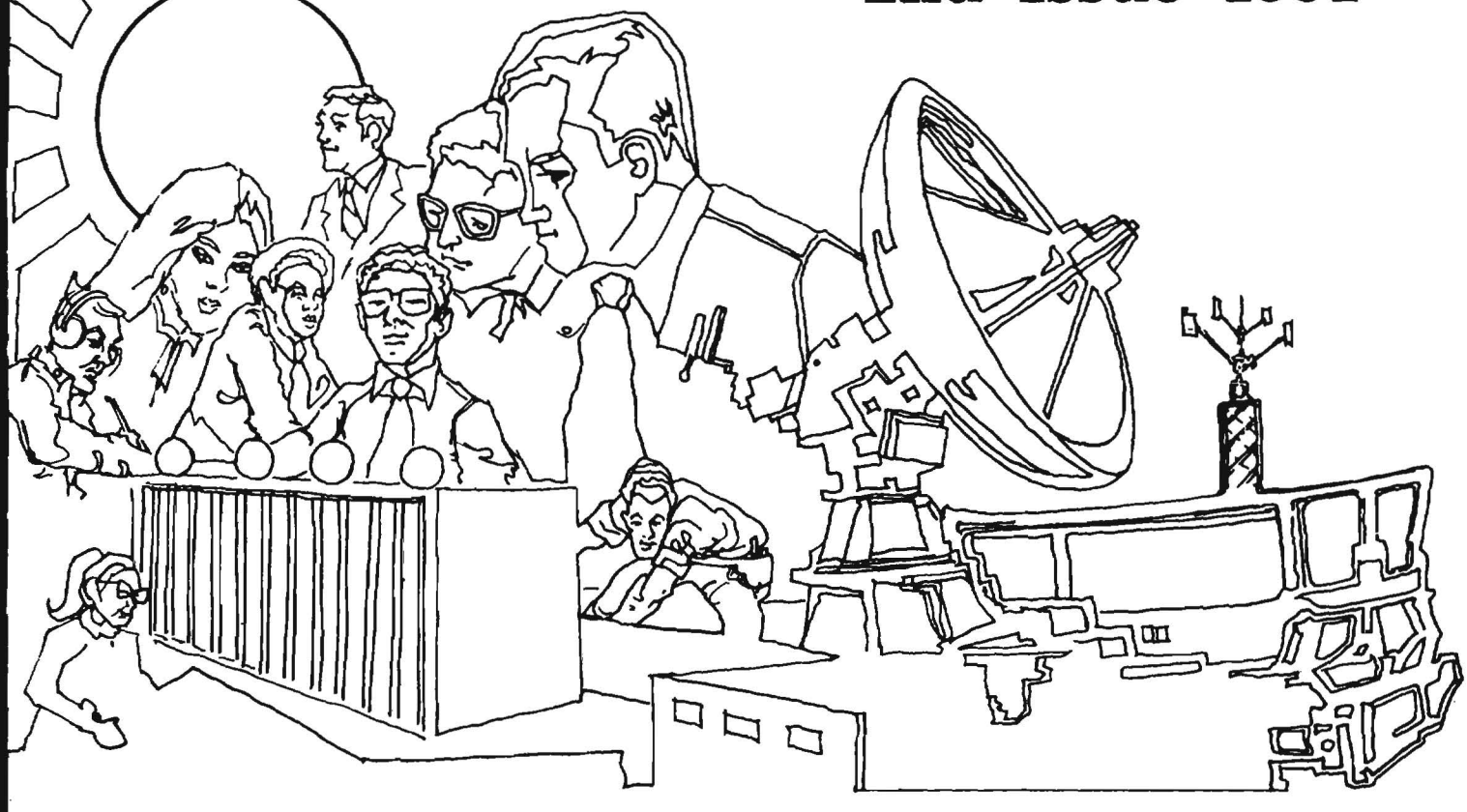
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

# CRYPTOLOG

## 2nd Issue 1991





P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

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

~~NOT RELEASABLE TO CONTRACTORS~~

# CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XVIII, No. 2 ..... 2nd Issue 1991



To submit articles and letters, please see inside back cover.

For New Subscription or Change of Address or Name

**MAIL** name and old and new organizations and building to:

Distribution, CRYPTOLOG, P1, NORTH
or
via PLATFORM: cryptlg @ bar1c05
via CLOVER: cryptlg @ bloomfield

**Please DO NOT PHONE about your subscription or matters pertaining to distribution**



All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

~~FOR OFFICIAL USE ONLY~~

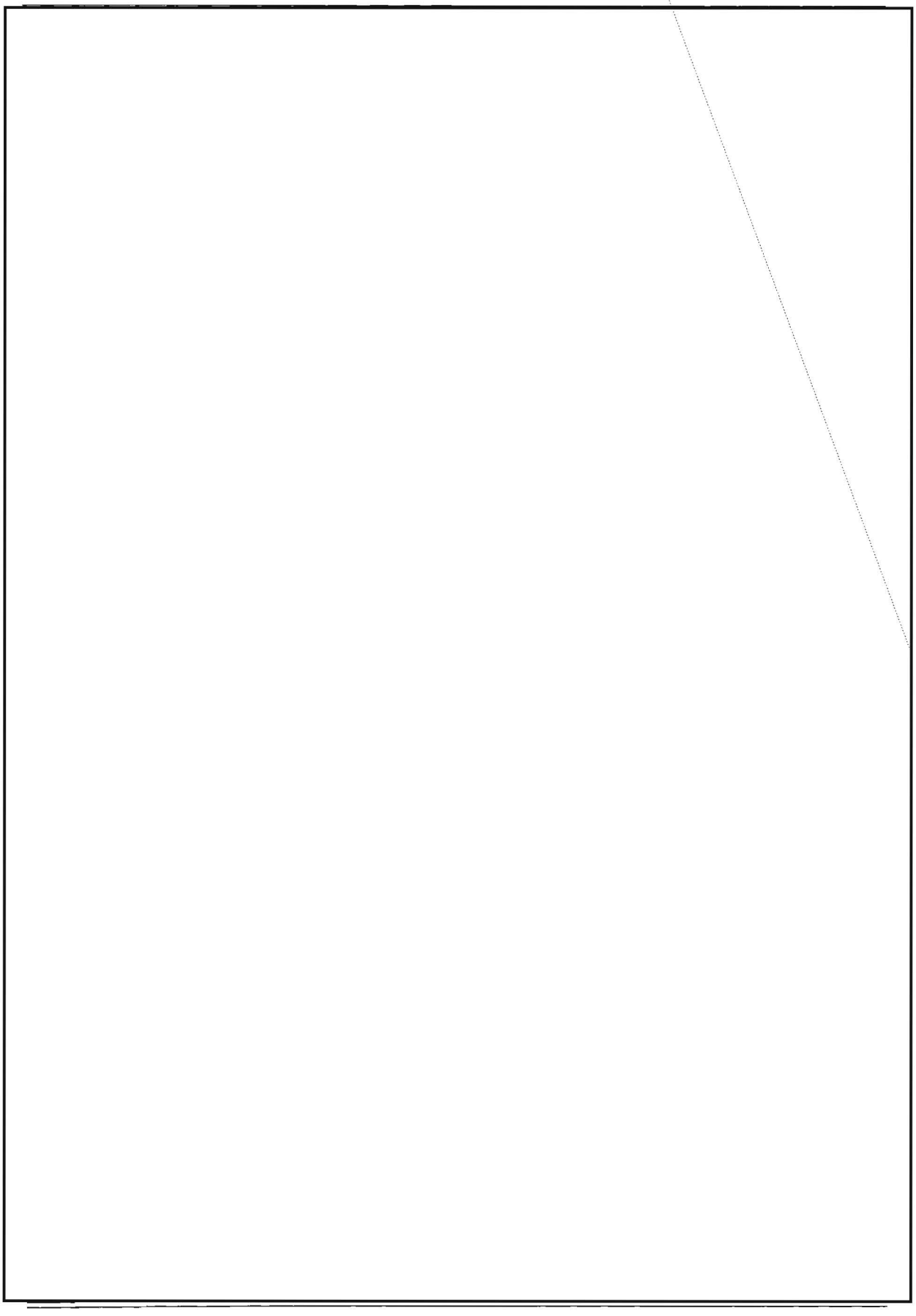
# SEA HUNT

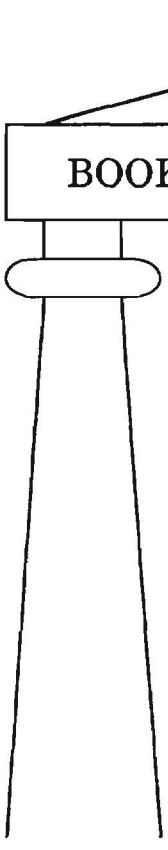
~~*This article is classified* **TOP SECRET UMBRA** *in its entirety*~~

P.L. 86-36



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





# BOOKBREAKERS' FORUM ON MACHINE AIDS

## 1971 * 20th ANNIVERSARY * 1991

**Wednesday, Thursday, Friday**

**30 October—1 November 1991**

❖ ❖

***Informal Seminars***

***on***

***Computer Aids to Bookbreaking***

Who should attend? Anyone working on codes or code charts:

Linguists
Cryptanalysts
Bookbreakers
Cryptolinguists
Providers of computer support to code problems
Managers of code problems

For more information and to get on the mailing list, please fill out the coupon below, or write your name, organization, and building on a piece of paper and send it to:

[redacted] **Chairman**
**Bookbreakers' Forum on Machine Aids**
**P15**
**Ops-1 NORTH**

