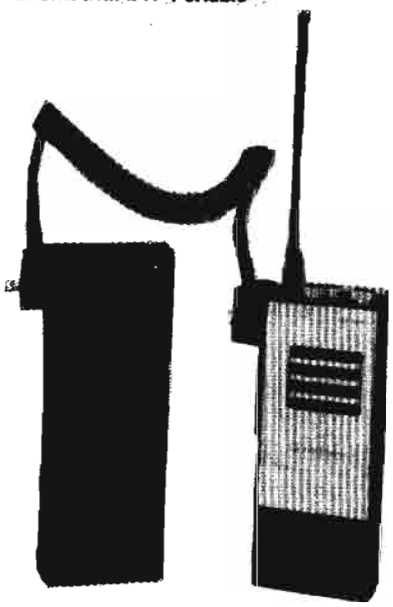
DDL-104 Digital Data Loader in Carrying Case

DDC-575 Digital Data Cipher, Single Configuration With Blank Panel

(U) SCIENTIFIC RADIO displayed their SR-800, a simple voice privacy device, which is not new. 3840 code combinations (in analog encryption) are available, and, at a lower price, a 128 code option is available.

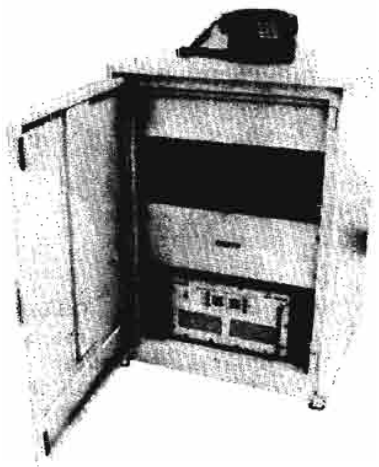


DES Key Variable Loader shown with DVP Portable



(U) MOTOROLA displayed several "DES Options" for DVP Digital Voice Protection Systems. The DES options W-338, H-338 and C-338 can be obtained with new radios or attached to existing MOTOROLA radios. Synchronization is achieved by a self synchronizing preamble. There is an internally derived pseudo random initializing vector, and a Key Variable Loader is used to set keys into the DES/DVP radios. To convert existing DVP radios to DES radios, the user only needs to exchange the DVP for the DES module. This implies that various crypto algorithms could be used for the DVP radios, in the same way that the MARCONI MINSTREL radio has several algorithms. Hence, the radios could be sold or exported with one algorithm, which is later replaced with a better one, without visible changes in the digital radio traffic. This may be a portent for the future.

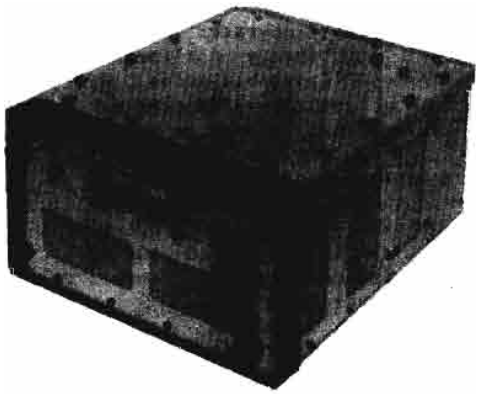
(U) GTE displayed their MRD-2000G TEMPEST Voice Digitizer, which uses the LPC-10/43 voice digitizer algorithm. The MRD-2000G is designed to interface to four wire or two wire telephone circuits, and with PABX and CENTREX trunks. It will transmit data at 2400, 7200 and 9600 bps in full duplex or half duplex mode. It uses a GTE fast synch algorithm. In addition to LPC-10/43, optional proprietary voice digitizer algorithms are available, viz: GTE LPC-10, APC-4, APC-4HSN, SBC.



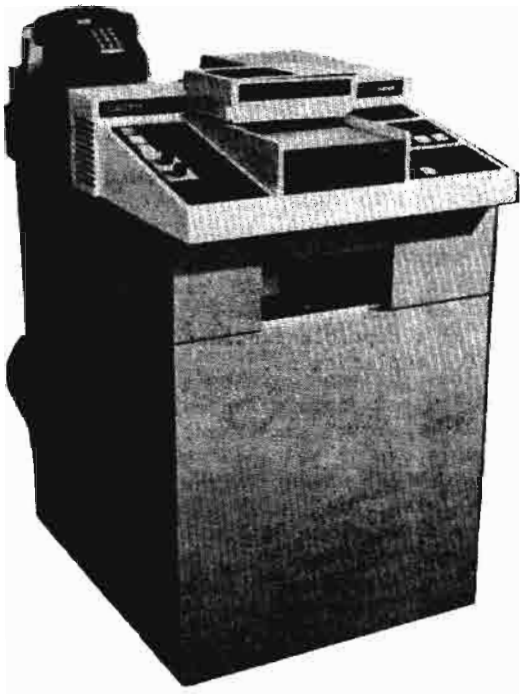
MODEL DVT-2000G TERMINAL

(U) GTE also displayed their model DVT-2000G telephone terminal with user furnished crypto specifications. This is designed for Government secure voice applications, and is used in conjunction with the MRD-2000G. A 7 inch space is provided for rack mounting of a customer furnished crypto unit, with a MIL-188C interface and 115 VAC power. The unit will operate over both two wire dialup unconditioned lines, and four wire tie lines with E&M signalling. The synchronization, using MRD-2000, takes 45 msec and uses 16 bit PN sequences. An optional push to talk feature can be incorporated.

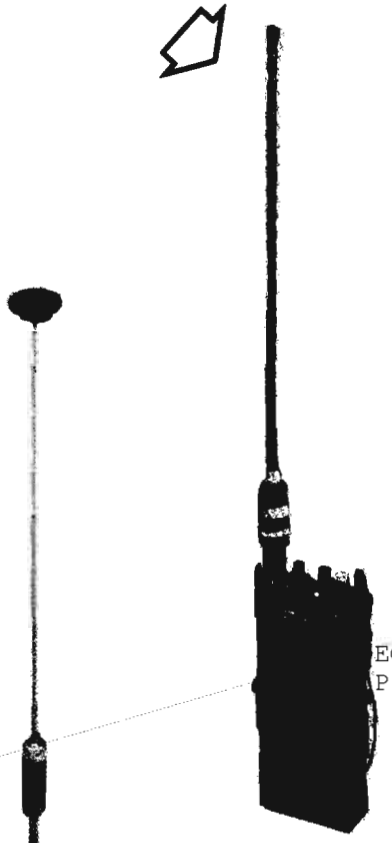
~~(C)~~ This illustrates the migration, i.e., technology transfer, into the marketplace of high grade speech processing and digital transmission developed for government and military needs.



MRD-2000G TEMPEST Voice Digitizer



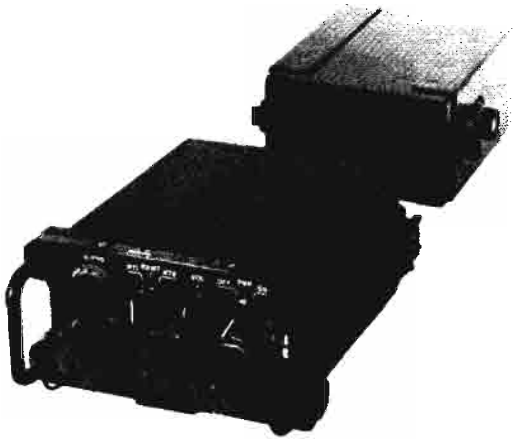
(U) MAGNAVOX displayed their Long Range AN/PRC-68 VHF radio, which can be fitted with a SVM-68 Secure Voice Module, the PCG-68 Programmable Code Generator for SVM-68, and the CSD-68 Code Storage Device for SVM-68. The new PRC-68 uses a different antenna to get a 5 Km range.



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

(U) MAGNAVOX has developed a M122 demolition control device with a fixed code to prevent erroneous detonation. At the factory, a unique (one out of a million) code is fixed in the sensors. A transmitter up to 8 kilometers away can send the code to the demolition units. Some military detonations take a long time to set up, and must be executed without tampering or misfires. The possibility of terrorist actions that set off civil detonators prematurely, which can cause unbalanced demolitions, can be countered by secure remote controls systems. Additional security for the sensor codes can be provided by a unit that can interface with the KYK-13, which also permits a number of sensors to be set off at once by the same code.

M122 DEMOLITION CONTROL DEVICE



(U) MAGNAVOX developed the MX-9331A/URC regenerative repeater for tactical secure voice. It will regenerate 16,000 bps or 18.75 kbps data. The MX-9331 allows the operator at the relay point to break in and listen to plain or cipher. It can be used with both VHF and UHF radios, and does the necessary operations to acquire, synchronize, and hold synchronization through fades.

