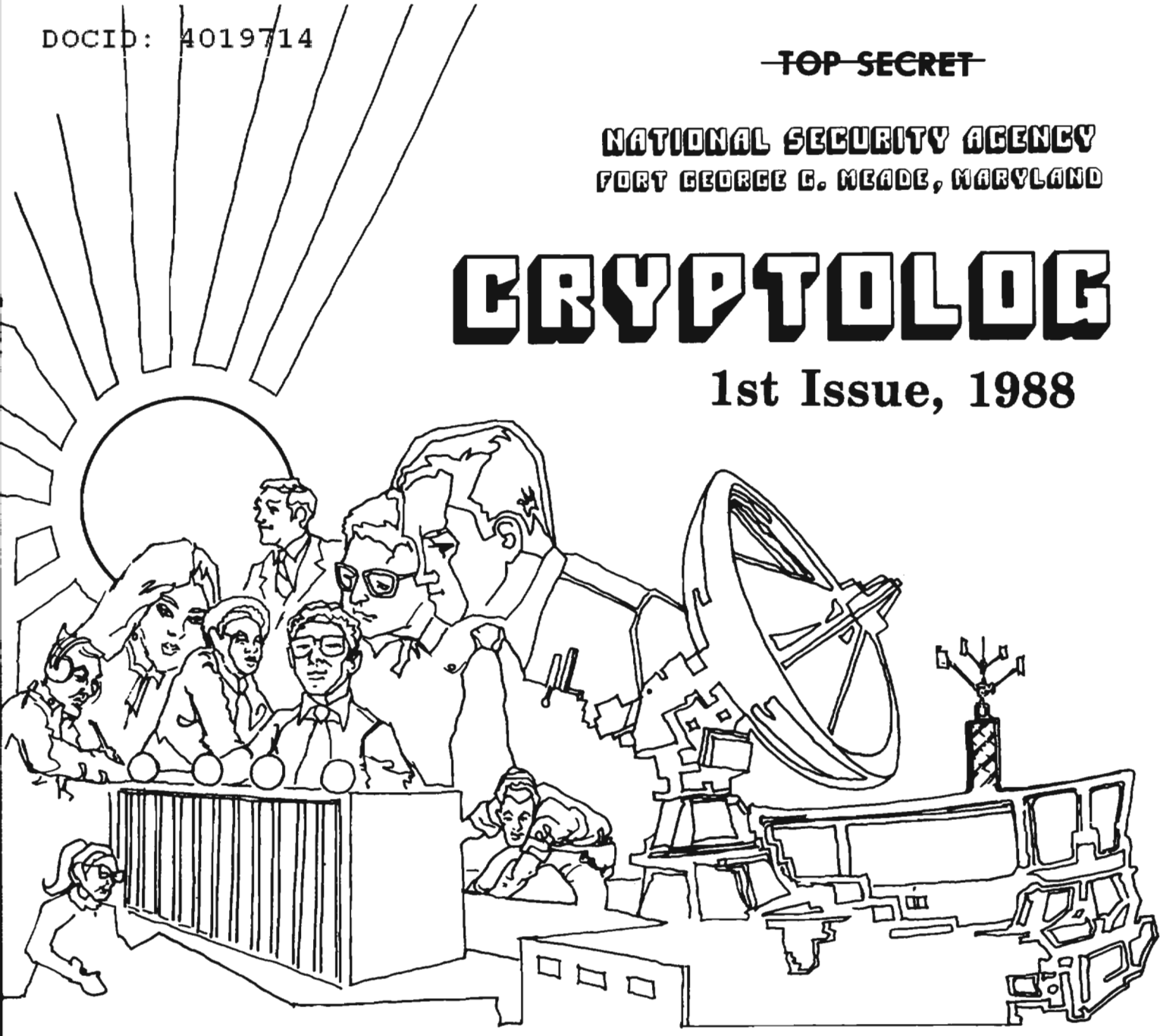
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue, 1988



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

P.L. 86-36

Published by P1, Techniques and Standards

VOL. XV, No. 1 ..... 1st Issue 1988

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization, and secure phone; also building and room numbers.

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

TIME TO WRITE

It's time to write at NSA!

Writing for a competition may bring you fame and fortune!

Writing for a competition may bring about revolutionary changes!

The most prestigious writing competition is the Agency's Cryptologic Literature Award. It brings very large cash prizes in addition to prestige. This year's deadline is March 31 for papers written in 1987. The papers may be submitted by the authors or by anybody else to: The NCS Registrar, Executive Secretary, Cryptologic Review Board, ITB.