P.L. 86-36

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Name_____

Organization_____ Building:_____

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -



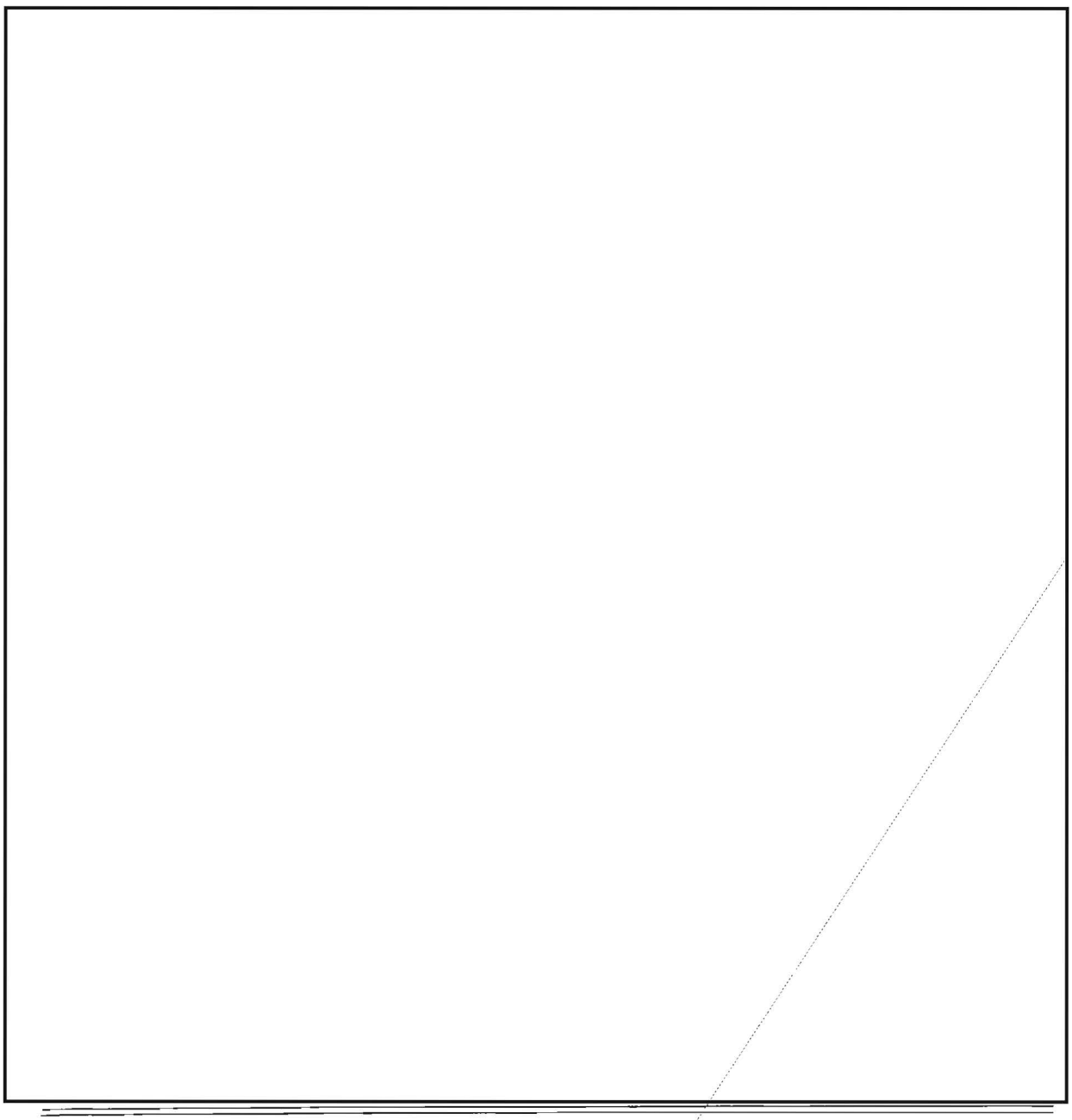
~~FOR OFFICIAL USE ONLY~~

# Textur Reporting

## *SIGINT with Feeling*

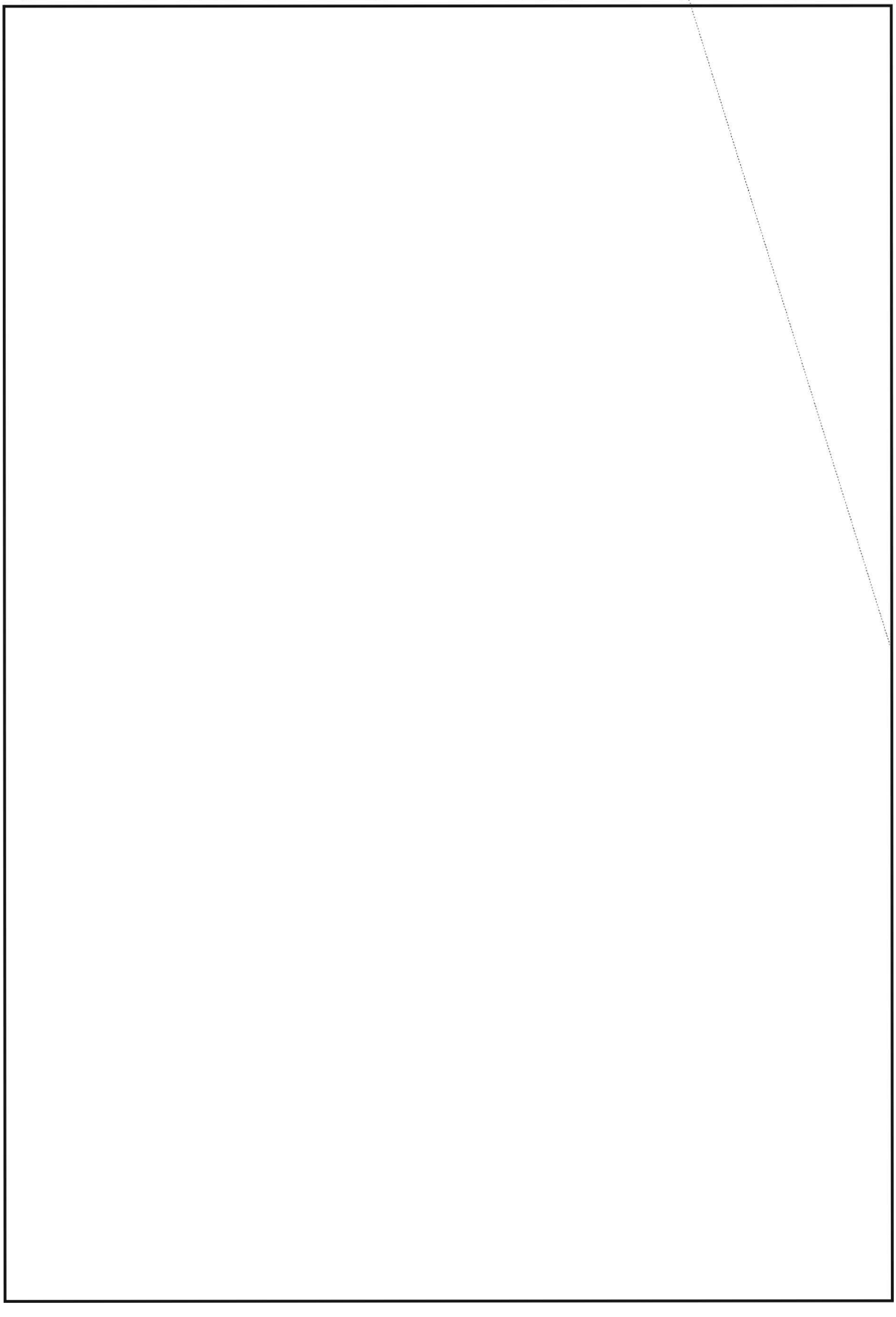
P.L. 86-36

E34





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

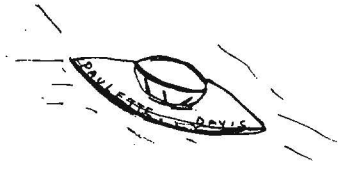


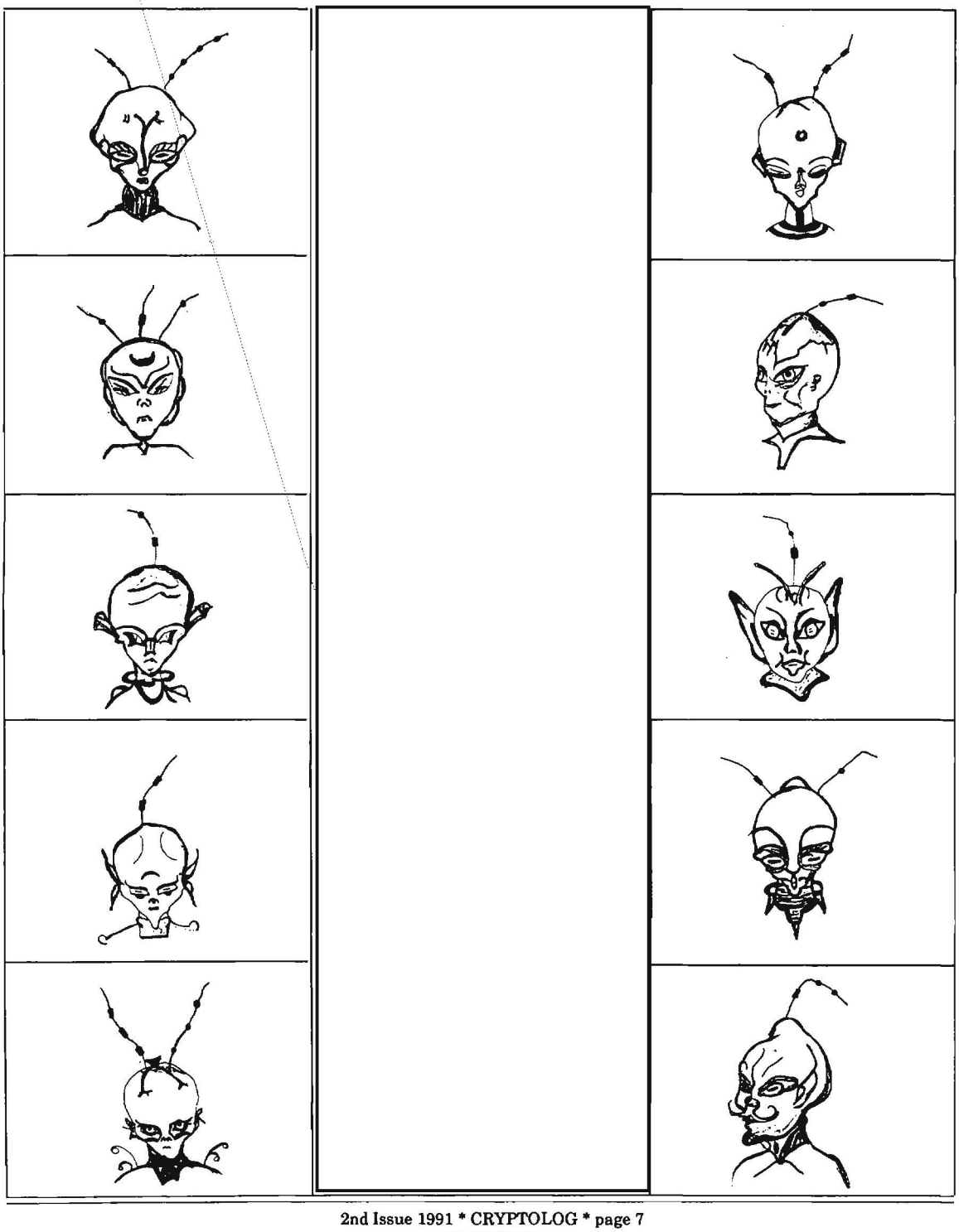
~~SECRET~~

# THE TEN MOST WANTED

by [redacted] W332 P.L. 86-36

P.L. 86-36





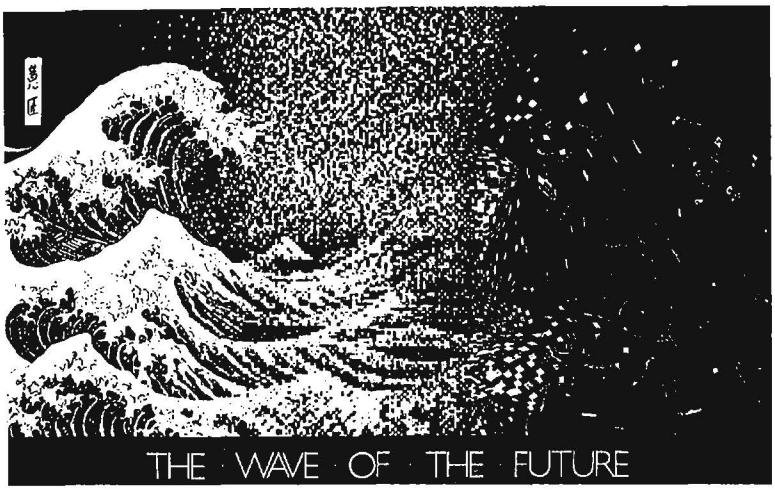


~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~(FOUO)~~ The staff of W332 will be very happy to brief any audience. The number to call is 963-6388 (secure); ask for [redacted]

*Find the hidden message! The first five solutions win CRYPTOLOG mugs. (P1 members and CRYPTOLOG Board members are not eligible for a prize.)*