(U) HONEYWELL advertised and displayed their SCOMP secure communications processor, bolstering their product evaluation with a letter on NSA stationary which labels the SCOMP "an acceptable candidate" for security-sensitive applications.

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755

DOD COMPUTER SECURITY CENTER

PRODUCT EVALUATION BULL

AS OF: 1 December 1981

PRODUCT: Secure Communication

MANUFACTURER: HONEYWELL Infc

DESCRIPTION:

The SCOMP hardware
Level 6 minicomputer w
Protection Module (SP
tation, paging, prot
Level 68 Multics,
translation for I

A basic se
tion on which
In addition,
and trusted
oriented c
its secu
hierarc
while
oper

STATUS:

The development of the SCOMP hardware, w
by the Naval Electronics System Command (NAVEL
recently been completed. It is currently oper
only a few laboratory and evaluation environmer
has recently transitioned responsibility for th
their Avionics Division (St. Petersburg, FL) to
Systems Operation (McLean, VA), and it will be ma
by the standard Level 6 facility in Billerica, MA

The security kernel software was developed as
the DARPA-initiated (NAVELEX sponsored) Kernelized
Operating System (KSOS) program and was designed to
a UNIX-compatible emulator. The emulator has been r
by the SKIP which is presently still under developmn
Therefore, software development for the SCOMP is not
self-hosted, but can be done on a standard Level 6.
tionally, the SCOMP is available in a NACSEM 5100 TEMP
version (AN/UYK-37(V)).

SECURITY EVALUATION STATUS:

Evaluation has not yet been completed. The DoD Comp
Security Center considers the SCOMP, with its security ke
a candidate for the class of products for which formal met
are employed to confirm the trustworthiness of the design.
An independent evaluation will be produced by the DoD Compu
Security Center.

ENVIRONMENTAL STRENGTHS:

The advantages of the HONEYWELL SCOMP derive from the
hardware support provided for security-related processing
requirements, and from enhancements designed with the goal
of maintaining performance for secure processing. The SCOMP
was originally targetted for general purpose, multi-level
secure, time-sharing applications. While the underlying
system was designed to support such an environment, the
currently available applications support software (SKIP and
trusted software) provide a secure base upon which one may
overlay specific applications. Although the evaluation has
not been completed, it currently appears that the SCOMP
will provide a state-of-the-art base for a variety of
security-sensitive applications. It should be considered
an acceptable candidate for a wide range of minicomputer
applications which require an enhanced architecture to
support secure processing requirements (e.g., communica-
tions processor, GUARD applications, data base systems,
etc.).

*The
an Evaluate
government de
products in a ma
Establishment.
to provide the statu
tion.

(U) TELETYPE displayed a MODEL 40/8C TEMPEST series teleprinter, which had the special feature of cassette input/output, in lieu of punched tape. One version of this teletype will accept a cipher device for on line secure transmission (Mod. 4033-8RYSB).

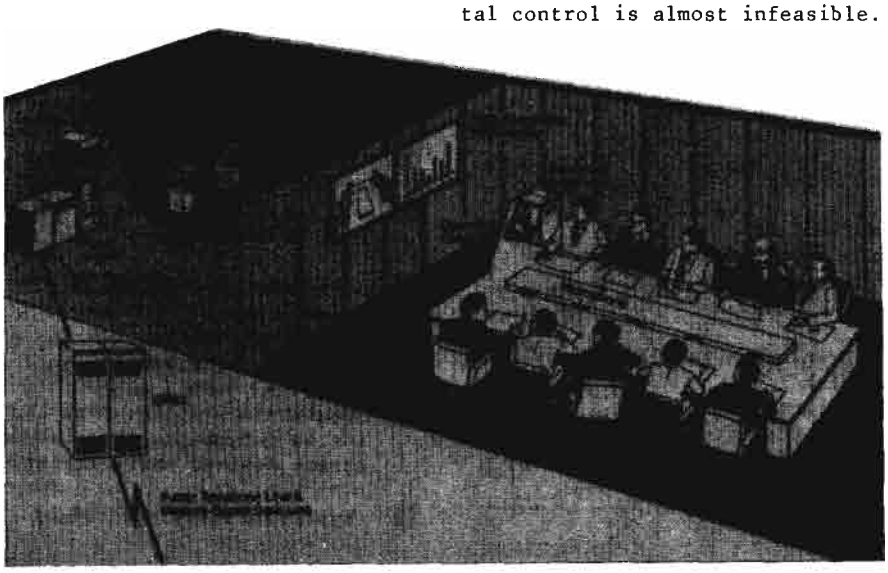
~~(C)~~ The point of particular interest is the cassette input/output. One of the cardinal needs in U.S. COMSEC is a convenient and cheap way of enciphering and deciphering offline traffic, so that sensitive traffic may be passed through the existing message centers without being read by the teletype operators. Small handheld computers can easily provide the encryption and message handling, and they will read and write audio cassettes. All that is needed is an interface device that will allow a handheld computer to use a cassette tape in the same format that the MOD 40/8C teletype accepts. This would permit cheap, reliable and unclassified encryption offline, with cassettes used as the medium for passing the traffic through the message centers. Since a major target country uses offline encryption for internal security employing punched tape, the U.S. could emulate this using audio cassettes.

Cryptology at ICC-82

(U) The Japanese intend to produce DES encryption chips for communications security. At the International Conference on Communications - 1982 (ICC-82), NEC displayed the NETEC-X1 TV Codec, for teleconference TV use, which does digital TV compression down to 1.544 Mbps, or 6.3 Mbps, and will use DES for encryption of both audio and video. At the 1.5 Mbps rate the image reproduction is fairly good, but there is a delay of about one second in response time. DES encryption will be used on four different codecs, viz: NPC-110A, NPC-111A, NPC-114A, and NPC-115A. The NETEC modems use only 1/40 to 1/6 of normal PCM TV signals, so that trunks or satellites can carry more conference links. NEC TVS (Telephone Video System) will also use encryption to send pictures over telephone lines. TVS-754 will send black and white, while TVS-751 will send color pictures or video frames. Both will use encryption.

(U) Although DES chips are difficult to manufacture, the Japanese have been very successful in copying U.S. technology. IBM still holds worldwide rights to the DES design, but it is unlikely that they would block NEC in implementing a publicly disclosed algorithm. Once the Japanese are able to produce the DES chips, U.S. export controls will no longer be effective. The proposed international data encryption standard is DES, and if it is adopted, the Japanese will be able to supply that market.

~~(C)~~ Summing up, the cryptology transfer inside the U.S., and across its borders, is creating low cost availability of tested and secure algorithms and key management schemes derived from U.S. cryptographic research. The use of Public Key algorithms to key airborne tactical voice links is a manifestation of this rapid spread. Serious problems arise in SIGINT, EW, Security and Counterintelligence. PK (public key) devices are an ideal way for a spy to transfer cryptographic data to a foreign buyer, without ever needing direct contact between the parties. While the academic community is concerned with publishing theoretical papers, the industrial community is interested in sales. The problem of control is that once the technology becomes cheap enough, or a market develops, governmental control is almost infeasible.



What Promotion Boards Want(U)

by [redacted] T1

P.L. 86-36

(U) Have you ever wondered what information in a promotion précis influences promotion board members? Have you tried to figure out what turns them on or off? If so, you are not alone. A group of T1 people approached this one head on. We asked some past and present promotion board members, "What do you look for in a promotion précis? What sells you on a person? What turns you off?"

(U) We share with you their pets and peeves. Perhaps you can add your own to the list.