While it's too late to write for this year's awards, you're just in time to prepare for next year's. And meanwhile, you can try the other competitions.

Just about every one of NSA's professional societies sponsors some kind of competition for writing, and most are open to all Agency employees regardless of discipline. Most competitions award cash prizes for the best entries. (It's not a bad thing to win an honorable mention, even without cash.) Usually winning essays are published, and sometimes, non-winning entries are published as well.

There's still another benefit to writing for a competition: the chances are very good that your words will be read by people who are in a position to act on your ideas. Some authors find this prospect even more appealing than winning a prize.

So, analysts, take pen in hand or put fingers to keyboard, and write!

THE DIRECTOR'S MAJOR THRUSTS

P.L. 86-36

Q1

Editor's Note:

An article on Thrust #4 by Glenn Stahly in CRYPTOLOG, 2nd Issue 1987, spurred many requests for information on the overall concept of the thrusts and for specifics on the other five of what were then six thrusts.

We are pleased to bring you this article by the Agency's coordinator for the thrusts.

Shortly after becoming Director of NSA in the Spring 1985, General Odom examined the Agency's missions and activities from the standpoint of existing international alignments. He realized that the requirements levied on NSA/CSS would continue to grow and expand, thereby straining its capabilities, so he developed six thrusts as a framework within which NSA/CSS could respond positively and effectively to existing and anticipated future requirements. He viewed the thrusts as areas of emphasis or direction on which NSA/CSS must focus its corporate energies to ensure the continuation of the vitality and responsiveness of its future missions.

General Odom based his original six thrusts on three basic considerations:

1) the estimates contained in the Future SIGINT Capabilities Study on the changing technologies expected to be applied in the telecommunications structures and operations of our target countries;

2) long-range estimates of the threat to our national security; and,

3) an examination of our customers' ever increasing requirements for intelligence information.

In October 1985 the thrusts were promulgated. They provide general direction in the areas of planning, budgetary programming, policy and operations. Now, all NSA/CSS specific plans must be consistent with, and support, the thrusts. In addition, the Service Cryptologic Elements (SCEs) are encouraged to use the thrusts as guidelines for their planning, programming and operations initiatives.

A paper on the thrusts was distributed to the Agency's key component chiefs and also to the SCE Chiefs, the Chiefs of Intelligence of the Military Services, and to the Director, DIA, as background information and to allow them to understand the direction in which we are heading.

The thrusts should be viewed as a synergistic set of forward-looking areas of emphasis that serve to:

THE TEN THRUSTS

1) to modernize the SIGINT collection and processing systems to cope with the changing target communications technology;

2) to integrate tactical and national SIGINT capabilities to satisfy more effectively military requirements in peace, crisis and war;

3) to maintain and improve our capabilities to support diplomatic, economic, and other non-military requirements for SIGINT support;

4) to maintain a large US lead in cryptanalytic capabilities, both in computers and in personnel;

5) to design a framework for a survivable SIGINT system, under all conditions, including general war, which we can develop incrementally and through astute dual-use applications over the next decade;

6) to provide easily attainable, inexpensive, user-friendly information systems security features;

7) to speed up research for major breakthroughs in the technology of computer security; at the same time, to help industry manufacture more "trustworthy" computer products for defense and other government needs;

8) to establish a program to reduce significantly the HUMINT threat to information security systems;

9) to provide modern, secure, user-friendly key management systems;

10) to overcome, by the end of 1991, the problem of wholesale obsolescence of COMSEC equipments and to establish a program to avoid it thereafter.

- provide a means for the Agency's managers and analytic elements to share in shaping the Agency's future;
- bring together separate budgetary programs (e.g., the Consolidated Cryptologic Program and the Tactical Cryptologic Program), thus allowing for the cooperative development of a total SIGINT system that will furnish critical intelligence information to SIGINT customers in peacetime, crisis, and war;
- influence our own cryptologic programs and enable us to influence other Intelligence Community programs that contain SIGINT capabilities but are outside the control of the CCP; and,
- serve as a yardstick against which the efficiency of all Agency resources (SIGINT, COMSEC, COMPUSEC) can be gauged and efforts redirected, where necessary, for maximum payoff.

Thus, the goal is to develop a coherent aggregate of capabilities that is technically healthy, secure, responsive to central NSA coordination and tasking under appropriate circumstances, adequately equipped to deal with all target communications technology, and concomitantly, one that is survivable.