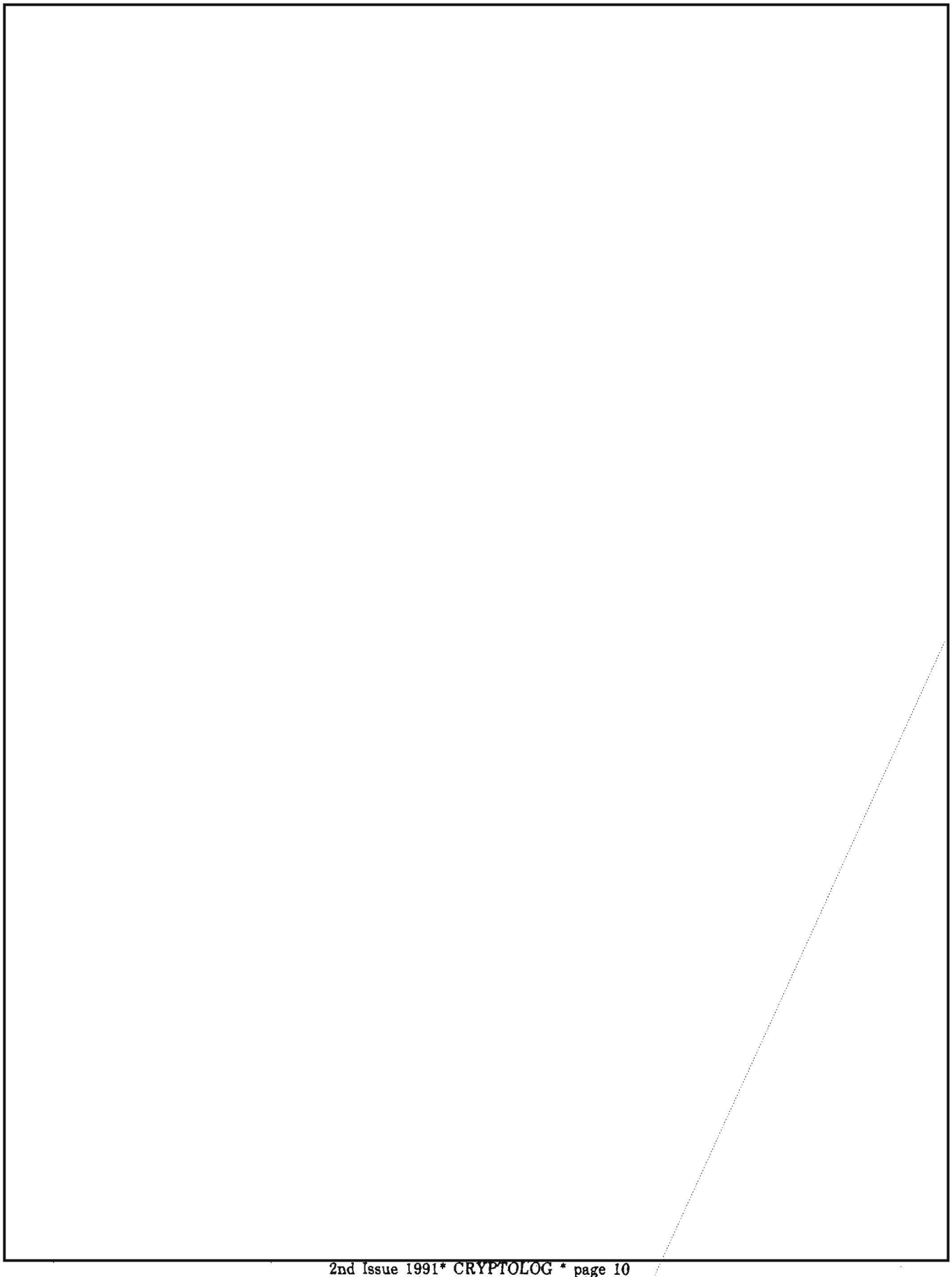


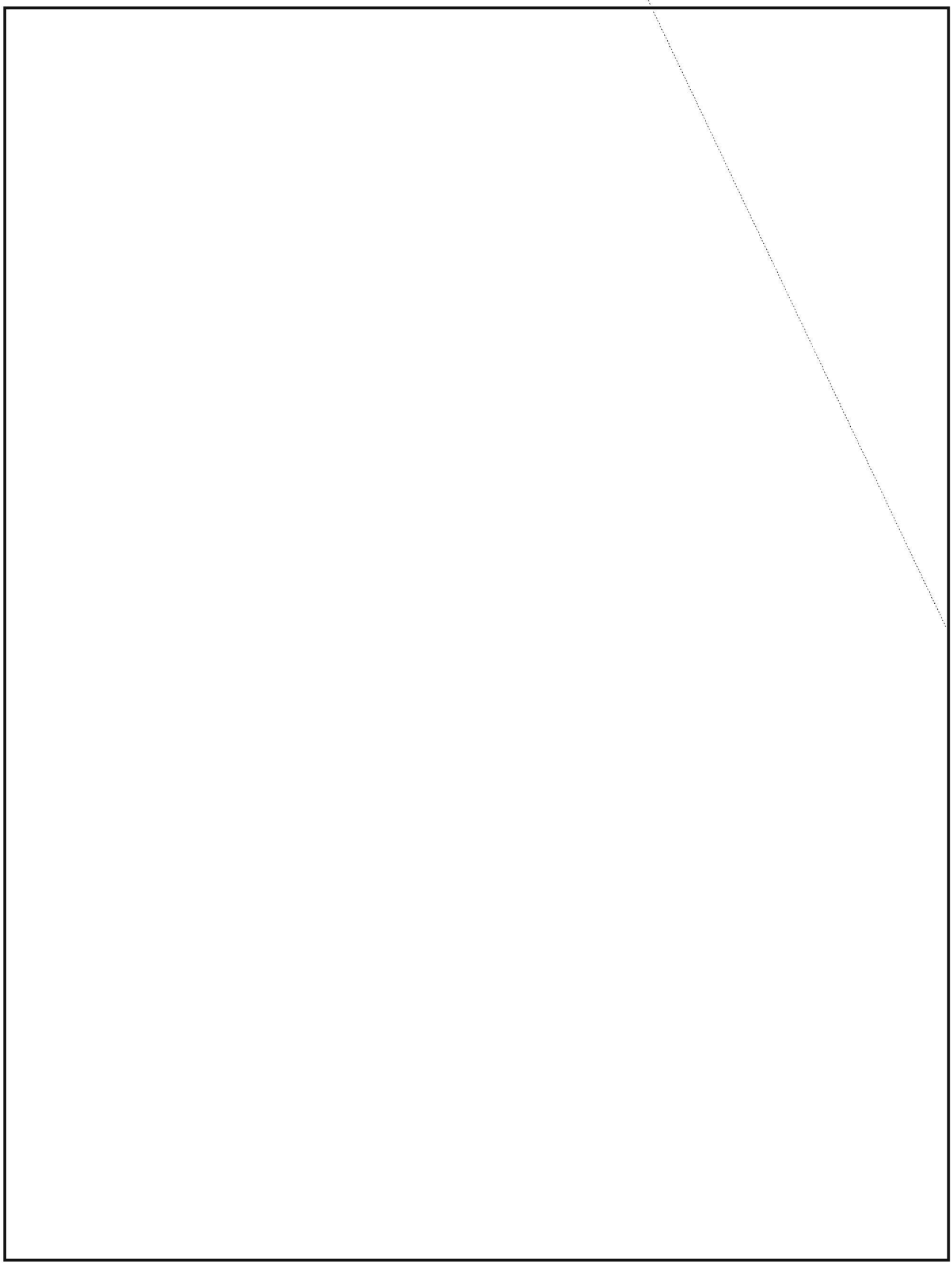

# NEW MILLIMETER WAVE DETECTION SYSTEMS

R541

(U) One of the strongest images of the recent war in the Middle East was that of reporters broadcasting seemingly effortlessly from rooftops in Baghdad or the sands of Kuwait. But this kind of mobile reporting is really not so easy because the equipment needed is quite heavy, the antennas are about 7-8 feet in diameter, and several technicians are necessary to operate the equipment. This may change quite rapidly in the future, however, as the push to higher frequencies in the millimeter range, conventionally, 30-300 GHz, will make truly suitcase-size earth terminals possible. With antennas as small as a foot or so in diameter and with enough bandwidth to accommodate all the reporters of a future operation (a truly large number!), such millimeter wave systems will really "wire" the global village. The military is already studying the use of this wavelength region for communication satellites which would use much smaller, much less complex ground sites, yet provide an enormous increase in channel capacity. Can the commercial world be far behind?

(U) Another image left with us from DESERT STORM was of smart bombs that homed in on their targets with surprising accuracy. Although these weapons were hardly news to even the most casual reader of *Aviation Week*, their actual successful use in combat will surely spur further research in this direction. One of the most promising proposals in the continuing search for battlefield superiority is the use of millimeter-wave guided weapons. This wavelength region is very well suited for such a mission. Metal targets stand out well from any natural background, and the target is not obscured by dust, fog, rain, or the smoke of burning oil wells. The small antenna would fit into a modest missile of only 3-6 inches in diameter, yet it would provide both sufficient gain and small enough beam width to readily find tank-size targets. Together with some modest processing capability such as "fire and forget," warheads delivered from long range could provide an enormous advantage on the future battlefield.





## Quasi-optics

(U) Quasi-optical concepts treat millimeter radiation as one would optical radiation in that lenses and other focusing elements are used to concentrate the energy to be detected. The main advantage over standard parabolic reflectors is that the system can be designed so that an array of detectors can be in focus and at the same time allow a "staring" nonscanning system to cover a whole sector without any need for mechanical movement. To take full advantage of this new capability implies that a detector array is available that has dimensions no larger than the wavelength of the radiation. In the millimeter wave region this means that the detectors must be made by some photolithographical process.

(U) Figure 3 shows a millimeter quasi-optic configuration that will be used in this new design. The detector is of a planar design which also incorporates an antenna placed at the focus of the quasi-optic system. There are several candidates for the detectors; two will be discussed in detail: superconducting tunnel junctions and Si/Ge superlattices.

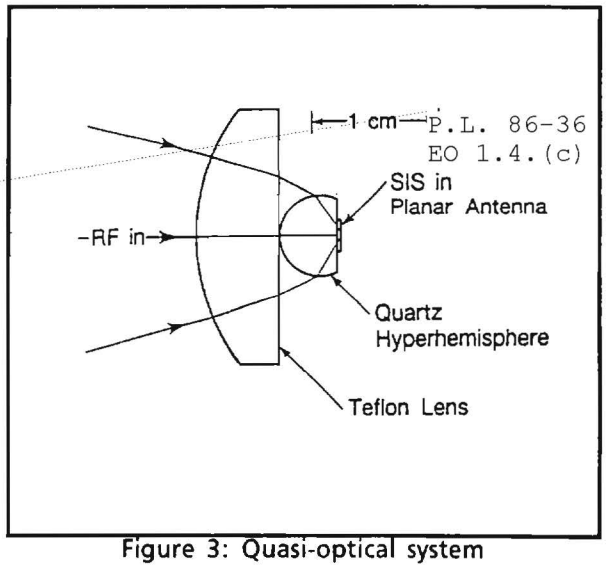



Figure 3: Quasi-optical system

## Detectors

(U) The superconducting detector depends on the quantum mechanical tunneling between two superconductors. This effect is best understood from studies of tunnel junctions consisting of two thin superconducting films separated by a several-nanometer-thick tunnel barrier made from the oxide of one of the metals or from some other insulating material.

(U) Superconducting receivers for infrared and millimeter waves depend on the nonlinear response of the tunneling currents when they are driven by constant and RF voltages. In fact, it has been said that this current-voltage nonlinearity is the strongest known in physics.

(U) Figure 4 shows an experimental I-V curve for a tunnel junction. The time-dependent

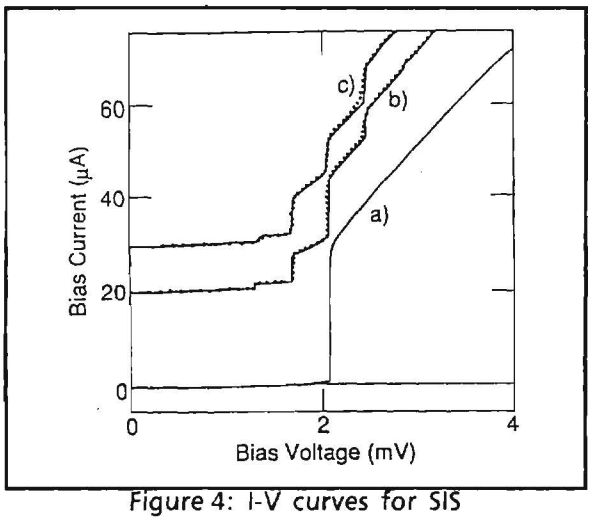



Figure 4: I-V curves for SIS

current I(t) resulting from a voltage V across a tunnel junction can be written :

$$I(t) = I_c \sin\phi + V[G(V) + G'(V)\cos\phi] + C\frac{dV}{dt}$$

The first term on the right is the lossless Josephson-pair tunnel current which depends on the phase difference Φ of the wave function of the two superconductors. The second term VG'(V) is the product of a voltage and a nonlinear coductance called the quasi-particle term. The third term represents an interaction between the first two.

(U) Most infrared and millimeter wave devices can be classified as either Josephson effect or quasi-particle devices depending on which nonlinearity is the important effect. The nonlinearity in quasi-particle conductance G(V) arises from the energy gap of width 2Δ in the density of excited single particle (quasi-particle) states. In an ideal junction at T=0°K, quasi-particle current can only flow when a bias voltage V>2/Δ/e is applied. Because of the singularities in densities of states at the gap edges, the onset of tunneling current at 2Δ/e has infinite slope in superconductivity theory.

(U) Figure 4 shows the discontinuity at 2 mv bias voltage. Though the slope is very steep, there is always some rounding of the corner at 2Δ and some leakage current is apparent at lower voltages. The other curves in Figure 4 involve photon assisted tunneling leading to an enhancement or reduction of quasi-particle current on a voltage-energy scale of the millimeter wave photon.

(U) It is the nonlinear tunnel junction I(V) characteristics that are to be used in this new millimeter wave detector system. These junctions are made by photolithographic techniques together with any tuning structures needed to match impedances. Arrays of junctions can easily be fit into the quasi-optic concept.

*Mixers*

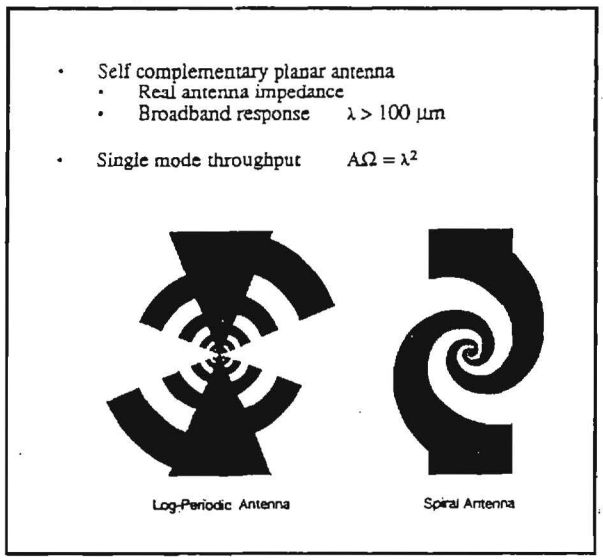
(U) The junction I(V) due to quasi-particles can be used in several ways to make a broadband receiver system. The nonlinearity can be used to make a quasi-particle heterodyne mixer which converts signals from some high RF down to a lower frequency where amplification and signal detection are more convenient. When strongly pumped by a local oscillator at $\omega_{LO}$, the local oscillator frequency, the mixer produces a linear response at the intermediate frequency $\omega_{IF}$ when a small signal is supplied at the signal frequency $\omega_S = \pm m\omega_{LO} + \omega_{IF}$.

(U) The full quantum theory is required to describe mixing in Superconductor-Insulator-Superconducting (SIS) junctions whose I-V curves are sharp on the voltage scale hω/e. When quantum effects are important, the theory predicts net mixer gain and very low noise and because of arguments related to the Heisenburg uncertainty principle, there is a minimum zero-point noise power for mixers of hωB. SIS mixers have been built at 33 GHz and at 90 GHz which have measured noise temperatures within a factor of two of this quantum limit. It should be pointed out here that the requirement of small current flow at voltages below 2Δ/e sets an upper limit of about $T_c/2$ on the operating temperatures that can be used for SIS mixers, where $T_c$ is the critical temperature

Operating temperatures that can be used for SIS mixers, where $T_c$ is the critical temperature where superconductivity vanishes. This cryogenic problem has been eased with the recent availability of NbN junctions with $T_c = 15°K$. At present there is no appropriate high $T_c$ SIS junction technology.

(U) Thin film SIS tunnel junctions can be integrated in a planar configuration with log-periodic or log-spiral antennas which have central lobes and are self-complementary, meaning they have a real impedance of 120 Ω. These antennas, shown in Figure 5, fit nicely into the quasi-optical concept of Figure 3.