PETS

- ☐ Describing job payoff relating to the characteristic described
- ☐ Giving numbers (quantitative things)
  - ★ People
  - ★ Dollars/Budget/Inventory
- ☐ Stating savings obtained
  - ★ People
  - ★ Dollars
  - ★ Space
  - ★ Material
- ☐ Listing unique contributions
- ☐ Logical order of events and accomplishments
- ☐ Bullets/One liners
- ☐ Off-duty activities
  - ★ Community involvement
  - ★ Leadership positions
  - ★ Unique abilities
- ☐ Using short sentences in plain, simple, readable English
  - ★ Impact sentences
  - ★ Quality vs. Quantity
  - ★ Specific application to individual recommended
  - ★ Active voice

PEEVES

- ☐ Using outdated information
- ☐ Repeating same information in all (or too many) categories, using same words
- ☐ Copying information verbatim from Personnel Summary
- ☐ Too wordy
  - ◆ "Snowed" with quantity, not quality
  - ◆ Not enough of the right kind of information
- ☐ Not expanding abbreviations
- ☐ Not explaining coverterms
- ☐ Using canned phrases
  - ◆ "Motherhood" statements
  - ◆ Government buzz words and phrases
  - ◆ "Jargonese"
- ☐ Using generalities without specifics
- ☐ Promoting the job instead of the person
- ☐ No specifics supplied about awards
- ☐ Lack of historical performance data since last promotion; no productivity specifics
- ☐ Nonconformity to format
- ☐ Errors and Inconsistencies
- ☐ No training courses or education since last promotion
- ☐ Paragraph structure
  - ◆ All begin the same
  - ◆ Passive voice
  - ◆ Long, poor sentences
- ☐ Mentioning outside work that has no bearing on duty performance or does not demonstrate desired characteristics
- ☐ Hyperbole

SHELL GAME (U)

WES

(U) You may not have realized it, but some of the commands on the UNIX system are really shells. As an example of a short UNIX shell, look a the UNIX command 'lsm' (whose full pathname is normally /usr/bin/lsm). Short but sweet! Another shell, this one rather long, is the UNIX command 'man' that is used to look up manual pages on your terminal screen (i.e., when somebody has misplaced your hardcopy manual).

(U) One shell file I have come to use regularly is called 'when' and tells me the last time someone has logged in. One of the first things I do when logging in is to ask 'who' is on the system. If someone I want to talk to is not logged in, my next question is whether they are around or away on leave or tdy.

(U) The shell looks like this:

```
:   Find out the last time a user logged in
:         wes 9/2/82
:
:                       Test for missing arg1
if "$1"x = x goto noarg
:
grep "^$1" /etc/passwd > tmp$$
ed - tmp$$
g/^.......*:./.*):$/s//ls -l 1/.llog/
w
q
sh tmp$$ | reform +m14 +t41 | rpl " 0 " "  "
rm tmp$$
exit
:                       Error message for no arg
: noarg
echo "User name not given"
echo "Usage: when username"
exit
```

(U) In its original form, the shell first checked the output of line of the 'who' output; if not, it went to look at the username's last login time. I found that too slow, and noticed that I tended to use 'who' first anyway, using 'when' only if the user was absent from the 'who' output. The 'reform' and 'rpl' were designed to format the output to match the 'who' format. If you like fast answers, you might just use 'sh tmp$$' without 'reform' or 'rpl' and leave out the test for a missing argument.

P.L. 86-36

(U) The following shell was written by [redacted] A205, and uses 'gath' in an interesting way to interactively collect data. The purpose of this shell is to send a file from one UNIX host to another.

(U) If all this looks strange, you will want to spend some time with the manual pages for 'gath' and 'send'. Enter your own terminal designator into lines 7 and 10 (where I have used ttyX). If you use more than one terminal, there are several ways of fixing the shell to accommodate this, perhaps by giving your current terminal as the first argument of the shell, or by executing 'who am i' and piping the result through reform to generate the wanted command line 'stty -echo > /dev/ttyX' in a temp file that would then be executed, etc.

(U) It really depends on what you like to do, and how slow you are willing to make the shell. I find that shells I use every day can be lean and clean, because daily use makes me remember what every option is. On the other hand, when I have a shell that is used only several times a month, it pays off for me to put in more bells and whistles, even at the expense of slowing it down. It isn't always easy to remember whether there are arguments needed and in what order, so I often test for that first, and use an error message that gives the correct format. That way, I can just give the command, and know that the error message will tell me how to use it properly.

(U) If you are interested in how slow or fast a shell runs (and you should be), get familiar with 'time' and use it on several versions of the same shell to find out which features cost the most in time and system.

```
gath >tmp$$
~-s
~:                Enter name of target computer
~=:?sys?
~:           Enter login name on target host
~=:?login?
~!stty -echo > /dev/ttyX
~:        Enter password for target login
~=:?passwd?
~!stty echo > /dev/ttyX
~:
~:
~:Enter the target file name,
~:    the name of the file on the target host
~=:?target-host-file?
~:
~:Enter the source file name,
~:         the name of the file on this system
~=:?source-host-file?
~:
~:If you are sending a file to target host
~:           enter an 's' otherwise enter an 'r'
~=:?direction?
if ?direction?x = sx goto SENDING
if ?direction?x = rx goto RECEIVING
: ERROR
echo Error: you did not enter an 'r' or 's'
echo            for direction of file transfer.
exit
: SENDING
cftp blocked suicide
*host ?sys?
log ?login?,?passwd?
rec fc '?target-host-file?'
*host *
sen fi '?source-host-file?'
*dou type i,s
*tra
*end
exit
: RECEIVING
cftp blocked suicide
*host ?sys?
log ?login?,?passwd?
sen fi '?target-host-file?'
*host *
rec fc '?source-host-file?'
*dou type i,s
*tra
*end
~:
~:No further input is required, wait for prompt
~.
sh tmp$$
rm -f tmp$$
exit
```

LINGUIST MACHINE (U)

P.L. 86-36

by [redacted]

G9

From time to time, one hears rumors of people who use the expression: "Run that by your linguist machine!" evoking a picture of a mindless army ~~(FOUO)~~ of translators mechanically plying their craft with a minimum of mental effort. If true, these rumors suggest that misconceptions exist about language work. This essay is intended to give those who are not linguists some idea of the things that a linguist encounters in his daily work. Although it is based on the experiences of a Japanese linguist and his perceptions of language translation, it is hoped that these observations may be of help in understanding the daily life of the translator of other languages as well.

~~(FOUO)~~ Sometimes linguists are told:

"Don't spend too much time on it; just translate it as it is--and get it out!"

Such guidance--while rightfully warning translators against including anything not in the original text--might suggest that translation is merely a matter of using a few dictionaries, remembering a few grammatical rules, and becoming accustomed to a foreign script or Chinese characters. However, language translation is not that cut and dried. Linguists face certain problems.

CULTURE AFFECTS LANGUAGE

~~(FOUO)~~ Differences between the cultures and decision-making processes of the U.S. and foreign countries can create a problem for translators. For example, if a Japanese official tells a U.S. official: "Goteian wo kentoochuu" (We are considering your proposal), the U.S. official may infer from that statement that a conclusion is likely to be forthcoming soon and that it could well be favorable. Actually, the decision could go either way and, whatever decision is ultimately reached, considerable time is likely to elapse. The delay in reaching important decisions in Japan stems from the decision-making process in Japan, which is based upon reaching a consensus among all parties involved, a process that can consume much time. Moreover, when a Japanese says "hai" (yes) to a proposal, he may mean only "yes, I will consider your proposal," since he hates to turn one down flatly. Or he may merely mean "I understand what you have said."

~~(FOUO)~~ Translators are forced to translate words and phrases that either have no equivalent in English or that have different meanings in English and other languages. For example, a Japanese writer will often begin with a deprecatory phrase like "kyooshuku desu ga..." that one might translate by such formulae as "By your leave, I would like to tell you the following," or "This might not be the place to mention this, but..." That kind of statement, which seems unnecessary to the English reader, appears to have an important social function in Japan, a relatively small nation that has traditionally found it necessary to preserve social harmony through convention.

~~(FOUO)~~ Perhaps it is because of this need to preserve social harmony that Japanese always appear to be apologizing. Japanese will often say "sumimasen" (I am sorry) when we would say, in an equivalent situation, "excuse me." Moreover, humility has traditionally been viewed as a quality of those possessing true learning and wisdom. A Japanese saying is "Minoru hodo atama ga sagaru inaho kana" ("The riper an ear of grain, the lower it bows its head"). Japanese, among others, do not like to make statements that will isolate themselves, a tendency made stronger by the group-orientation of Japanese society.

~~(FOUO)~~ One might cite many other examples of cultural differences that can make direct translation difficult--if not impossible. Translating the Japanese term "tatemae" is difficult for that reason. Americans and Europeans are taught to "practice what you preach," but in Japanese culture, there is apparently more open admission that, given human frailty, one's ideals or principles are not always practical or realizable. The Japanese have the word "tatemae" to express that idea, whereas we must do so indirectly by saying, "If I had my druthers, I'd..." or "That's the ideal, but..."

~~(FOUO)~~ Japanese appear to leave more to the imagination of their audience when speaking or writing, and often end sentences with statements that make their thought tentative, as in "I would like to go, but..." or "it could be perceived that way, but...." After the word "but" ("ga" in Japanese), the reader is left to fill in the sentence, as in "...but I might be wrong," or "but what do you think?" By being vague and tentative, the speaker in

Japanese society protects himself if he is wrong, does not suggest by his words that his listener or reader is ignorant--thereby embarrassing him--and, above all, demonstrates that he is not being "namaiki," i.e., that he is not running counter to the natural rules of social behavior within groups, or between superior and subordinate, by being excessively individualistic, selfish, or assertive. These ideas are difficult to render in direct translation.