The original six are now ten – five SIGINT and five INFOSEC. The original Thrust #6 was a broad, generic statement about continuing the present revolution in improved COMSEC and repeating that revolution in COMPUSEC. Subsequent study led to the conclusion that this thrust did not adequately address INFOSEC-related needs and concepts. The Director and the DDI thereupon developed five INFOSEC-related thrusts as a replacement for original Thrust #6. These new INFOSEC thrusts were promulgated on 4 November 1986.

In the past year, the Director and the chiefs of key components reviewed each thrust. Generally the status review takes this form:

> A knowledgeable person presents an overview of the thrust topic, followed by a round-table discussion led by the Director. The subject then is examined from the perspectives of planning, policy, operations, funding, resources, etc. When the discussion uncovers a shortfall or deficiency or poses a question that cannot be resolved at the table, a task is assigned to a single key component to lead a study of the problem

EXPLANATORY NOTE

on Thrust #10, block or wholesale obsolescence.

Updating our current COMSEC equipments piecemeal is somewhat like trying to update the kitchen of a single apartment in a 70-year-old building. You can't just replace the old frig with a refrigerator-freezer, or the old stove with a microwave oven-cum-stove; you can't merely install a dishwasher, garbage disposal, and a washer-dryer. You'll probably have to rewire the entire building and replace all the plumbing. And, very likely, you'll have to make sure that the connections to the water mains and sewers are up to the task.

So, like the old frig and stove, our COMSEC equipments are old technologically and cryptologically. Replacing tens of thousands of devices all at once is a daunting task as well as an extremely expensive one. We want to plan our modernization so that the same situation of wholesale obsolescence does not recur ten or twenty years hence.

and report the results to the Director. Other contributors are also designated, a suspense date is set, and the item is then inserted into the Thrust Tracking System. (Each action item specifies a "deliverable" to be presented to the Director, e.g., a briefing, paper, study, or funding item.)

The Director continually has reaffirmed his commitment to the thrusts within the Intelligence Community and outside it as well. For example, the first time he publically referred to the thrusts was during his budget testimony to Congress, linking budget items to a specific thrust. He refers to them during his interactions with the JCS, with the cryptologic and intelligence elements of the Military Services, with the Intelligence Community Staff, and with the US Commands. Moreover, whenever an opportunity arises, the Director seizes it to further the thrust concept and its use, not only within the NSA/CSS, but throughout the Intelligence Community and Defense establishment. For example, General Odom presented the five INFOSEC-related thrusts at the December 1987 meeting of the DoD-sponsored Military Communications Electronics Board which he hosted.

The NSA/CSS Field Representatives have been made fully aware of these thrusts. Moreover, the Director personally encouraged them to carry the message to the CINCs and local military commanders in order to gain their support for NSA/CSS programs and initiatives. Similarly, the SCEs are to use them for their own planning, programming and operations.

At NSA/CSS, the Director and the senior managers continue to review the thrusts, adding action items as they arise.

To involve the analytic elements, the Director sent a memorandum on 20 April 1987 to the Agency's workforce reaffirming his commitment to the thrusts and encouraging echelons two to three levels below to become familiar with them, to understand them, and to use them in their everyday decision-making. During his address to NSA seniors in June, the Director underscored their applicability to the Agency's future, stating that, even though the ten thrusts provide broad overall direction, they contain enough specifics to serve as a guide. Furthermore, he pointed out, there is sufficient latitude and freedom within them for the NSA/CSS workforce to excel and innovate. He emphasized that managers can use the thrusts to understand how he would respond in his interactions with other US government agencies and with Congress. The thrusts should be viewed not as a rigid set of directions but as areas in which managers and analysts alike are encouraged to participate and in which to take creative and innovative action.

The thrusts will continue to represent areas of interest and concern for the future efforts of the NSA/CSS. Previously, NSA Directive 25-2 "NSA Goals and Objectives" represented the Agency's future aims, but this directive was replaced by the thrusts. The usefulness of having areas of interest that can be understood by managers, analysts, customers, and laymen alike will undoubtedly pay dividends for NSA.

ADMINISTRATION

In order to keep up with the activity generated by the thrusts, there must be a focal point for

~~CONFIDENTIAL~~

UNITED STATES GOVERNMENT

memorandum

DATE: 20 April 1987

REPLY TO ATTN OF: DIR

SUBJECT: Director's Major Thrusts (U) - INFORMATION MEMORANDUM

TO: DISTRIBUTION III

1. My basic planning guidance, the six thrusts, have served as our overall direction for more than a year. In the meantime, it became clear that the sixth thrust needed further elaboration for the INFOSEC mission.