Figure 5: Wide Band Antennas




*Direct Detectors*

(U) Another SIS concept for a detector is the direct detector, also called a video, or square law detector. This design uses the nonlinearity of the quasi-particle I-V curve to rectify a coupled RF signal. The current responsivity $S_I$ of such a detector is defined as the induced direct current divided by the available signal power $S_I = \Delta I_{dc}/P_S$. In the quantum theory, the current responsivity is obtained from the small signal limit of the theory of the pumped I-V curve for millimeter wave photons of energy $\hbar\omega$, at the bias point $V_0$:

$$S_I = \frac{e}{\hbar\omega}\left[\frac{I_{dc}(V_0+\hbar\omega/e)-2I_{dc}(V_0)+I_{dc}(V_0-\hbar\omega/e)}{I_{dc}(V_0+\hbar\omega/e)-I_{dc}(V_0-\hbar\omega/e)}\right]$$

(U) The quantity in square brackets above is the second difference of the unpumped I-V curve for the three points $V = V_0$ and $V = V_0 \pm \hbar\omega/e$, divided by the first difference computed at $V = V_0 \pm \hbar\omega/e$. In the classical limit, where the current changes slowly on a scale of $\hbar\omega/e$, the differential approximation gives the usual result for a diode detector:

$$S_I = \frac{1}{2}\left(\frac{d^2I}{d^2V}\right)\Big/\frac{dI}{dV}$$

If the I-V curve is sharp enough that the current rise at $2\Delta$ occurs within the voltage scale $\hbar\omega/e$, and if the bias voltage $V_0$ is just below $2\Delta/e$, then $SI = e/\hbar\omega$. This quantum limit to the responsivity corresponds to one extra tunneling electron for each coupled photon.

(U) Since direct detectors do not preserve phase, there is no quantum limit to the detector noise analogous to that of the mixer. The intrinsic noise of the SIS direct detector is simply the shot noise in the dark current $\langle I \rangle$ at the bias point $V_0$. For a postdetection bandwidth B, the noise equivalent power (NEP) in units of $W/Hz^{1/2}$ of a RF-matched detector is:

$$NEP = \frac{\langle I^2 \rangle^{1/2}}{S_I B^{1/2}} = \frac{\left[2eI_{dc}(V_0)\right]^{1/2}}{S_I}$$

(U) When the signal power is increased, the responsivity of an SIS detector falls; however, the power required to saturate the device is much greater than that of a single junction mixer.

*Experiments with SIS Direct Detectors*

(U) The first experimental test of an SIS direct detector in 1980 showed excellent agreement with the quantum theory. The current rwith the quantum theory. The current responsivity

$S_I$ of 3600 amperes per watt was within a factor of 2 of the quantum limited value e/hω at 36 GHz. These results have been repeated at much higher frequencies recently. The NEP measured at 36 GHz was 2.6 x $10^{-16}$ W/$Hz^{1/2}$ which is essentially the performance of the best millimeter wave astronomical instruments.

(U) Little progress in the sensitivity of SIS direct detectors has been made since the first experiments. However, the limit set by shot noise in the junction current is not fundamental. The fundamental thermally activated leakage current is of order $I \sim \exp(-\Delta/kT)$, which is many orders of magnitude smaller than the extrinsic leakage current that is observed in all SIS junctions. Progress has been slow because relatively few applications of SIS junctions depend in a critical way on leakage current. This situation is now changing. The promise of X-ray detection concepts based on quasi-particle trapping and subsequent tunneling has greatly increased recent activity. Several well funded groups in the US (and in Europe) have announced their intentions of producing junctions with leakage currents reduced by orders of magnitude.

*Integration of Direct Detectors and Antennas*

(U) The SIS direct detector is a fast very broadband RF detector and is the most sensitive detector at millimeter wavelengths for temperatures >1°K. As a planar lithographed structure it is compatible with planar lithographed antennas, coupling structures, filters, etc. Such elements can be fabricated into focal plane arrays by conventional optical lithography. This includes the self-complementary structures discussed above such as log-periodic and log-spiral which have no characteristic length dimension, and therefore have real terminal impedances and extremely wide bandwidths. The impedance of the SIS detector junction, however, has both real and imaginary parts so that a matching network is needed for coupling. This is also shown in Figure 6 along with the equivalent circuit.

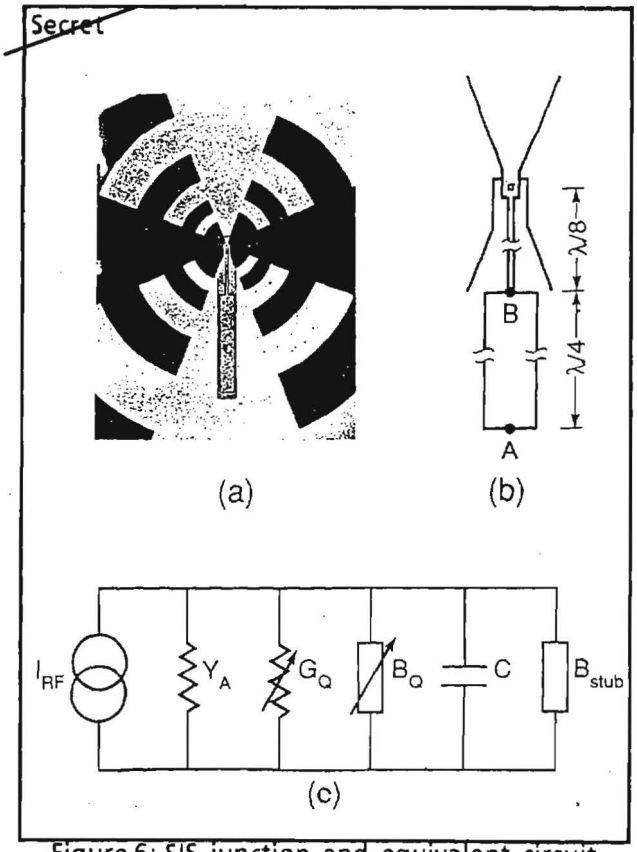


Figure 6: SIS junction and equivalent circuit

(U) The full power of microstrip technology can be applied to the coupling of SIS direct detectors for millimeter wavelengths. The loss in superconducting films is negligible for films at temperatures well below $T_c$; therefore, lossless broad band couplers, band and low pass filters, and even multiplexors can easily be implemented. The possibility also exists to deposit several direct detectors on a single antenna and to couple them via multiplexors and band pass filters. A frequency multiplexed spatial array of detectors can be produced in a way that can meet all the objectives of a search system.

## Novel radiometer for millimeter waves

(U) A novel radiometer configuration, suggested by Prof. Richards, uses one SIS junction pumped with a local oscillator as a heterodyne down

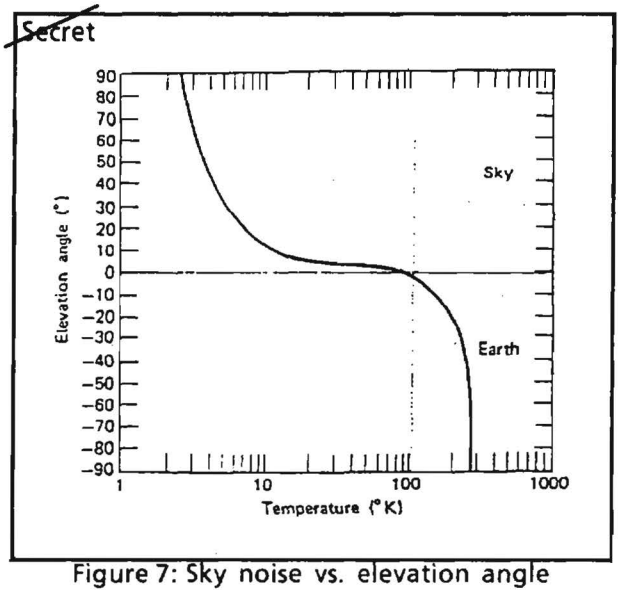



Figure 7: Sky noise vs. elevation angle

converter followed by a second SIS junction, which is used as a millimeter wave photon detector. From one viewpoint, the mixer is a preamplifier for the photon detector. It amplifies the photon arrival rate by the product of its power gain and the frequency down-conversion ratio. The SIS photon detector is used at the relatively low IF frequency where its NEP is better than at the RF frequency. From another viewpoint, this system is a simplified version of a heterodyne radiometer that avoids the need for the IF amplifier because of the conversion gain of the SIS mixer and the excellent performance of the SIS direct detector. This configuration appears to have higher sensitivity than the SIS direct detector while retaining its high speed and operating temperature. It appears to be simple enough that planar integrated arrays or detectors are possible. Prof. Richards may apply for a patent for this novel receiver design that uses the strengths of each part of a tunneling junction operations.

(U) Preliminary steps have been taken to test this receiver concept. The antenna coupled SIS mixer and the SIS direct detector have been fabricated and separately tested. The new element, which has been successfully tested, is an efficient low pass microstrip filter required to connect the mixer to the detector. The overall system is being assembled for a proof of concept.

## FIELDABLE SYSTEMS

(U) With the very low noise wideband receivers available from SIS technology ($T_N < 4°K$), there are several options as to how an actual fieldable system architecture would look. For example, at W band (75-110 GHz), one can see from the data in Figure 2 that present mixer noise alone leads to a temperature of 9000°K (15 db = 9000°K). If the system is constrained to look at the earth at $T \approx 300°K$, then the increase in bandwidth for the same sensitivity would be $9000/300 = 30$.

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

# On Becoming a Well-Rounded Chinese Linguist

(U) One of my lifetime goals is to feel comfortable with the Chinese language and to understand Chinese culture and society. The trouble is that Chinese is difficult to learn, and nobody knows that better than a student of Chinese, even after 30 years. With that in mind, I'd like to present my views on what becoming a well-rounded Chinese linguist means in the SIGINT environment and to offer some suggestions on how to become one.

(U) In these days of high technology, people in all walks of life necessarily have become increasingly specialized. Doctors specialize in various kinds of ailments; lawyers specialize in various kinds of law; mechanics specialize in different makes of car. At NSA we are no less specialized. We have specialists in computers, traffic analysis, collection, and language analysis, just to name a few fields. Furthermore, our specialization extends beyond these major categories; for the SIGINT linguist, the result can be using language that is very narrowly focused.

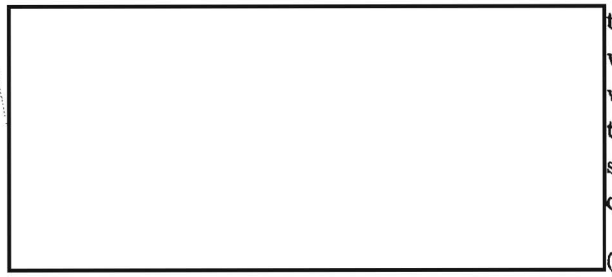
~~(C-CCO)~~ NSAers tend to be so specialized that we are encouraged to diversify in order to broaden our experience. But in the language career field one can specialize in graphic or voice. I did not support the distinction because I believe that a major goal of the language certification process should be to identify "all-round" good linguists, encompassing both graphic and voice, but I will concede that it works well for individual career advancement.

## ON THE TESTING PROCESS

~~(C-CCO)~~ The PQE testing process has evolved from identifying "all-round" professional linguists to identifying linguists whose "professionalism" is somewhat more focused. If you have been around since the Chinese PQE first began, you will remember that in the early days aspirants were required to demonstrate expertise in graphic AND aural Chinese.

~~(C-CCO)~~ To have passed one of the early PQEs was a major accomplishment, and those who did, genuinely could be considered to be good, all-round linguists, not only in a general sense, but also as SIGINT linguists. Furthermore, they reasonably could be expected to be capable of handling any language task with a minimum of training. They certainly met the standard of the day which went something like, "Professional (Chinese) linguists should be able to handle any language task which they might be called upon in the middle of the night to perform without assistance, and produce finished material upon which an end-product report reliably could be based."

P.L. 86-36



~~(FOUO)~~ The point is that the certification process in my opinion identifies and fosters well-rounded linguists only in the sense that they are well-rounded with regard to related-fields and SIGINT disciplines, not in the sense that their specific language expertise is broadly based.

## THE WELL-ROUNDED LINGUIST

(U) Now my idea of an well-rounded linguist doesn't mean that you have to be highly proficient in every aspect of the language, although that's certainly a noble goal to shoot for. I do believe, however, that well-rounded Chinese linguists should have certain basic skills, and those skills are the same for virtually any language, either native or acquired. Namely, they are the abilities to read, write, and speak the language to a sufficient degree that they can function well in-country.

~~(TS-CCO)~~ So how does one go about becoming an well-rounded Chinese linguist? There is no single roadmap on how to do it, but if you haven't already guessed, I have some personal opinions based upon my own experience and those of my colleagues.

(U) First and foremost, of course, is education. That doesn't necessarily mean having a college degree, but it certainly means having a solid background in formal Chinese language training. Many of us acquired this training through intensive instruction at the Yale University Institute of Far Eastern Languages, and later, the former American Embassy School of Chinese Language and Area Studies in Taichung, Taiwan.

(U) Secondly, and perhaps equally important is that one just has to love the language and culture. There has to be a desire to go beyond the minimum necessary to perform the job, and this, I believe, is the key to success in learning beyond the classroom walls. I like to think of linguists who have that desire as "purists" to some extent; we learn because it's there. I don't mean to imply that we consider ourselves scholars, although I'm sure there are some among us who fit into that category.

(U) What I'm really driving at is that learning Chinese has to become an avocation, and wanting to become better at it is just natural. However, as natural as that desire may be, it also takes a fair amount of work.

~~(TS-CCO)~~ Since I'm just a student of Chinese and not a true scholar, I want to share a few of my ideas, which upon reflection helped me, in the hope that others might find them useful.