~~(FOUO)~~ Differences in cultural outlook pose problems for translators in many languages. In Arabic, phrases like "In sha 'Allah" (literally meaning "God willing," but actually used to express the idea "I hope that ....") are used constantly. U.S. policy-makers tend to view the world through the eyes of American culture. What is difficult to express to U.S. policy-makers in translations is that unlike U.S. culture, which tends to reserve religion to one day a week, i.e., to the Sabbath, in Arab culture, religion (Islam: literally "submission") permeates everyday life which constantly reminds one in the Moslem world of the mutability of life and the limits of what any one person can hope to accomplish. In Arabic culture, the emphasis appears to be on "man proposes and God disposes" rather than on "God helps those who help themselves" as it seems to be in the U.S. Again, when translating Arabic, it is difficult to convey that dissent is often couched in religious terms. The same problem exists for the Russian translator. How can they make U.S. policy-makers aware that they should not dismiss statements of communist ideology as mere propaganda for public consumption?

~~(FOUO)~~ In Brazilian Portugese, there is the phrase "Nos le damos um jeitinho" (literally "We'll make a little allowance for you"). It is difficult to convey, in direct translation, the possibility that Brazilians do not necessarily share the American belief that "If I make an exception for you, I must make one for everyone." For that matter, how does one explain to foreigners our belief that "problems are opportunities in disguise" or that one should undertake "challenges," like going to the stars, merely because doing so is difficult, and that one "actualizes" oneself in the process?

~~(FOUO)~~ Unless translators have grown up in a foreign culture, or have access to native speakers or to persons with near-native fluency to explain things, translators may often miss part or all of the meaning of what they are translating. A Japanese hotel employee may say "Hai, wakarimashita" (Yes, I understood) to a request from a guest who wants to have his laundry done. What he means is that he will see to it that the laundry gets done. Similarly, two parties to an agreement may say that the agreement was "ryooshoo shimashita" (acknowledged), meaning that both sides went along with the agreement. Such terms apparently enable the speaker in Japanese society to save face and preserve dignity. Also, when a person in Japanese society offers someone something, he expects to have his offer politely refused before it is accepted.

~~(FOUO)~~ A classic case of different perceptions in different cultures concerns traffic signals: the Japanese refer to the dark green signal, and some foliage, as "aoi" ("blue"). That is because the Japanese divide the spectrum at a different point than do Europeans, so "aoi" has been incorrectly rendered as "blue" rather than "green."

~~(FOUO)~~ Japanese poetry, like the poetry of other countries, is particularly culture-sensitive. In her famous haiku poem, the Japanese authoress Kawa no Chiyo paints a picture with only 17 syllables:

「朝顔に
釣瓶取られて
貰い水」

"ASAGAO NI

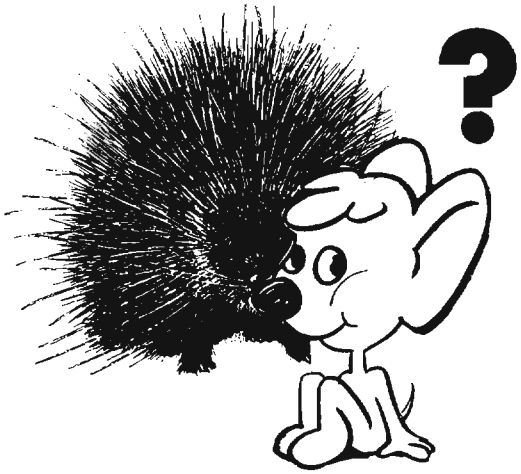
TSURUBE TORAETE

MORAEMIZU "

This poem may be translated as:

"When (I) found that the well bucket had been claimed by morning glories, (I could not bear to use it to draw water, so I was forced to) borrow water."

This poem, like the language in general, shows the Japanese predilection toward allowing one's imagination to fill in the unexpressed, as well as the great love of Japanese for beauty.



AND IF THAT'S NOT ENOUGH...

~~(FOUO)~~ Linguists might be told "Just do a 'quick and dirty' on it--get it out 'on the street' ASAP!" and be compelled by the nature of the material they are translating to rush out a translation. The problem is that they become caught between the need to speed the completion of the translation and the need to turn out a translation that is accurate and clearly understandable. The history of translation is replete with instances of mistranslations, the their consequences, arising from too hasty translation. A classic example of this took place at the start of World War II, when a translator rendered the Japanese decision to "mokusatsu suru" the U.S. peace proposal as to "dismiss it with contempt" instead of to "hold off on taking action." More recently, during his visit to the U.S. in May, 1981, Prime Minister Suzuki said that Japan's defense policy will be "harinezumishiki." A Japanese interpreter, apparently doing a "quick and dirty" translation, rendered the term as meaning "like a barbed mouse." What Suzuki's interpreter meant to say was that "Japan's defense policy will resemble a bristling porcupine." The confusion apparently arose from the Japanese word "nezumi" (rat), which is common to the Japanese words for mouse (hatsukanezumi) and porcupine (harinezumi). The net result of the mistranslation was to temporarily give perplexed and exasperated U.S. policy-makers the mistaken impression that Japan intended to renege on its security commitments. That is because "mouse" connotes timidity in American culture. The matter was cleared up shortly thereafter, when Prime Minister Suzuki spoke of a U.S.-Japanese "alliance." (Indeed, controversy within Japan over the meaning of the word "alliance" led to a change of foreign ministers.)

~~(FOUO)~~ In addition to being accurate, a translation or report must be easy to understand, and must contain no "double entendre," i.e., it must not be worded in such a way that two or more interpretations of a sentence are possible. Not long ago, the manager of a government translation "shop" that farms out material to be translated to contractors gave a talk on government language work. He said that as a result of the poor pay and resulting low standards for contract translators, the translations that they produced were so unreadable that some customers of their work became convinced that "foreigners cannot express themselves properly." The point is that if a translation is not crystal clear, it is not likely to be respected by the reader. It is particularly difficult to turn out easily readable translations from Japanese, a

language whose structure is very different from English. A Japanese sentence is often more equivalent to an English paragraph in length and completeness of thought. It can go on for pages, and must be broken down into shorter sentences in English.

~~(POUO)~~ In attempting to make translations readable, translators must determine how colloquially to render the translations and how to reflect the strength of the statements accurately. (Generally speaking, transcripts of conversations can be translated more colloquially than narrative portions of a text.) Take this sentence, for example, in Japanese: "Moo nihonjin ni hohoemikakeru jiki ga satta." This sentence can be translated more literally, and less forcefully, as: "The time for smiling at the Japanese is past," or it can be translated in a more colloquial and hard-hitting manner as: "It is time to stop being 'Mr. Nice Guy' with the Japanese." Colloquial translation can also be very helpful when a phrase cannot be translated directly. For example, take the phrase "sekai no aru no Saudei" as part of a sentence. A literal translation of this phrase, "Saudi Arabia, a country in the world" fails to convey its actual meaning. A colloquial translation can be employed toward that end: "Saudi Arabia is proud that it has found a 'place in the sun'."

KEEPING UP WITH THE LANGUAGE

One of the biggest problems is that dictionaries of foreign languages are often inadequate and, even with the help of native speakers or other linguists with near-native ability in the language being translated, translators are often forced to build a meaning for the words, phrases, and passages they encounter in translation. Take, for example, the following sentence in Japanese:

"Kokoro ga sutarete kite iru."

Kenkyusha's New Japanese-English Dictionary (the principal dictionary used by the Japanese linguist and the most complete one for use in translating modern Japanese) gives quite a few definitions for the word "Kokoro," among which are "heart," "mind," "feeling," "sincerity," "interest," "care," "will," and "intention." None of these definitions quite fits the meaning of the word "kokoro" in the sentence. Translators must look at the examples given in the dictionary to obtain a "feeling" for how the word is used in a sentence and must also see how the word is used in the context of his text. In this sentence, "kokoro" is the immediate subject of the sentence, the particle "ga" marks the subject, "sutareru" is the verb meaning "to decline," and "kite iru" indicates that the sentence is in the present perfect. From the dictionary examples used to show the meaning of "sutareru," it is apparent that the kind of "decline" denoted by the Japanese verb is a moral decline. From the context of a sentence or passage, it is possible to derive the meaning of "kokoru" as "concern for others" and, as a result, to ascribe a meaning to the sentence as a whole as "People have become less public-spirited" or "People are now more concerned only with their own welfare." (Note that a subject, "people," had to be added to make the sentence grammatical in English. It is quite common for Japanese to omit the subject. That is because Japanese writers or speakers will not repeat the subject of a sentence if they believes that it is apparent to their audience. Translators or interpreters must constantly try to determine what the subject is and supply it in the translation.)

Since foreign countries obtain many of their technical terms from English, one might expect that technical terms would cause few problems, but that is not always true. Some countries prefer to coin native equivalents of foreign technical terms out of pride in their

languages and cultures, and to facilitate understanding of the terms involved. The coining of such neologisms poses a problem for translators, because dictionaries fail to keep pace with them, while translation tends to take place on the frontier of knowledge, including current events and scientific discovery. To add to the problem, the translator often cannot do an effective job of translation without some understanding of that technical subject matter.

The job of translators is first to figure out what words or phrases mean in the original language being translated, and then, if necessary, to ascribe a meaning that fits the context. Foreign loan words provide a good example of this. English loan words in Japanese can take on quite specific meanings with no English counterparts, or they may have no counterparts in English whatsoever. For example, in Japanese "ootobai" (autobike) means a large-size motorcycle, "mopedo" (moped) a medium-size motorcycle, and "mootaabaiku" (motorbike) a bicycle with an engine powering it. English loan words in Japanese may also be borrowed from British English with their American English counterparts taking on different or more specific meanings. For example, "bisuketto" (biscuit) is the British English word for "cookie," and "kukkii" (cookie) is apparently used more to refer to cookies made at home, while "bisuketto" apparently refers to store-bought cookies.

Translators must take into account that British and American English expressions can have diametrically opposite meanings. For example, to "table" a matter means to place it on the agenda in British English, as well as in diplomatic terms, but means to pigeonhole it in American English. "Abekku," from the French "avec" ("with"), has the very specific and different meaning of Japanese of "a couple on a date." Thus, translators must also determine the meaning of loan words borrowed into a foreign language from other foreign languages.

Linguists often must know a little about the phonetics of foreign languages before he can find, or artificially reconstruct, personal or place names written in Japanese phonetics. For example, they must know that "hi" in Japanese phonetics is equivalent to the "ach" sound in German. Translators must realize that the "ga" in Japanese can be pronounced "nga," before they can look for, say, an Indonesian place name starting with "Ng."

Sometimes the translator must know the origin or "locus classicus" of a word or phrase before they can translate it, or translate it well. For example, the Kenkyusha dictionary translates the adjective "naniwabushitekina" as "of the old feeling of Naniwabushi" and does not elaborate. The literal meaning of the term is "like a tune from Osaka," but knowing that does not explain how it is used metaphorically. In order to understand that, and therefore to be able to translate the expression, one must know that a "naniwabushi" is sung with great emotion and fanfare. One may then translate the expression as, in colloquial parlance, "to make a big production" about something, or to play something up unnecessarily. To give another illustration, most Japanese--but very few Americans--are familiar with the expression "Columbus' egg" ("koronbasu no tamago" in Japanese). As in the American English expression "I chopped down the cherry tree," one must be familiar with the story behind the expression in order to fully understand the meaning. As the story goes, Columbus asked his shipmates to see whether they could stand an egg on its end. When he saw that they could not do so, Columbus merely bashed in the end of the egg on a table and caused it to stand that way. Once one has heard this story, one can translate the expression as meaning "deceptively simple."

Conclusions

There is much more to translation than using dictionaries, learning the rules of grammar, and becoming conversant with the intricacies of alien scripts. The translator must try to wrest the meaning of words, terms, phrases, and whole passages by referring to examples in dictionaries, conferring with native speakers or near-native speakers of the language being translated, by acquiring knowledge of technical, political, economic, and other developments through education and experience, and by using his imagination and creativity. He must then rewrite the meaning in English since it usually cannot be translated directly.

Because many years and great efforts are required for one to become a good linguist and interpreter between different worlds, and because that task is so important, every effort should be made to provide linguists with the material and non-material incentives to encourage them to remain in this career field.

An Old Problem (U)

by WES

(U) Answer next month.

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

All I ever wanted to know about DES (U)

by [redacted] C11

P.L. 86-36

We are rapidly moving into the "information society" (if indeed we are not already there). All the information in this "information society" to which I refer has value to at least two people (the sender and the receiver), and most of it has value to a few, perhaps many, other parties as well. There certainly is a need to protect most information from falling into the wrong hands. I am referring here to all types of information, both classified and unclassified, military and commercial, etc.

This need to protect information is especially acute at the most vulnerable point--when information is transferred via some communications medium from one place to another. It was to aid in filling this need to protect unclassified information that the National Bureau of Standards (NBS) placed a call in 1973 to all interested parties to submit suggestions for an encryption algorithm that could be used as a National Standard for Data Encryption. Only one algorithm was submitted that was judged to be adequate for U.S. Government use in protecting unclassified information. This algorithm, submitted by the International Business Machines (IBM) Corporation, was reviewed, accepted, and published by NBS in 1977 as Federal Information Information Processing Standards Publication 46 (FIPS PUB 46). This standard describes a mathematical algorithm for transforming 64 bits of data, using a 64 bit key (56 independent bits, and 8 bits parity) into a 64 bit output. This algorithm is the Data Encryption Standard (DES). The NBS followed FIPS PUB 46 with another standard describing several modes of encryption that could be used with the algorithm. This new standard, FIPS PUB 81, described how the DES algorithm could be used in a communications system in both the block and stream cipher modes [1].

In 1976, the Federal Reserve System wanted to purchase a data communications system for use in banking and Electronic Funds Transfer. They requested that NSA help them in the area of cryptographic protection. Out of this effort came the beginning of two standards for using the DES algorithm in unclassified U.S. Government cryptographic applications.

- The first of these two standards, Federal Standard (FS) 1027, prescribes general physical and electrical measures to insure that neither the key variable nor the plaintext data is compromised. This standard is a security-related document.
- The second standard, FS 1026, prescribes only electrical measures to insure both:
  - Interoperability of equipments from different manufacturers, and
  - Security.

These standards have gone through a lengthy process of review and comment (as do all standards generated in a public forum). FS 1027, on general security, has been approved; FS 1026, on interoperability and security, is near final approval.

The balance of this article is devoted to an explanation of the objectives of these standards and how they are written to achieve these objectives. FS 1027 is described first since it is a general standard applying to all DES cryptographic components, equipments, systems, and services that the U.S. Government procures.

FEDERAL STANDARD 1027

FS 1027 prescribes general security requirements for equipment that uses the Data Encryption Standard (DES) algorithm for enciphering data. The word "general" perhaps best describes the standard in that it specifies only general physical and electrical parameters that must be met by any equipment (voice, data, facsimile, etc.) that uses the DES in a telecommunications environment. The scope of the standard can be best described by examining the security objectives of the standard:

- To prevent inadvertent transmission of plain text.
- To prevent theft, unauthorized use, or unauthorized modifications of cryptographic equipment while installed.
- To prevent unauthorized disclosure or modification of key variables while in DES cryptographic equipment.
- To provide interoperability between key variable loaders and DES Cryptographic equipment, and to permit the use of standardized keying material for U.S. Government applications of the DES algorithm.
- To prevent data encryption when a critical cryptographic failure condition exists, and to generate an alarm when a critical cryptographic failure is detected.

These objectives are met in the following ways.

Physical Security

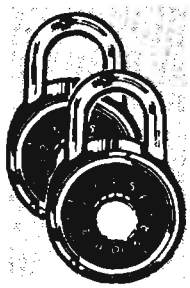
The standard requires that the Data Encryption Equipment (DEE) have enough physical integrity to insure that any unauthorized access to the equipment (either to remove it or to tamper with it) will leave signs that can be easily detected by visual inspection only (e.g., bending of the front panel, drilling of holes, etc.). Two different physical keys are required to insure that secure mounting, tamper resistance, and key variable protection are provided for.

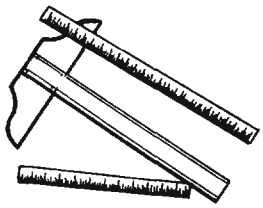
Key Variables

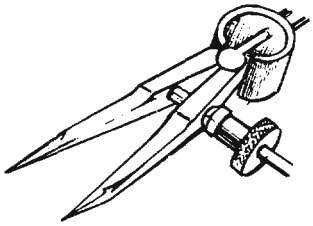
The standard provides for the protection of DES key variables both as they are entered into the DEE (two methods provided) and as they are used internally within the equipment. Key variables can be entered either via a self-contained manual input device (e.g., a hexadecimal key pad) or through a standardized electrical interface to a key variable loader (e.g., a KOI-18, which is a general purpose key variable entry device). After the DES key variables are entered into the encryption device, the standard requires that it must not be possible for the key to be compromised in either of two ways:

- by being read back out of the DEE, or
- by external access as a result of any single failure.