*Written Chinese*

(U) Let's start with written Chinese. I can't over-emphasize how important learning Chinese characters and reading are. The more characters you know, the easier it is to learn new characters and new character compounds, thereby, increasing yourreading and oral vocabulary. Remembering a word or phrase is easier if you can visualize the characters for it. So, firstly, you should take as many formal reading courses as you can, but don't stop there. Subscribe to—at least, scrounge—original language magazines and or newspapers, and read, read, read. Take the time now and again to mark characters which you don't know in at least one short article, look them up in a dictionary, make and study flashcards (I'm a staunch advocate of flashcards). Translate a short passage occasionally to keep your skills sharp, especially if you don't get that kind of practice on the job. As your vocabulary grows, the reading gets easier and more enjoyable for you are relying less on the dictionary. Also, frequent reading in Chinese helps keep you abreast of what's happening in Chinese society.

(U) As to learning cursive script, take a basic course, learn to write some of the cursive forms, and whenever you have some time, practice using them until they become second nature (you don't have to become extremely proficient to make it useful). When you doodle, doodle on your note pad in Chinese using what you have learned.

Think of word compounds and write the characters a few times just to improve your handwriting and for retention. If you can't recall a character, stop and look it up. Read as much handwritten material as you can get your hands on until you feel fairly proficient at it. Once you are proficient, though you'll get rusty if you don't use it often, you will be able to pick it up fairly quickly when the need arises.

~~(C-CCO)~~ Become familiar enough with the STC book so that you can at least turn to or get close to the correct page for a given radical when you want to look up a character. Even if you don't learn the exact STC groups for lots of characters, simply knowing how to find them rapidly may help you either on the PQE, in solving garbles in STC traffic, and other operational situations where STC is required.

*Aural Comprehension*

(U) For aural comprehension, listen to recorded materials from the radio, or videotape the Chinese language news from Taiwan off the PBS television station in Washington if you can. Take every opportunity to speak Chinese in restaurants, or wherever else you find someone with whom to talk—being ever mindful of security considerations, of course. If you have a good ear, take a tour in transcription to improve your aural comprehension and expand your general knowledge.

## MUSINGS

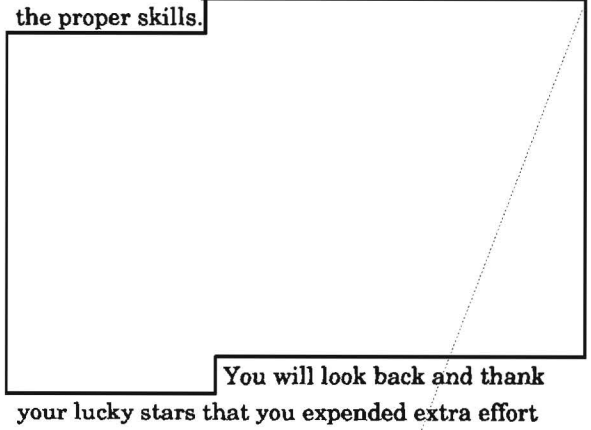
(U) On a more general note, pick up a Chinese-English dictionary from time to time and just browse through it. You'll be surprised sometimes to find the characters for word compounds you know how to say but not necessarily write, not to mention revisiting compounds long since learned and forgotten. Moreover, you can learn some interesting things which you might not otherwise learn from newspapers and other media.

(U) Now, I know that family, friends, outside interests and commitments all compete for the same free time needed for language study such as I have described. Nevertheless, I've found that if you're serious, you can find some time in a busy schedule even if it's not daily. I sometimes think of what my calligraphy teacher in Taiwan once said about practicing writing Chinese characters with a brush pen. When I reached a certain point, he told me that I no longer needed his instruction, and that if I would just take 15 minutes to practice each day, I would do just fine.

(U) Sixteen years later I often wish I had taken his advice. Instead, I let something or other interfere with my practice sessions so my calligraphy never reached the point I had hoped it would. Recently it dawned on me that if in all these years which I have been associated with Chinese language, I had learned just one new character per day, even with interruptions from other activities, I would know all the characters I would ever need to know.

~~(C-CCO)~~ Will the effort to go an extra mile to learn through self-study ever pay off or will it simply be an academic exercise? I believe it does pay off. It goes without saying that you will derive self-satisfaction as your skill with the language expands, but I believe you will find that by increasing your overall language capability your efficiency on the job will improve as well. You'll spend less time consulting dictionaries, increase your ability to scan for significant items, and be able to handle a wider variety of subject matter.

~~(TS-CCO)~~ Moreover, you never know what opportunity may present itself in the future if you have the proper skills.

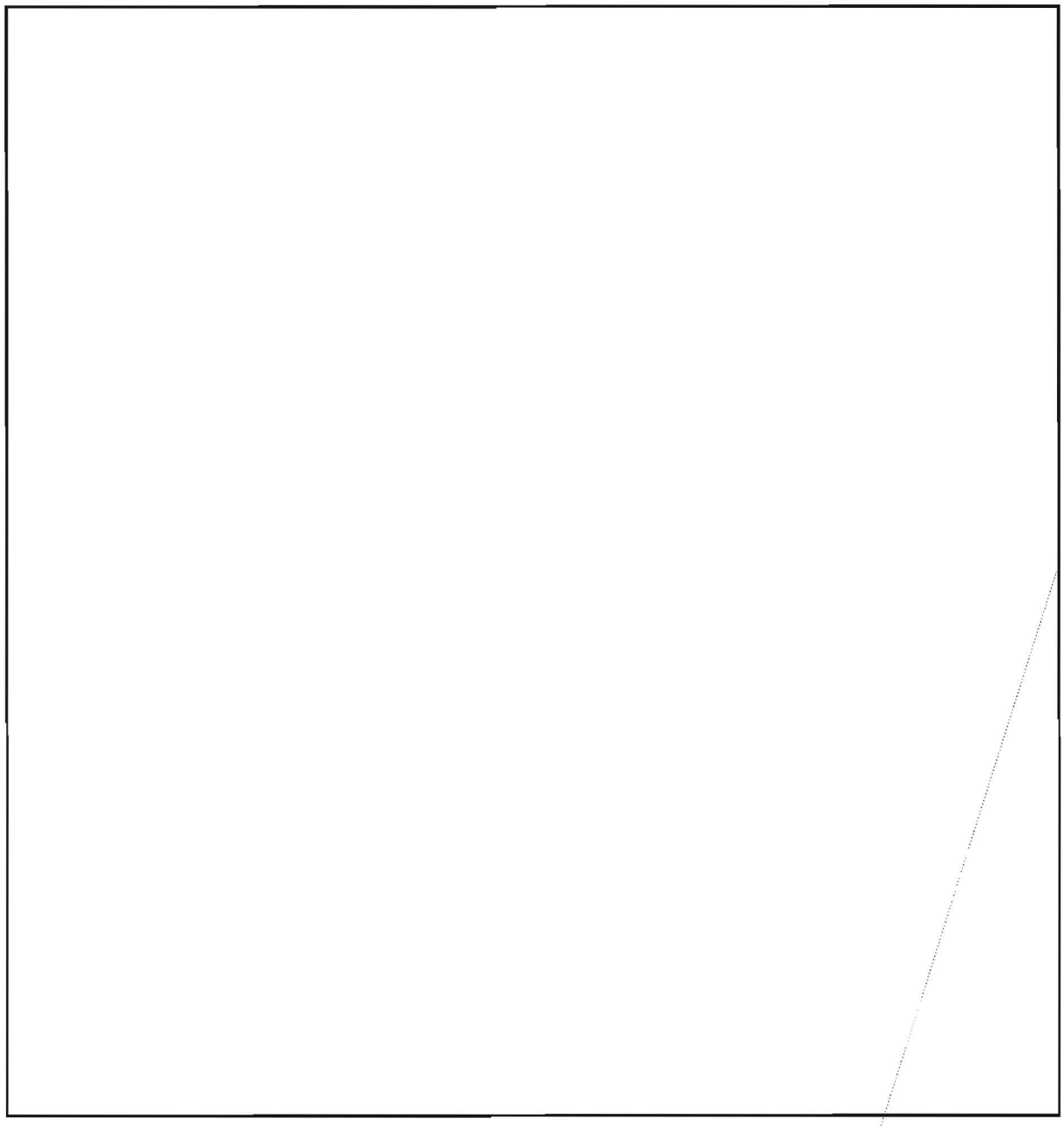


You will look back and thank your lucky stars that you expended extra effort over the years to round out your language and cultural training and experience, and take pride in the accomplishments derived from your efforts to become a well-rounded Chinese linguist.

□

# CRYSCOM Requirements for Data Encryption-Decryption Exchange

[redacted] P13, CRYSCOM Exec P.L. 86-36

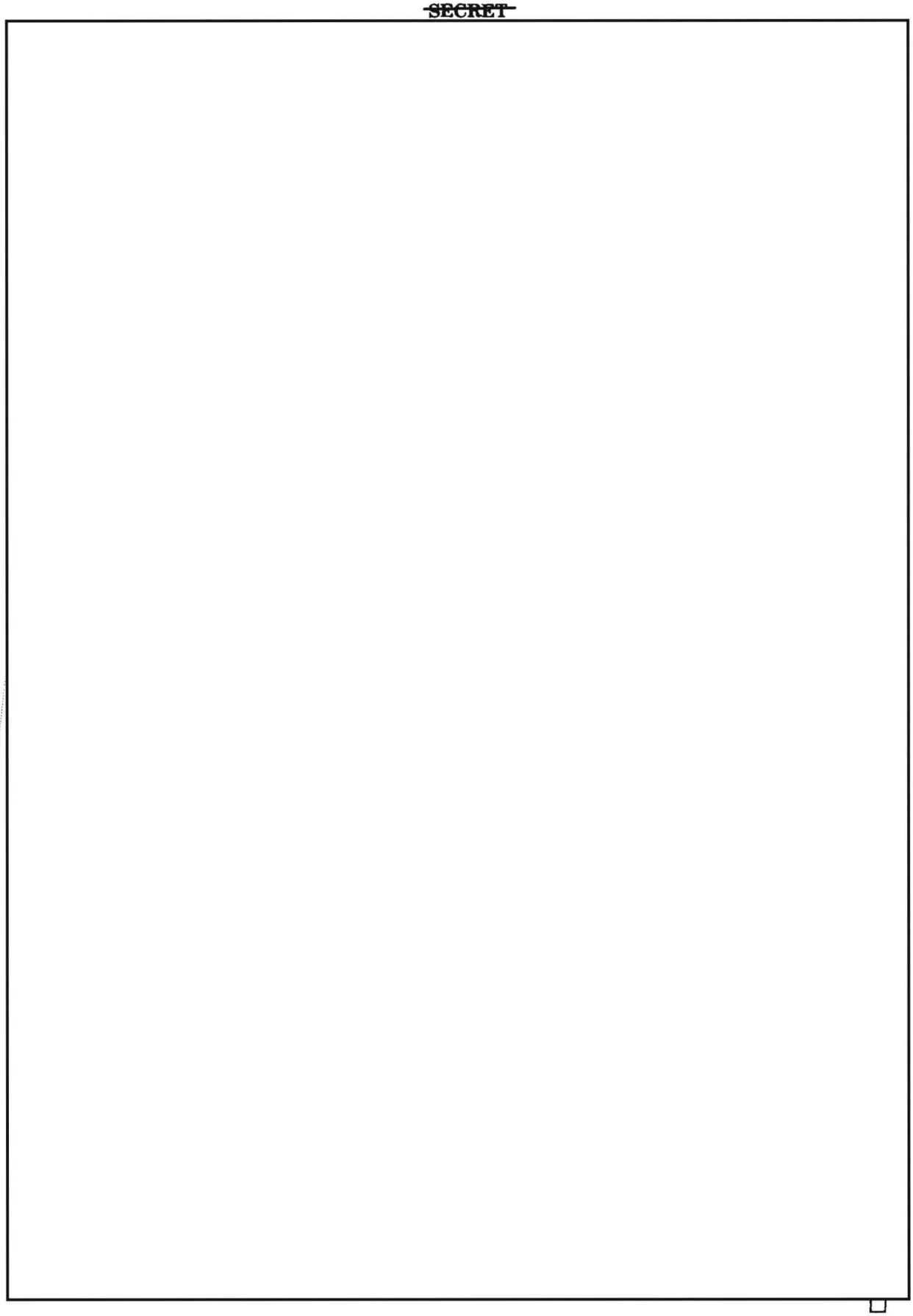




~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

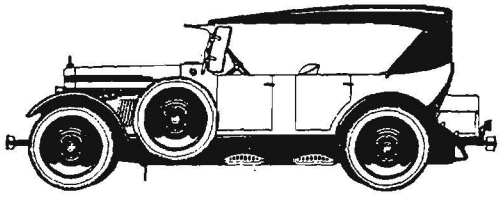
P.L. 86-36
EO 1.4.(c)
P.L. 86-36



## *On the Lighter Side*



# RANK HATH ITS PRIVILEGES



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

[redacted]

Contributed by [redacted]



## *Computer and Information Sciences Institute*

*Special Interest Group on*

[redacted]

If you use data from multiple sources (or support those who do) to track, identify, or evaluate targets, you are doing [redacted] and may benefit from exchanging ideas and software.

**MONTHLY MEETINGS**

Wednesday 25 September 1991 0930 9A135 P.L. 86-36

*Subject*: Geographic Information Systems

*Speaker*: [redacted] T51

Thursday 31 October 1991 0930 9A135

*Subject*: New Multi-media technologies for information dissemination

*Speaker*: [redacted] P05

## Fingertip Intelligence

[redacted] W2

(U) In 1987 W2 set out to expand access to information in order to increase productivity and to improve the quality of its products. We were hoping, at the same time, to make the production process more enjoyable for the analysts by giving them graphical user interface (GUI) and personal computer networking technology. Both are now an integral part of our systems and applications.