To further insure protection of the key variables, any detected tampering (e.g., unauthorized physical access) shall automatically zeroize (erase) the key variable.







Initialization Vectors (IV'S)

The standard requires that IV's that are used

- be generated by the DES process or some other random means,
- that they be either 48 bits (Cipher Feedback) or 64 bits (Output Feedback or Cipher Block Chaining) long, and
- that they are used to initialize each new cipher text chain.

Encryption Functions and Alarms

Extensive automatic "self tests" are required by the standard to insure that the DEE does not fail in some undetected manner and transmit either plain text or (worse yet) raw key. To this end, the encryption self testing must be done by either:

- having two complete DES encryption devices that are continuously compared as a self check, or
- frequently encrypting test words and checking the results.

Fail Safe Design Requirements

The standard requires that, to insure the security of the plain text and key, the unit shall be designed in such a way that any single failure will not allow either transmission of the key variables or transmission in depth (use of the same IV).

Test Mode

As an additional safeguard, an externally (e.g., manually) initiated test mode is required. This mode is analogous to a self test, and that can provide assurance of that the equipment is operating properly.

Control Functions

A standardized set of DEE control functions is required (e.g., Power ON-OFF, Reset, and Mode). This requirement assures that DEE operators will have the requisite standardized control functions necessary for total system security.

Status Indicators

Visual status indicators for the control functions (above) are provided by the standard.

Retention of Critical Storage

It is important that proper encryption parameters (e.g., key variables, IV's) be used at all times, even after power interruptions. To insure this, the standard requires that the DEE shall be able both to retain these parameters during power interruptions, and also to test that the correct parameters have been retained.

Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC)

To insure that there are no compromising RF or power line emanations that would invalidate

the protection provided by the rest of the standard, the DEE is required to have a specified degree of EMI and EMC protection.

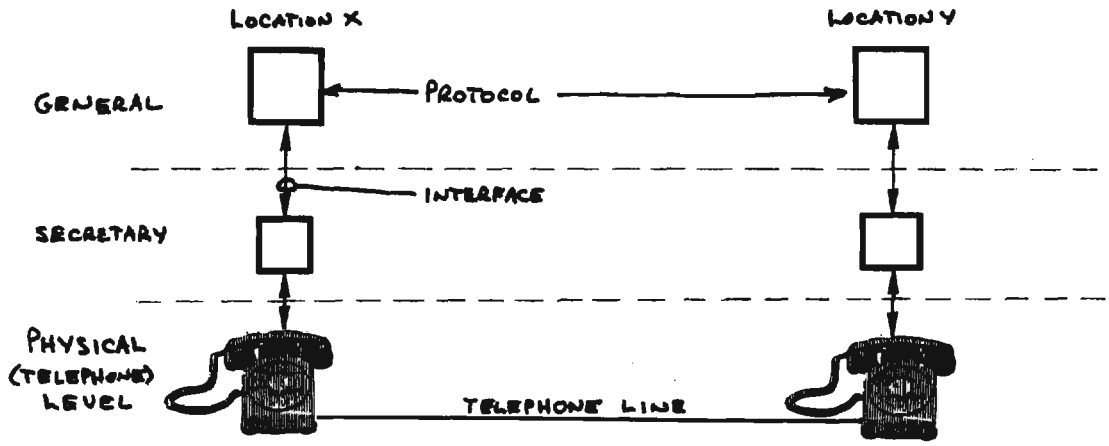
PROPOSED FEDERAL STANDARD 1026

PFS 1026 describes the application of the DES algorithm to data communications for ADP systems and for narrative text information systems. This standard refers to the International Standards Organization (ISO) Open Systems Interconnection (OSI) model for data communications at the Physical and Data Link Layers. At some future time, there may be a whole list of standards that describe encryption at a range of OSI levels, from the simplest at the Physical Layer (Level 1), which is sometimes called the "RS232" level, to the most complex Level 7, which is called the "Applications" Layer. Before we describe the Proposed Federal Encryption Standard, an explanation of the layered structure in data communications is in order.

The OSI architectural model of data communications was developed by the ISO as a conceptual framework within which data communications equipment can be designed and built to be interoperable. This conceptual framework encompasses a wide variety of communications procedures (called protocols), that range from the most simple and specific to the most complex and general. This wide range has been divided into subdivisions called Levels. The simplest level, called Level 1, is the Physical Level, or Layer, and is commonly exemplified by the familiar RS232 interface seen on most printers, data terminals, modems, etc. The most complicated level, called Level 7, is the Applications Level, or Layer. The other levels are:

- L2, Data Link,
- L3, Network,
- L4, Transport Layer;
- L5, Session; and,
- L6, Presentation.

As an illustration, suppose that General X wants to speak on the telephone with General Y (see Figure 1). Perhaps he would tell his secretary to get General Y on the telephone and to call him (General X) when the telephone connection is established (a General only talks to other Generals and to his immediate secretary). General X's secretary goes to her telephone and places a call to General Y's office. General Y's secretary gets General Y on the telephone and then relays to General X's office that all is ready for the conversation. General X's secretary receives this information, gets General X on the telephone, and the call can then be completed. This simple example illustrates the layered concept of communications: there is a "General" layer, a "Secretary" layer, and a "Physical Telephone" layer. Within these layers, there is a General-to-General communications protocol and a General-to-his-Secretary communications interface. There is a similar set of protocols and interfaces at the Secretary and Telephone layers. The OSI layered structure is similar to this, with the (Physical) Telephone layer being analogous to the Physical Layer.



GENERAL X TALKS TO GENERAL Y

FIGURE 1.

PFS 1026 describes the application of the DES algorithm to data communications at both the Physical and Data Link Layers. The standard describes on-line (not off-line) encryption; i.e., encryption that occurs simultaneous with the communications process itself.

There is a two-fold objective for the standard:

- to permit interoperability, and
- to provide acceptable security for government data communications facilities, with protection against
  - a "passive" security threat, where the interceptor merely reads the communications traffic but does not divert, modify, jam, or in any way change the traffic; or
  - an "active" security threat, where the interceptor not only does the interception, but also modifies the traffic in some way, i.e., inserts, deletes, modifies, or repeats the traffic.

The proposed standard provides a method of encryption that, with one exception, can achieve all the above objectives. The one exception is encryption at the Physical Level (Level 1), where it is possible to provide only passive security threat protection, due to technical parameter limitations of the physical communications process. The proposed standard also provides a method of electronically distributing DES key variables with the same degree of protection provided to other data.

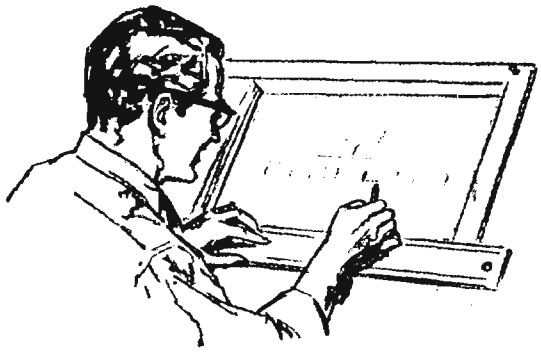
It should be pointed out that encryption at the Physical Level can be done completely independent of any data communications protocol that may be used. Encryption at any other level (e.g., Data Link, Network, or higher), must be implemented in conjunction with, and fully compatible to, whatever communications protocol is used at the layer where encryption takes place. The advantage of encryption at the Physical Level is that the implementation is very simple and, hence, inexpensive. The disadvantage is that the traffic must be decrypted at each intermediate switching center through which it is routed. Hence, at each intermediate node of a network, the traffic must be protected; i.e., it becomes "red" data. The advantage, then, of encryption at higher levels of the OSI architecture is that the higher the level of encryption, the fewer security restrictions there are at intermediate switching nodes. For example, if encryption is done at the network level, then the "black" (encrypted) data resulting from the encryption process can be passed safely through any network that does routing at either the Link or Network level. Examples of this type of network are ARPANET and TELENET.

Conclusion

In this short article, I have attempted to provide a brief overview of the DES Federal Standards that have been and are being widely distributed throughout both the Government and private industry. The overall objective of this is to provide minimum security and interoperability standards to which the commercial manufacturers can provide equipments in a competitive market place. Early indications are that these objectives are being met, since commercial DES cryptographic equipments are beginning to appear, and are being used by both private industry (banks) and the U.S. Government.