~~(FOUO)~~ We have made progress towards the goal of reaching out with our fingertips for intelligence information via computer keyboards; we call this "fingertip intelligence." This means making computers the indispensable tool that people instinctively reach for when they need information, or want to share it. The process calls for:

- a graphical user interface via windows software that provides a what-you-see-is-what-you-get (known as whiz-e-wig, from the initials) view on the monitor;
- running multiple applications (word processing, spreadsheet, graphic editing, etc.) in multiple windows with some background processing;
- scanning in graphics and images to use in publications or in vuegraphs and slides, or to pass on to others over the network;

[redacted]

- running analytic processes on minis and mainframes remotely;
- using an ever-growing number of applications. The possibilities are astounding!

(U) We are taking advantage of the better and faster hardware and software that the computer industry is developing, and also the more appealing features, so that now, people are using computers not because they have to, but because they want to. For example, we have been successful in retrieving data from the VAX, then running an analytic program and outputting the results using Corel Draw graphics, and then importing it all into PowerPoint presentation software or into an Excel spreadsheet, and inserting the results in a reported created in the Word for Windows word processor. And we don't have to close anything down to switch applications.

~~(FOUO)~~ That all these applications can talk to one another has proven the value of our set-up. For example, the new data on target performance we have just entered on the spreadsheet is automatically updated in the report sitting in the word processor. Keeping the documentation in sync, that is, not having to enter newer data manually everywhere it appears, save time and assures accuracy. This is what analysts like.

(U) This process is not limited to the confines of W2, but through networking it can reach the other side of the world! We are now working to integrate intelligence information and to automate procedures to manipulate, assemble and distribute it. We are also trying to improve electronic mail.

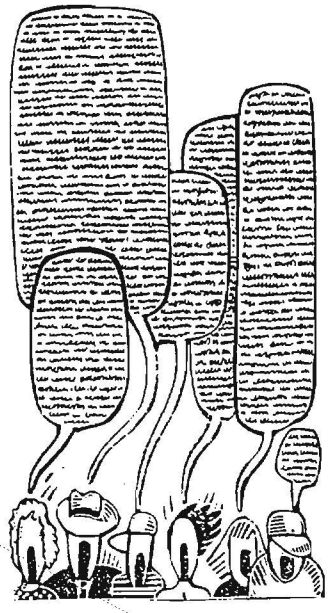


~~(FOUO)~~ It is new technology that has made this possible—the faster machines with more storage and computational capabilities. Now we are poised to bring all the pieces together on our UNIX-based [redacted] workstations as part of the W2 project [redacted] It will incorporate the features described above, a boon to the analysts. But no one division or office can implement this vision alone; we are working diligently with other people in the Agency and outside, too.

(U) If you'd like to pay us a visit, call [redacted] W24, on 968-8963, or me on 968-4236. We'll schedule a demo for you in our dynamic and ever-changing environment.

□

## *Comment on* GISTER



[redacted] W044

~~(FOUO)~~ The article on the GISTER program (CRYPTOLOG, 1st issue 1991 pp 1-7, by [redacted] G52), was intriguing.

[redacted]

(U) The spreadsheets that can perform these tasks are: Lotus 1-2-3 Release 2.2 for IBM machines; Lotus 1-2-3 Release 3.1 for IBM and Unix machines; Wingz and Excel for Macintosh machines. There are ways to enter the GISTER text files from the DOS machines to the Macintosh machines to use these spreadsheets. I would be glad to give a demonstration of the technique to anyone interested.

(U) I am happy that [redacted] a linguist, has written such a useful and impressive program on his own, which could have cost the Agency a tidy sum were it contracted out.

(U) It is also nice to have a publication like CRYPTOLOG handy that allows feedback on the articles written. I would never have known about Jim's work, because I am not involved in language problems, and my technique mentioned above, if useful to anyone, would not have been published.

[redacted]

## *Update on* GISTER

[redacted]

# Using C++ for Compute-Intensive Code:

## Linear Discriminant Analysis

[redacted]
P.L. 86-36

C++ offers advantages besides allowing a programmer the use of the magic phase "object oriented". It encourages writing code that is easier to read and easier to maintain. This article describes a short experiment to measure the run-time penalty paid when using C++ specifically to write readable code.

C++ allows the programmer to define data types and operations on those data types. This can be used to allow the programmer's code to more directly represent the algorithm. I have been looking at some linear discriminant analysis software and decided to use it as a test. The first step of this software creates a covariance matrix from known data. The experiment described here compares the run times of this first step using Microsoft C version 5.1 as the standard C. This result was compared to a C++ version compiled using Turbo C++ version 1.0 and Zortech C++ version 2.1.

An early experiment was done using Rogue Wave's matrix classes for C++. This software was discarded because the increase in run time was incredible and also because the package would not allow the operation matrix = vectorT * vector. The Rogue Wave package is written in the same style as the NIH classes. This style has classes inherit properties of more basic classes which inherit properties of still more basic classes... This approach has advantages, but it causes the software to run slower because of a lot of nested subroutine calls. (Turbo C++ and Zortech C++ both refuse to inline code with loops, and most of the matrix code has loops.)

I wrote a simple matrix class which is used in the results below. The test code reads 500 data vectors from a file, each 90 elements long. These vectors are used one at a time to build the covariance matrix. Most of the time in the entire test program is consumed by the operation:

$$\textbf{covariance\_matrix = covariance matrix + data\_vector}^{T} \textbf{*data\_vector}$$

Two C++ versions were created. One uses code that directly follows this expression, the other uses a subroutine. Except for this one line of code, the two C++ version are the same. The straight C version uses a subroutine. The run times were as follows: (times are in minutes:seconds)

| Type of code used | Microsoft C | Turbo C++ | Zortech C++ |
|---|---|---|---|
| code follows expression | N/A | 1:22 | 1:06 |
| code uses subroutine | 0:18 | 0:18 | 0:18 |

The times are good only to the nearest second or two. The table shows that to achieve the run time of the straight C version, the time-intensive calculation needs to be in a separate subroutine. The results are the kind that make everybody happy. If you don't want to change to C++, they show that C++ has terrible run times. If you want to use C++, they show that C++ doesn't have to be slower than straight C.

Here is the critical line of code used in each of the three versions:

Straight C: ddiadic(quapar,vector,vector,len,len,len);
C++ (fast): quapar.covar_calc(rowvector);
C++ (slow): quapar += (rowvector.transpose()).product(rowvector);

Unfortunately the easiest to read code is also the slowest.

C++ "attaches" the data to the code that processes it. For example, it is very easy to give each matrix a name so that the code can report not only a error, but the matrices involved. This means that if you tried to add two matrices of different sizes together, the code would not just report "Error: matrices are different sizes", but could also tell you which matrices are involved. This makes for very friendly code. The straight C code used for the test follows the traditional math programming style and doesn't check for any errors.

## WHY THE C++ CODE IS SLOWER

I believe that the creation and destruction of scratch variables is the major reason that the C++ code runs slower. Look again at the critical calculation:

**covariance_matrix = covariance_matrix + data_vectorT * data_vector**

The C++ expression causes the following steps to be done:

1. Create a data vector and put data_vector$^T$ into it.
2. Create a matrix and put data_vector$^T$ * data_vector into it
3. Destroy data vector containing data_vector$^T$
4. Add matrix from step #3 to covariance_matrix
5. Destroy matrix containing data_vector$^T$ * data_vector

Each time the line is executed, two intermediate values are created, used, and destroyed. By replacing the line with a call to a subroutine, the need for the intermediate values is eliminated. It would be interesting to see how much time could be saved by using some sort of cache for intermediate data elements. That is, instead of destroying a intermediate data element, put it aside in case you will need it the next time through the loop.

## CONCLUSION: USE C++

The two major steps of real time programming are; first make the code run right and only then make it run fast. C++ has significant advantages for writing code that runs right and as this experiment shows, C++ can run fast.

## WHY IS ZORTECH C++ FASTER THAN THE TURBO C++?

The test code had a verbose option that would print out each time a data element was created or destroyed. For example, the critical calculation caused the following lines to be printed when the Zortech C++ version was run:

```
column_vector (rowvector transpose )(90,1) created
matrix ((rowvector transpose ) matmul rowvector)(90,90) created
matrix ((rowvector transpose ) matmul rowvector): deleting data, destroyed
column_vector (rowvector transpose ): deleting data, destroyed
```

The format of the line is type of matrix, the matrix's name in parenthesis, the size if created, and a comment saying created or deleted. An intermediate data element takes the name of the original element with the name of the operation added. For example, the line:

```
column_vector (rowvector transpose )(90,1) created
```

says that a column vector with name "rowvector transpose" with size 90,1 was created.

Here is the corresponding output when the Turbo C++ version is run:

```
column_vector (rowvector transpose )(90,1) created
column_vector (Copy of (rowvector transpose ))(90,1) created
column_vector (rowvector transpose ): deleting data, destroyed
matrix ((Copy of (rowvector transpose )) matmul rowvector)(90,90) created
matrix (Copy of ((Copy of (rowvector transpose )) matmul rowvector))(90,90) created
matrix ((Copy of (rowvector transpose )) matmul rowvector): deleting data, destroyed
matrix (Copy of ((Copy of (rowvector transpose )) matmul rowvector)): deleting data,
      destroyed
column_vector (Copy of (rowvector transpose )): deleting data, destroyed
row_vector (Copy of (Row 20 of means)): deleting data, destroyed
```

Notice all the "Copy of . . . " lines generated. Turbo C++ is creating copies of matrices that the Zortech code didn't need. Why are all these extra copies made?

The difference between the two is caused by how the compiler handles return values. For example, look at this subroutine:

```
Matrix dummy(void)
      {
      Matrix X();    // X is an automatic variable
      X = ...        // Put a value in X
      return(X);     // Return X
      }
```

The above subroutine returns a variable ("X") that is automatic and goes out of scope when the subroutine returns. Turbo C++ creates a copy of X and destroys the original when the subroutine returns. Zortech C++ postpones the destruction of X until the subroutine's return value is no longer needed. At least one of the reasons that Turbo C++ runs slower is because of all the extra copies it makes.

# Book Review

*Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943*, David Kahn, Houghton Mifflin Company, Boston, 1991.

*Reviewed by: Vera Filby, D9*

Many NSA people have read or know of David Kahn's first book, *The Codebreakers*, a massive and erudite world history of cryptology. With this background of knowledge, an Oxford doctorate in history, and the acquaintance of many who remember the events recounted, Dr. Kahn was well equipped to tell the story of the German naval Enigma cipher machine and the struggle to turn it into a weapon against the U-boats.

Readers who have followed the cryptologic history of the Battle of the Atlantic will find much in this book that is familiar, but they will enjoy it all the more for that reason and will appreciate it for its new information, its entertaining style, and its novel approach. The theme is the recovery of Enigma materials from U-boats through circumstance of war and from ships by chance or by planned seizure.

Information encrypted in naval Enigma was desperately needed in Britain's deadly battle against the U-boats, and the struggle to break the system was long and hard. Veterans of that effort were among the more than 70 people interviewed and 20 reached through correspondence - German, Polish, French, British, and American. They included cryptanalysts, U-boat and ship captains and crew members, intelligence officers, radiomen, and others.

Among them were Gustave Bertrand, wartime head of French espionage, Norman Denning, head of German intelligence in the Operations Intelligence Centre, and Harry Hinsley, who as a Cambridge history student joined the G.C.&C.S. (now GCHQ) at Bletchley Park, taught himself traffic analysis and soon demonstrated its operational intelligence value. He became a naval intelligence analyst, and many years later was chief author of the UK Government's official *British Intelligence in the Second World War*. Dr. Kahn is reputed to be a skillful and persistent interviewer, with a knack of asking questions to which he already knows the answer or part of it, perhaps in the hope of confirming it or eliciting more information.

Other sources, besides many of the books and articles published on the subjects covered, included ships' logs, reports, memoranda, and personal papers in German, British, and American libraries and archives.

Dr.Kahn's accounts of the ship captures are full of color, excitement, and suspense. He is a great teller of sea stories. The parallel story of the Enigma machine and its ramifications he treats with thoroughness and clarity, beginning with the day, 15 April 1918, when the inventor, Arthur Scherbius, offered his cipher machine to the Imperial German Navy, up to the end, when the Enigma decrypts were no longer needed. He recounts vividly the Polish, French, British and American experience, with special attention to the Polish story. He describes in detail the construction and workings of the machine, the means and methods of atttack, and associated codes and ciphers, with the focus always on the naval Enigma. Luftwaffe Enigma was first broken on 22 May 1940 and thereafter air traffic was read regularly. But the naval remained resistant. Naval Enigma was more complex and naval communications more disciplined, and only limited and temporary successes were achieved until December 1942.

With the Enigma buttoned up, the analysts at Bletchley worked on and broke lower level systems. One of these was the Dockyard Cipher, which was used for messages to and from shore stations and patrol boats, minesweepers, auxiliaries, and other vessels. In time the analysts discovered that messages sent in Dockyard were sometimes sent also in Enigma to ships equipped with Enigma, thus producing cribs, which they called "kisses."

## GIFTS FROM THE SEA

A bit of help for the analysts in Bletchley's Hut 8, the naval cryptanalysis section, came from an unexpected source early in 1940 when the minesweeper *H.M.S. Gleaner* encountered and attacked the German U-boat U-33 at the entrance to the Firth of Clyde 12 February. The skipper of the damaged submarine decided to surface and make a run for it. Enigma parts were distributed among crew members to be dropped into the sea if they had to abandon the submarine. The *Gleaner* spotted the U-33 and continued the attack. In the danger and confusion, one seaman forgot to sink his piece–a wired rotor.

On 26 April a British destroyer returning from Norway stopped and boarded a trawler identified as Dutch and named *Polares*. A crew member threw two canvas bags overboard, but the boarding party was able to capture one of them. When the contents arrived at Bletchley they were found to contain Enigma keys for four days in April.

Nearly a year passed before the struggling cryptanalysts received another gift from the sea in the form of key tables for February. In March 1941 a destroyer accompanying troop ships carrying commandos for a raid on German-occupied Norway encountered an armed whaling trawler, the *Krebs,* in the Lofoten Islands. Documents retrieved from the ship after it was fired on and destroyed included gridded charts, the February Enigma keys, rotor settings, and the plugboard setting. With their help, the Hut 8 analysts decrypted messages which included weather reports and information on the movements of weather ships to and from fixed areas where they were stationed for periods of several months. The analysts were soon getting kisses from weather messages.

## WEATHER

Germany could not do without weather information from northern waters. It was essential for current data and forecasts for all purposes but especially to support air operations against England. Only ships at sea could provide a steady flow of observations, so fishing vessels were used to serve as weather stations. Even U-boats were pressed into service. To deny the data to the British, reports had to be encrypted, and the system used to do it was the Enigma.

Weatherbirds will appreciate the significance of this. Not many NSAers know about the Weatherbirds–an informal club of SIGINT weather analysts. Weather is usually a low priority target for SIGINT–until there is a crisis; then everybody wants the weather support. SIGINT weather can provide identifications and locations, contribute to traffic analysis, give tipoffs to related activity, reveal information about the entities it serves, reflect such events as airfield openings and closings, and indicate future events. In *Seizing the Enigma* Weatherbirds will learn how the Enigma encipherment of weather led to its own undoing.

Losses of ships carrying war materiel, food, and other necessities of survival were increasing, and help from Bletchley was urgently needed. Harry Hinsley, studying the weather messages along with his other traffic, had a stunning idea. Why not go after a weather ship? His suggestion went through channels, and the *Muenchen*, which was about to sail to a grid square northeast of Iceland, was selected. A task of force of destroyers located the ship on 7 May and shelled it. Before abandoning ship, the radioman, who had been transmitting a weather report, gathered up the Enigma machine, the current keys, and other materials, put them into a lead-weighted bag, and threw them overboard. But the boarding party did succeed in collecting some documents. Among them Bletchley identified the Short Weather Cipher, Enigma settings, and the June keys. The Short Weather system reduced synoptic weather ele-

ments to single letters which were then enciphered in Enigma and could be transmitted in 15-20 seconds.

Recoveries from the U-110, captured only two days after the seizure of the *Muenchen*, and from the targeted fishing vessel *Lauenburg* on 28 June brought gold to Bletchley–keys, an indicator book and enciphering instructions, the U-Boat Short Signals Book, machine instructions, settings, and the July home waters keys.

In contemplating the damage the encipherment of weather brought on the Germans, one cannot help wondering why they risked their most powerful system for it. Why not some other cipher? The objective was to secure the weather information, but more important was concealing the fact that the information was weather, specifically weather from ships at sea. But why put Enigma in double jeopardy, by using it for that purpose and sending it out on small vessels vulnerable to capture?

There is another mystery. Short-form Enigma weather reports from U-boats were decrypted and sent to the weather central in Germany. Selected reports were reenciphered in a weather system and broadcast to ships at sea and shore stations. How could the COMSEC authorities have allowed this to happen? The only answer is that the Germans had absolute faith in the impenetrability of Enigma. They did conduct investigations when compromises were suspected, but the findings always concluded that the source could not have been Enigma.

### THE BATTLE OF THE ATLANTIC

As Dr. Kahn notes, the Battle of the Atlantic was the only battle that lasted from the first day of the war to the last. Thoughout much of that time, the numbers of ships lost to U-boats reflected the status of solution of enciphered commuications on both sides. The picture could be modified by other influences–improved DF techniques, for example–but the effect was always there, sometimes dramatically. Sinkings in the last half of 1941 amounted to 600,000 tons. In the same period of 1942, losses reached 2,600,000. The Germans broke Naval Cypher No. 3 and read much of the naval traffic throughout 1942. Naval Cypher No. 5 replaced Nos. 3 and 4 in June 1943, and from that point on, British naval was denied to them. Meanwhile, the British lost the Enigma when the M4 model was introduced on 1 Februry 1942.

Salvation came from the destruction of the U-559 by the destroyer *Petard* in the eastern Mediterranean in October. Men from the *Petard* boarded the sinking boat, with bodies floating all around them. They succeeded in getting many documents out, but an officer and a seaman went down with the U-boat. The documents they had given their lives for were current editions of the Short Signal Book and the Short Weather Cipher.

The sequence of events that followed their arrival at Bletchley led to a break into the Atlantic U-boat key SHARK in December. By January and February 1943 sinkings were reduced to half of the losses in the previous two months. In June 1944 an American task force captured the U-505 and retrieved from it the grid position Adressbuch. This filled the last gap, and thereafter the Allies read naval Enigma currently.

To complete the picture, Dr. Kahn devotes a chapter to the American role in the naval Enigma. Once coordination was achieved, the naval analysts at Nebraska Avenue worked closely with those in Hut 8, exchanging cribs and recoveries.

In a final summation, Dr. Kahn writes that ULTRA's greatest gift was that "it saved lives. Not only British and American lives, but German lives as well. That is the debt the world owes to Bletchley codebreakers; that is the crowning human value of their triumphs."

## BULLETIN BOARD

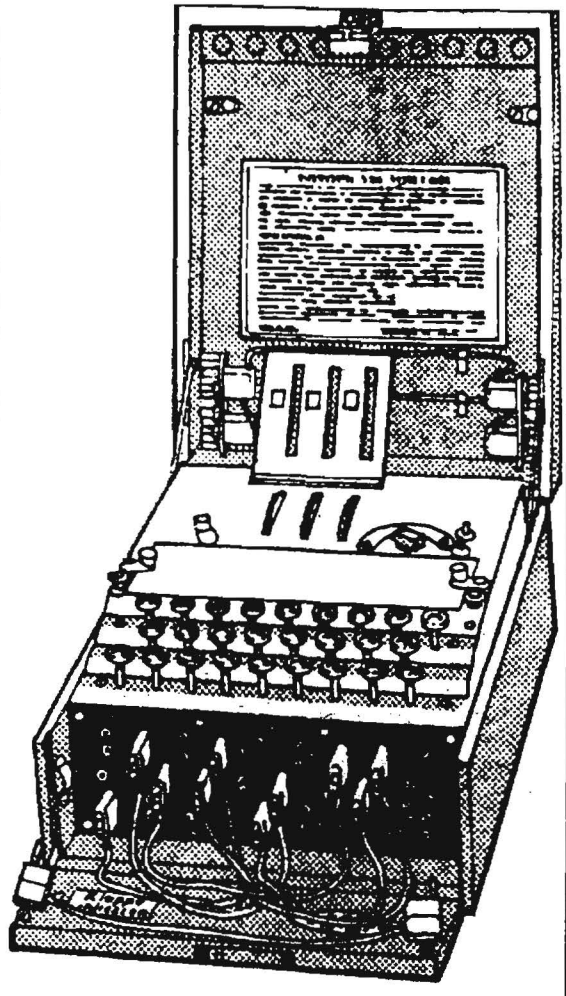
**Will the person who borrowed *Editing Your Newsletter* in looseleaf format kindly return it to the CRYPTOLOG office, Ops-1, 2N018. No questions asked.**

# On the Enigma



ENIGMA, an off-line cipher machine, was the first wired wheel machine to be used to any significant extent. It appeared in Germany about 1925 as a commercial offering, at which time it had three wheels and a reflector (Umkehrwalze). In 1926 the German Army introduced a version which had different wirings, a different reflector, and a new feature, the plug board (Stecker-verbindung, or "stecker" between the wheels and the input-out functions. The Poles attacked the German Army usage and made limited progress by discovering that some from of ENIGMA was being used and that the first six letters of each message were probably indicators. In October 1931, the French intelligence services developed a source within the Cipher Bureau of the German Ministry of Defense who supplied them with copies of code clerks' instructions for ENIGMA and, subsequently at regular intervals, with copies of daily key lists (but no wirings).

The French Cipher Service looked at these and immediately declared the machine impossible to solve. French intelligence then obtained permission to give the information to France's allies and to suggest a common attack on the problem. GC & CS (Government Code and Cypher School, the predecessor of GCHQ) was given first chance, but they "Filed their copies of the documents" and did not respond to the offer of cooperation. (Gordon Welchman, however, believes the British had more effort against ENIGMA before the war than they indicated to the French.) The French then approached the Poles, who accepted with enthusiasm and promised to share results of their work. However, all cryptanalytic efforts failed. At that point, 1 September 1932, those in charge of Polish intelligence brought in three mathematicians, Marian Rejewski, Henryk Zygalski, and Jerzy Rozycki. In the middle of October, 1932, Rejewski was put to work on ENIGMA and, using information in the documents from the French which

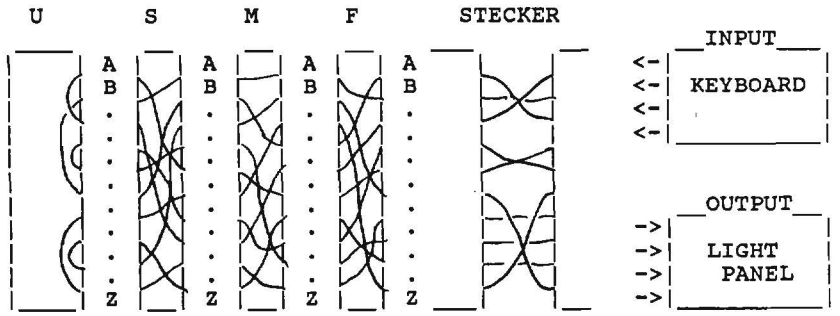


**Above: the Enigma machine, a mechanical device for coding invented by the German Arthur Scherbius. Its keyboard is similar to a typewriter, but the letters strike rotary disks that choose substitute letters at random to create encoded messages.**

showed how the Grundstellung indicator system worked, he was able to in about a month to develop a theoretical method for recovering wheel wirings based on the fact that message settings (of the three wheels) were enciphered twice to produce the six-letter indicator sent at the beginning a a message (this was the Grundstellung indicator system).

Unfortunately, the amount of work needed to carry out the calculations was prohibitive (and might be prohibitive even with modern computers). Then Rejewski was given two more documents that had been procured by France, these

The ENIGMA as it was at that time looked like this:




containing two monthly schedules of daily settings (Wheel orders, Grundstellung wheel settings used for enciphering message setting, and plug board connections). At this time, wheel orders were being changed only every three months, but by luck the two months provided by the German source fell in two different quarters. All this information permitted the theory to be simplified sufficiently for Rejewski to recover wirings of the three wheels and reflector by the end of December 1932.

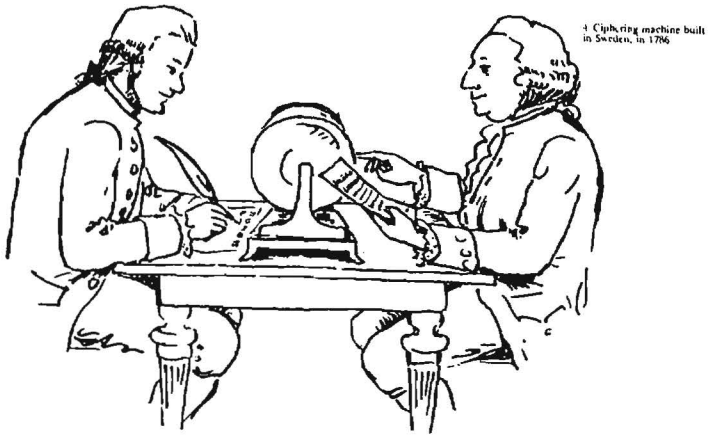
There were three 26-point wired wheels which could be inserted into the machine in any order (but not backwards). There was a reflector (Umkehrwalze) which had input-output contacts on only one side that were connected to each other in pairs. Each wheel had one notch on it which controlled the stepping of the wheels. The fast wheel, F, advanced one position for each encipherment of a letter; the medium wheel M, did not advance for an encipherment unless either F advanced off of its notch or unless M itself was at its own notch, in either of which events M advanced on position. The slow wheel S, did not advance for encipherment unless M advanced off of its notch, in which case S advanced on position. The reflector, U did not step during the encipherment of a message (and in fact was not settable). The stecker between the "maze" and the input-output mechanisms could be changed by the operator but remained constant during the encipherment of a message; it consisted at this time of 14 points connected straight through and 12 points exchanged in pairs.

In addition to all these variable, the alphabet ring on each wheel (by which the wheel could be set in a specified position at the beginning of a message) was rotatable relative to the core of the wheel and could be put at any one of 26 offsets. Thus, setting the wheels so that the same letters appeared at the bench marks would produced different settings of the wirings themselves if the alphabet ring offsets (Ringstellung) were different. Once all these variable elements were appropriately set up, the code clerk typed each plain text letter in turn and, for each one, wrote down as cipher text the letter which lit up. Depressing the key also caused the wheels to advance appropriately.