---

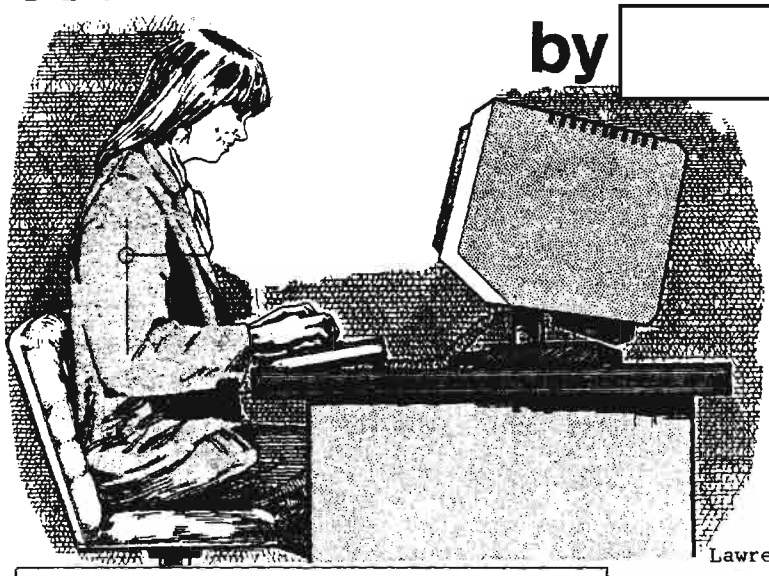
1. The two block modes are the Electronic Code Book Mode (ECM) and the Cipher Block Chaining Mode (CBC). The two Stream modes are the Cipher Feedback Mode (CFB) and the Output Feedback Mode (OFB).



Human Factors Corner

by [redacted]

P.L. 86-36



SYMPOSIUM ON VIDEO DISPLAY TERMINALS AND VISION OF WORKERS, National Academy of Sciences, 20-21 August, 1981
(reprint from Human Factors Letter #2-81)

I attended this meeting, along with two other members of Human Factors SIG (Don Landry and Don Friedmann). There were very few printed handouts, and no proceedings were issued at the symposium itself, though some form of printed report may be published later. The following paragraphs contain a summary of my impressions, and some comments on important questions raised in my mind by what I saw and heard.

The Symposium was composed primarily of panel discussions, preceded by one or two introductory or overview presentations. The program was as follows:

I. Introduction and Overview (Edward Rinalducci, Marvin Dainoff)

II. Methodological Issues in Field Surveys of Video Display Terminal (VDT) Operators. (Robert Guion, Steven Sauter, Dainoff, Olov Ostberg, Hugh Taylor)

III. What Visual Problems Have Been Associated With Video Viewing? (Leonard Matin, Lawrence Stark, Ostberg, Leif Hedman and an extensive panel)

IV. Optical Contributions to Visual Discomfort and Visual Performance With VDTs (Harry Snyder, Vincent King, Etienne Grandjean, and a panel)

V. Radiation Exposure (David Sliney, William Murray, panel)

VI. Opthalmic Pathology--An Epidemiological Perspective (Alfred Sommer, Arthur Frank, Lawrence Stark, William Halperin, Hugh Taylor)

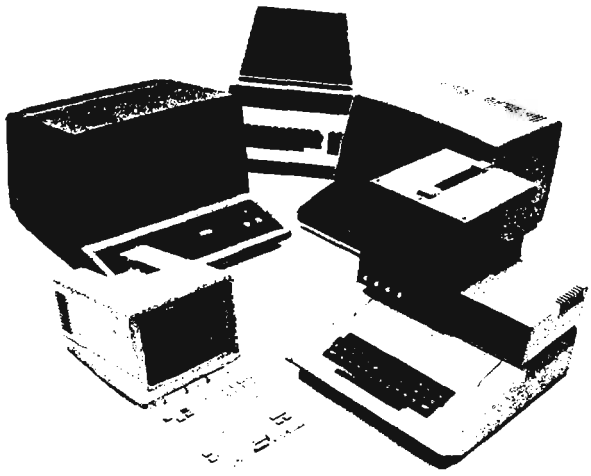
VII. Job Design and Organizational Aspects (Robert Guion, panel)

VIII. What Measures Might Alleviate Operator Discomfort Associated With Video Viewing and Improve Performance? (Harry Snyder, K.H.E. Kroemer, Martin Helander, panels)

A. Display, Lighting, Workplace, and Job Design

B. European Guidelines and Other Approaches

IX. What Research is Needed? (Rinalducci, panel)



The weight of opinion seems definitely to favor the safety of CRTs, at least as far as acute, immediate health effects or damage to vision are concerned. Most experts seem to agree that there are no discernible acute effects of radiation. There may be temporary changes in vision after several hours of unbroken CRT work, but these disappear entirely after a few minutes away from the scope. Similarly, temporary aches and pains may arise from sitting in a cramped and unnatural posture for long hours at a terminal; these, too, vanish after a break or change of position, or even a change from one piece of work to another. In fact, the ordinary fluorescent lights used in most offices give off far more potentially-harmful radiation, and may have more impact on vision as well, than any CRT. Chemicals used in widely-available copy papers, and airborne particles of dust from carpeting, wallboard, drapes, and office furnishings may account for far more health hazard than anything related to CRTs.

Despite these reassuring words on acute effects, some major questions remain. All the experts admit that few studies have been made on longer-term effects of radiation on health or fertility. Little or nothing is known about long-term effects of daily CRT use on vision, mental health, or muscular and skeletal health. Some forms of radiation which CRTs might emit, and which might be harmful, are as yet unmeasured in the field because no instruments are yet available to measure them under field conditions. A final, and in my opinion highly important class of potential problems remains still to be addressed by empirical studies: the complex area of job design, automation and regimentation of office work, and changes in the way a worker thinks of himself or (more likely) herself and the job. Since I find this last area most interesting, I will focus my comments on the findings of the panel on "Job Design and Organizational Aspects", chaired by Robert Guion, Department of Psychology, Bowling Green State University, Ohio.

This panel was the only one which included any women, or any real representation from office workers or VDT operators as such. The other panels were made up almost exclusively of professors and researchers, and were entirely male. Panel members were the following: Janet Bertinuson (Consultant, Occupational Health); Richard Granda (Design Center/Human Factors, IBM); Etienne Grandjean (Swiss Federal Institute of Technology); Judith Gregory (Working Women Educational Fund); Steven Sauter (Dept. of Preventive Medicine, Univ. of Wisconsin); and Lambert Stammerjohn (Motivation and Stress Research Section, NIOSH). I noted that there were a considerable number of women in the audience throughout the Symposium; many of these were supervisors of office workers or human factors professionals interested in problems of VDT operators. In discussions at breaks, etc., I overheard a number of complaints from women attendees that many speakers were "naive", didn't know "what was going on in the real world", and were out of touch with the viewpoint of the office worker and manager of VDT operators in a real-world setting. Ms. Bertinuson and Ms. Gregory succeeded in counteracting some of this "ivory tower" atmosphere for the Job Design panel, in my opinion. I will summarize the panel discussion for several major questions:

- How do task characteristics vary in different types of VDT work?

  Ms. Bertinuson provided an excellent overview of this topic. She distinguished five major categories of VDT work, depending on such things as eye-movement, decision-making, use of keyboard and screen, etc. I believe these categories might usefully be applied to VDT work in the Agency also. Arranged on a scale of increasing variety and decision-making, the categories are:

  - Data Entry. The eyes are focussed on a source document much of the time. There is a high rate of keystrokes per

minute and hour. Work is routinized and repetitive. Speed, accuracy are strictly monitored. There is little opportunity for control by the worker over pace or work content; the jobs are "dead-end" and offer few intrinsic rewards. Many jobs are short-term or temporary, involve concern about job security.

- Data Acquisition. The eyes are focussed on the screen much of the time. Information is retrieved by small bursts of keying, viewed on screen, perhaps with a certain amount of data entry as well. Work is more interactive and "screen-intensive". There is somewhat more variety, less rigid routine.

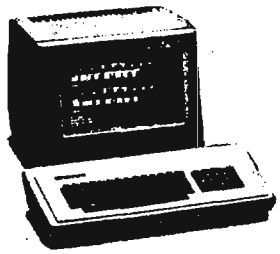
- Interactive VDT Use. Also screen-intensive, but with still more variety, decision-making. There is eye movement between the keyboard and screen when the operator is first learning the task, more focussing on the screen alone after experience. These jobs can vary greatly depending on how management views and structures them for the operators. For example, in a travel reservations application, operators interacting with customers have more freedom than people in a "back room" who are driven by a computer which schedules and allocates their work. A big problem for operators in these interactive jobs is the wait time for system responses on the screen; management thinks this is a "rest" for the operator, whereas in reality it is a constant stressor, which feels to the operator like "hitting a wall" over and over again. Another major problem is the highly symbolic nature of the content, with predesigned formats and codes which may have little meaning for the operator, and management's attitude that operators should work mindlessly: "Don't think about it--just do it; thinking will slow up your work too much!"

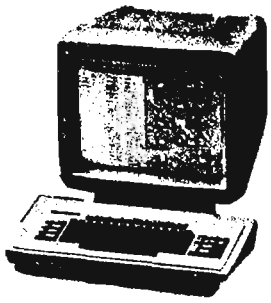
- Word Processing. This includes a wide range of decision-making and control by the operator over how the job is done, and how the system is used. At best, the operator can format, compose, edit, decide when to make a hard copy, when to edit on the screen, etc. Again, a lot depends on how management has structured the job, and what restrictions are placed on the worker.

- Creative, Free use of VDT as a Tool. Programmers and systems designers who develop systems, procedures, and formats; scientists and engineers and other researchers; creative writers, executive secretaries and office managers, graphic designers--these are the "crème de la crème" of VDT users. They are the people who say "I love MY terminal--I wish it was really mine, to take home with me at night!" They are free to use the terminal and the entire complex of computing power behind it as their own creative tools at their own pace.

● In What Ways Has the Introduction of VDTs Restructured Jobs?

Dr. Sauter asserted that there are indeed sources of stress which are unique to VDT jobs when they are badly designed. Primary among these is a different pattern of temporal constraints, a more rigorous pacing of work, especially for data entry jobs, but also in potentially freer kinds of jobs when they are restrictively and harshly constrained by management. He said that the time pacing stress in VDT jobs is worse than that in the actual industrial assembly-line. The worker on an assembly line can usually "work ahead" and give himself a break or change of pace, whereas the computer is always "ahead of" the VDT worker no matter how fast she works. Another unique feature of the VDT job is the apparent "smartness", omniscience, control of the system over the worker, and its capacity to monitor her actions. Dr. Sauter listed the following stressors which were found to be specific to VDT operators when they were compared to workers in similar jobs but





not using VDTs: loss of control over pacing of work; fewer rest breaks; more pressure of work; lessening of co-worker interaction; loss of interest in the work; less variety in the work. This was true even in the case of a data entry job, where a former keypunch operator complained that now she could no longer punch her own control cards, or exercise what little control she had before over formats.

Ms. Gregory provided some vivid illustrative examples of actual cases where health complaints were involved, to hammer home some of these points about the way job design factors can change the way basically similar VDT jobs impact on the workers. For example, in one law office, a high-level word-processing specialist at one extreme was able to choose for herself when to make a hard copy, edit this in pencil, then make the changes via the terminal, thereby limiting and controlling the time she was required to view the screen. On the other hand, lower-level word-processors doing the exact same job in a secretarial pool were not permitted by management to make a hard copy, but were forced to edit directly via the CRT at all times, so that they had no control over the amount of time spent viewing the screen, or how they did the job (on the pretext of "saving time" and "increased efficiency"). In an insurance office, claims examiners were kept on mandatory overtime for ten-hour days over periods of up to 8 weeks; they reported severe health complaints! Customer-service representatives at VDTs in a telephone office were paced by an automatic call-distribution system that allowed them only a set time for each call. In a publishing firm, CRT typists were monitored; their keystroke rates were publically posted for each week, and they were paid on a floating scale proportional to the posted rate! VDT operators in a travel office were allowed a ten-minute rest break after 2 hours, but if they had a customer call at that time, were forced to forego their break entirely and work 4 hours straight until lunch or quitting time. These are some examples, randomly chosen from all too many similar cases in the real world, of the ways mean-minded and short-sighted management uses VDT's and automation as ways of regimenting office workers into an assembly-line. It was pointed out that 90% of female clerical workers are not unionized.

● What Should Be Done to Improve VDT Job Design?

Ms. Gregory offered a number of good recommendations. She began by asserting that the new technology offers us an opportunity for good design, not just an unimaginative "electronic equivalent of the old job at a speeded-up pace". More, not fewer, skills should be built into jobs. The operators should be afforded more, not less, control over work pace. More on-the-job training should be made available to all employees to allow for advancement, instead of the present trend toward a small elite of flexible jobs at the top and a vast increase in the number of routinized, dead-end jobs at the bottom. Increased pay and lowered working hours should be offered to workers as a consequence of the increase in productivity and lower error rate made possible by VDTs. We need to reverse the present trend in the US toward using VDTs as an excuse to turn more and more tasks into rigid, routinized "data entry" type jobs. We should follow the initiative of Europe in allowing more work breaks, requiring a broader mix of tasks, and regulating the amount of time spent at a screen. Richard Pew made some imaginative suggestions from the audience during the discussion: make data entry itself more interactive, by providing good error messages and prompts to let the operator find and correct errors; provide individual performance feedback to the operator herself from keystroke monitoring, so that she may better her own performance, while only global statistics are provided to management; put tools for work-scheduling into the hands of the operator, so that she may use the computer as an aid in planning her own tasks over a day or week.

I Remember... (U)

by [redacted] T5

MILLION DOLLAR 'PLUG'

(U) As part of my job as book buyer for the Agency during the 1960s, I often visited a bookstore off Wisconsin Avenue in Georgetown, down from Massachusetts Avenue, also known as Embassy Row. The manager surprised me one day by saying that the fire hydrant in front of his store was worth a million dollars to him. Although I knew that his stock was large and that his store had spread out over several houses in a row, I could not believe he was saving that much on insurance, so I asked him what he meant.

(U) The manager explained that because the parking space in Georgetown is so limited, the diplomats could always find a place to park directly in front of his store by blithely ignoring the fire hydrant. Thus he estimated that the plug was worth a million dollars in increased business.

EXPRESS SERVICE

(U) During the 1960s, Library Acquisitions had a pool of LIC (Limited Interim Cleared) people that could be drawn upon for help. Once I had a top priority request from the Front Office for a newly published book, and there was no staff car available. I asked for a volunteer to ride the shuttle bus to the Pentagon, make a mad dash to the bookstore there, and return with the requested book on the returning shuttle bus. A young man made the trip. He was thrilled with the excitement of the trip to the Pentagon, but I often wonder if he still remembers what book he brought back. I don't.

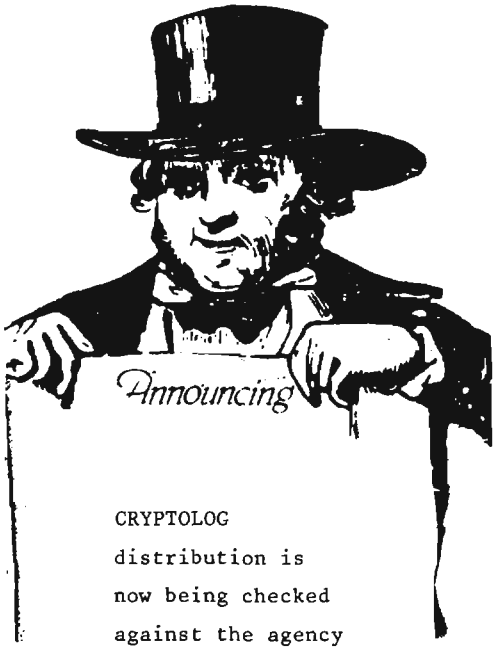
N.S.A. Means?

(U) Those employees who came to work before September 1960 were always cautioned to remember that N.S.A. stood for "never say anything." After the defection of Bernon F. Mitchell and William H. Martin, the Washington wits whispered that N.S.A. stood for "not secret anymore."

Solution to last month's NSA-CROSTIC

"Swahili [Dictionary]," [redacted] from an article entitled "Language in the News," CRYPTOLOG, September 1974

"Kajiga Balibutu, a priest from...Zaire... recently completed and published a 700-page Swahili dictionary. Unfortunately, the report from Azap (the Zairese news agency) didn't [mention] whether the volume was a bilingual dictionary or was entirely in Swahili, but our guess is that it is the latter."



CRYPTOLOG distribution is now being checked against the agency locator file. If you move and don't change your locator information, you may lose your subscription to CRYPTOLOG.

P.L. 86-36

★24 .oN CITSORC-ASN

This one has a few super-easy definitions for the benefit of those who complain that these puzzles are too hard. After all, you can hardly go wrong with Shakespeare or Eisenhower, can you?