In July 1939, the British and French were informed of the Poles' success on ENIGMA and GC & CS accelerated its own partly successful work against it. ENIGMA was used by the German Army, Air Force, and Navy, among other government elements. Although rather heavy, it was small enough for one person to carry and it operated from batteries, so it was suitable for field use. The Germans continually improved their usage of ENIGMA by changing wheel and reflector wirings a number of times; by increasing the number of available wheels from which daily wheel orders could be selected (they went from three to five to eight in the course of time); bu changing the indicator system several times; by increasing the number of steckered letters from 12 to 20; by devising the number of steckered letters from 12 to 20; and by devising nonreciprocal steckers.

□

*David W. Gaddy, D9*




# *Breaking into Our Past: Enigmas of Another Kind*

Cryptology embraces two ancient practices—concealing the meaning of one's communications from unintended eyes, and deducing the hidden meaning of the communications of others. One we term cryptography; the other, cryptanalysis: "code making" and "code breaking." Cryptanalysis, we say, yields communications intelligence, COMINT. But COMINT is both a product and a process.

Historically, cryptanalysis was a matter of circumstance, of the chance capture or interception of a cryptogram. No thought was given to organizing systematic efforts to capture cryptograms—the communication technology would not prompt thought along those lines or support an effort. (How many "daily hours of cover" would one devote to capturing enemy couriers?) But the technology changed in the 1860s in America—not with Morse's telegraph, which required a physical tap—but with a system of visual signals invented by an army surgeon, Albert James Myer. The Myer system (a binary code, by the way) made battlefield telecommunication practical. It also introduced a communication technology susceptible to interception. The rudiments of cryptology are evident in the American Civil War.

A little more than a decade after that war, the telephone came on the scene, and it was enthusiastically adopted by our army signal corps. But, from the standpoint of cryptology, this was little different from Morse's electromagnetic telegraph—interception required physical contact with the wire involved. The invention of wireless communication near the turn of the century changed everything. Technology would now support an organized, systematic COMINT effort, even as it was demanding a new look at security.

Modern cryptology is built on the foundation of the First World War, when military use of wireless first became widespread. The advanced nations maintained some interest in the subject during the 1920s and '30s, albeit in varying degrees. For the United States, this was the era of Herbert Yardley and his *American Black Chamber* and William F. Friedman, who created a scientific basis for cryptology.

But it is to World War II that we look when we think about the origins of modern cryptology, and for good reason: cryptology continued from "hot war" into "cold war" without dropping a beat. In fact, it thrived. Now a half century separates us from the exploitation of the German Enigma and the Japanese Type 97 machine Americans called PURPLE. That generation has largely passed from the scene. Sons and even grandsons (yes,

and daughters and granddaughters) have displaced them.

The passing of the generation that established modern cryptology has removed from our ranks the pioneers in what we now consider our profession. We have lost some of the lore, some of the technical knowledge, and some of the enthusiasm that they possessed, when ciphers were broken by individuals, and when each accomplishment broke new ground. The process has become less individualistic and more mechanical. Mathematicians and scientists have replaced students of the humanities. Sometimes it is difficult for newcomers to understand their role in the greater scheme that engulfs them.

In the fall of 1989, we moved to remedy this by putting greater emphasis on recalling to memory the past accomplishments and the pioneers who laid down the trail we follow. The Center for Cryptologic History is an effort to rejuvenate our history program and to make it relevant to the needs of a new generation of young professionals and modern decision-makers. The scope of our inquiry extends from a better understanding of the sweep of American cryptologic history and its European antecedents, all the way to the lessons of DESERT STORM.

While the recent subject may be of more pressing interest, our present purpose is to share a puzzle from the more distant past. It is somewhat like the "missing link" to anthropologists: in our case, it is an unidentified cipher device that may extend our knowledge of our craft.

**The Cylinder-Cipher Enigma**

In 1890, a disgruntled French cryptographer revealed a device he had been unsuccessful in persuading his own government to adopt. The Bazeries "cylinder-cipher" comprised 20 disks or wheels—rotors, one might say—arranged in a specified order on a shaft or axle. The letters of the alphabet were placed around the rim of the disks, scrambled. The cryptography was that of polyalphabetic substitution, an improvement on the familiar Vigenere in that the alphabets were mixed. To encipher, one aligned the disks to spell the plain text, then selected and transmitted as his cipher text any other line of mixed letters. On the receiving end, one set up the cipher text, then simply turned the cylinder until plain text was revealed.

This concept, and virtually the identical device, was adopted by the United States Army Signal Corps and introduced in 1922 as its M94. That same year a scholar (and former World War I cryptologist) who was working among the papers of Thomas Jefferson in our Library of Congress discovered in Jefferson's own hand two papers describing the manufacture of just such a cipher device, called a "wheel cipher" by Jefferson. Since that time Jefferson has been considered the inventor of this type of cipher device. He is so identified in the most recent book on the subject, Silvio Bedini's *Thomas Jefferson, Statesman of Science*, published in 1990. Bazeries, it was assumed, independently invented the same device; the Signal Corps copied him, unaware of the achievement of its esteemed countryman. Bedini followed the directions and made a copy. But now the plot thickens, as they say in detective stories.

A few years ago there appeared at a sale in the Washington area a device of this very type. It was suspected of being of American Civil War origin, perhaps Confederate. The price was right; we bought it. Upon examination, it was evident that pieces were missing, including several of the disks. Some disks had been removed and replaced in reverse order. Letters were obscure or even obliterated altogether. But nothing about the device suggested Confederate use. On the contrary, accented letters showed that it was intended for the French language. Superficial appearance suggested that it was older than the war of the 1860s, perhaps early 19th Century or even late 18th.

The former owner was from West Virginia, an area that was part of Jefferson's home state during his lifetime. Could this be the source of Jefferson's knowledge of such a cipher machine? His undated description is not necessarily evidence of original thinking. But how did the device come into American hands, and when? It retains 35 of a possible 40 disks, each bearing 42 mixed

letters, digits or punctuation. Would this larger, more involved version be earlier or later than the Jefferson-Bazeries-Signal Corps concept? We have no answer as yet. The mystery remains. But the mystery deepens with another bizarre parallel.

Some years back another former cryptologist was working among the historical archives of his own nation. He, too, discovered a description of a cylinder-cipher, similar in principle to the one we are studying. The researcher was Sven Wasstrom of Sweden. The documentation he had found was dated 1786, well before the earliest date postulated for Jefferson's description. It described the invention (dare we say?) of a Baron Fridric Gripenstierna, offered to King Gustav III. Working with Boris Hagelin's famed CRYPTO AG, Wasstrom assisted in making up a copy of the 18th Century device.

And there our story ends for the moment. It is an amusing curiosity, a diversion. Or is it more than that? In 1865 the United States Army came into possession of a type of cylinder-cipher used by the army that most threatened the very existence of the United States, the Confederate States Army. It was simply a mechanical means of using the conventional, straight-sequence, 26x26 Vigenere square or tableau. But suppose each column had been separated by sawing through the cylinder. Suppose the alphabets to have been scrambled, instead of in direct sequence.

Now come forward in time: apply electricity to this manual device. The disks become rotors, the heart of mid-Twentieth Century cipher machines, the embodiment of another Enigma. Whether for the old cryppie or the youngest member of the new generation, discoveries of this nature illumine the still obscure background of our technical history. They hint at continuity "behind the scenes," perhaps even at international cooperation—or espionage. At a minimum they give us a fuller appreciation of our heritage. We believe that such knowledge enriches our profession and justifies the modest attention we devote to the subject.

□

## *Notice to Subscribers*

Distribution for this issue reflects changes received by COB 30 August 1991.


To change your mailing address, please write your name, old organization and building, new organization and building, on a piece of paper, put it in a **shotgun—not one-time**—envelope, and mail it to:

DISTRIBUTION, CRYPTOLOG, P1 NORTH

*or send it by electronic mail:*

PLATFORM: cryptlg @ 1barlc05

CLOVER: cryptlg @ bloomfield

**Please do not phone about your subscription** because:

- After every issue there are over 300 changes to the distribution, about 300 in the first two weeks after CRYPTOLOG hits the streets.

- The distribution list is kept on line on a shared computer in another room.

Editorial

# *Dump Core! Recycle!*

Now is the time to come to the aid of the future.

Just about every analyst has a stash of technical papers, working aids and other materials on favorite projects worked long ago that have been saved "just in case" or that "really should be documented," as people tell their friends, "some day when there's time."

There's no better time than the present, with reorganizations in the air and rumors of an early out.

Getting started is the hard part, for it's a formidable prospect to document a project years later, and it's tempting to put it off to a time when you'll feel up to it.

Maybe you should try for Plan B: instead of trying to document the entire project, organize your materials as a resource for future research. All you have to do is put the papers (or mag tapes, or whatever) together neatly. (Those red accordian envelopes are just the thing.) Write a "Scope and Content" paper—it could be hand-written on one sheet of paper. This means indicating:

what's it all about
why it was important, or proved not to be
what years the materials cover
what your role was
any details you can recall. (It's all right to say you don't know!)
other comments
your name, present organization, date.

There! That's not so hard! Now set it aside and take out your persumm. Using it as an outline, dump core! Tell all you know about those projects—opening and closing field stations, setting up the very first whatever . . . What it was like back in the olden days . . . Add those comments to the surviving papers.

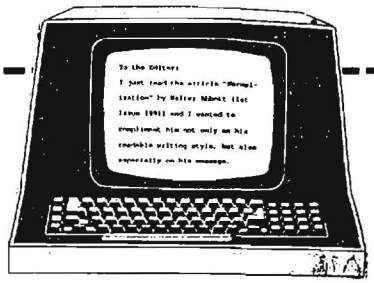
What about those general working aids and monographs that do not belong to any one project: MILCRYPT III, a monograph in the Blue Ribbon Series, a "How to" ITN that's still valid . . . too good to throw away though it's coffee-stained, maybe it should go somewhere . . . but maybe it's filed somewhere? Don't bet on it! Recycle!

*Send cryptanalytic materials to:*

SAB 2, Door 22, T5411 [redacted] P.L. 86-36

*Send all other materials to:*

SAB 2, Door 22, T5411, NSA Archives



To the Editor:

I just read the article "Normalization" by [redacted] P.L. 86-36 [1st Issue 1991] and I wanted to compliment him not only on his readable writing style, but also especially on his message.

I have been dealing with several third party organizations for years and have even visited one of them for a short TDY. Most of these relationships have existed since long before I came on board at the Agency, and I've always dealt with them from this side of the ocean, so I guess I have considered them as bureaucratic construction, a "given" that was to be dealt with in the context of today's world. I've never really given a lot of thought to the reasons, beyond the obvious monetary ones, that motivated our third party partners to enter into the relationship in the first place.

In the age of the computerization of everything to the point where all some of us is push buttons all day long, it's refreshing to be reminded that our relationships with our partners is really very personal sometimes.

[redacted] *A3204*



P.L. 86-36

# CRYPTOLOG

## *Editorial Policy*

CRYPTOLOG is a forum for the informal exchange of information by the analytic workforce. Criteria for publication are: that in the opinion of the reviewers, readers will find the article useful or interesting; that the facts are accurate; that the terminology is correct and appropriate to the discipline. Articles may be classified up to and including TSC.

Technical articles are preferred over non-technical; classified over unclassified; shorter articles over longer.

Comments and letters are solicited. We invite readers to contribute conference reports and reviews of books, articles, software and hardware that pertain to our mission or to any of our disciplines. Humor is welcome, too.

If you are a new author, please request "Guidelines for CRYPTOLOG Authors."

## *How to Submit your Article*

Back in the days when CRYPTOLOG was prepared on the then state-of-the-art, a Selectric typewriter, an article might be dashed off on the back of a used lunch bag. But now we're into automation. We appreciate it when authors are, too.

> *N.B.* If the following instructions are a mystery to you, please call upon your local ADP support for enlightenment. As each organization has its own policies and as there's a myriad of terminals out there, CRYPTOLOG regrets that it cannot advise you.

Send two legible hard copies accompanied by a floppy, disk, or cartridge as described below, or use electronic mail. In your electronic medium (floppy, disk, cartridge, or electronic mail) please heed these strictures to avoid extra data prep that will delay publication:

- do not type your article in capital letters
- do not right-justify
- do not double space between lines
- but **do** double space between paragraphs
- do not indent for a new paragraph
- but **do** paragraph classify
- do not format an HD as DD or vice-versa–our equipment can't cope

The electronic mail address is *via* PLATFORM: cryptlg @ barlc05
or *via* CLOVER: cryptlg @ bloomfield

CRYPTOLOG publishes using Macintosh and Xerox Star. It can read output from the equipment shown below. If you have something else, check with the editor, as new conversions are being added. Be sure to label your floppy or cartridge as to the hardware, density, format, and software you used. Don't forget your name, building, organization, and phone!

| HARDWARE | MEDIUM | SOFTWARE | FORMAT |
|---|---|---|---|
| SUN | 60 or 150 MB cartridge | ascii only | TAR or RAW |
| XEROX VP 2.0 | 5 1/4" floppy only | n/a | n/a |
| MACINTOSH | 3 1/2" DD disk only | MS WORD<br>MacWrite<br>TEXT<br>WriteNow | n/a |
| IBM & Compatibles | 3 1/2" 1.2 MB disk<br>5 1/4" DD or HD floppy | MS WORD<br>WordPerfect<br>WordStar<br>ascii<br>DCA (IBM revisable) | DOS |
| WANG | n/a | n/a | n/a |

~~TOP SECRET~~