2. I believe that most of you have come to realize the coordinating effect these thrusts can have on all our programs in NSA. There is considerable linkage from one to another, and success in one either adds or reinforces success in another. I intend them as a general idea of where we are going. To the extent you understand them, you can anticipate and take initiatives on your own which are compatible and helpful in their larger context. In other words, they are meant not to constrain or restrict innovation and initiatives but rather to guide your innovations and initiatives into constructive directions for the USSS as a whole. They allow you to anticipate how I will judge the worth and utility of proposals and actions. They also allow you to fit your initiatives with those of other managers in other components and organizations without major confusion and cross purpose about final objectives. Finally, they help me keep track of where we are as a whole and what we may be neglecting or overemphasizing.

3. I intend to repeat the thrust reviews again this summer. These will involve a look at what we have accomplished since the last review and also another look at things we may be missing, actions we may have neglected, and things we might do to speed up and improve our programs under each thrust.

4. To make the most of these reviews, managers at lower levels need to think through the thrusts and ask what is lacking in our program efforts as viewed from their level. I want to get as much insight from two and three levels below as possible. While it may not be possible to act on all points raised from below, it is important to consider those points. They enriched my understanding last year in the review process, and I want even more this year. They also give me a sense of how well you understand my general guidance.

~~Classified By NSA/CSSM 123-2~~
~~Declassify On: Originating Agency's Determination Required~~

OPTIONAL FORM NO. 10
(REV. 1-80)
GSA FPMR (41 CFR) 101-11.6
5010-114

☆ GPO : 1985 O - 461-275 (428)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

5. Those of you in the support areas may not immediately see the direct relevance of the thrusts for you. In many cases it is indirect, but it is there. As we succeed in thrust one, two, three, and four for SIGINT, we create strains and new demands on training, communications, logistics, and facilities. To understand better these impacts on the support areas, I recently held a Corporate Management Review. Support, we determined, needs more attention, more resources, and stronger leadership in some cases. I do not view this emphasis on support as a change to the basic thrusts. I see it as essential for continued success in those thrusts. As we progress and you see that my program decisions emphasize some support areas, do not misread them as lessening emphasis on the thrusts--quite the contrary.

6. I share these thoughts with you to alert you to upcoming reviews and to give you time to think through once again the rationale of my general guidance so that you may profit from it and help me carry it through. As we progress, we may see reasons to modify the guidance. I do not see it as inexorable, and I am ready to make changes when the reasons are compelling. In the meantime, its firmness should be a help at all levels in making good decisions toward our shared goals.

WILLIAM E. ODOM
Lieutenant General, USA
Director, NSA/Chief, CSS

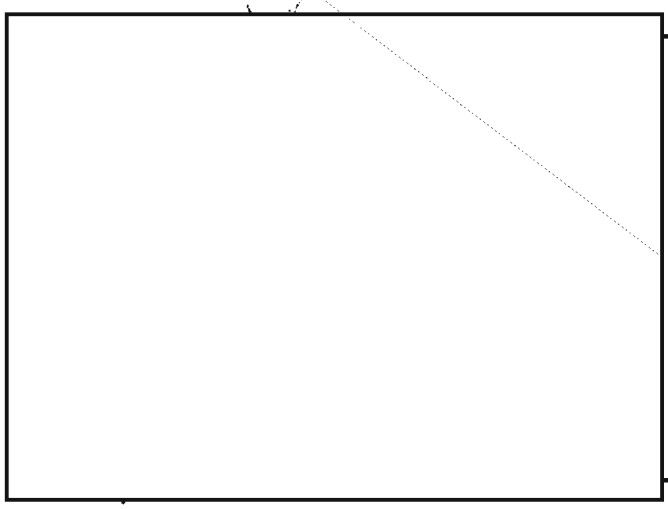
handling the myriad actions that emerge from the status reviews. At the outset, the NSA Chief of Staff administered the overall Thrust System in the Director's name. Recently, however, the DDPP assumed this responsibility. Q1 does the day-to-day work of handling the status reviews, preparing agendas, drafting summations of the meetings, initiating and maintaining the Thrust Tracking System, monitoring progress of the individual action items, negotiating and arbitrating between and among the various players, and submitting a monthly report to the Director on the status and health of the thrusts, and conducting follow-up actions. □

BULLETIN BOARD

WANTED: EXPERIENCED USERS OF UNICOS/UNIX

(U) Are you an experienced user of UNICOS/UNIX and willing to help others learn it? If so, please get in touch with [redacted] CRYSCOM Chairman, G451, and let him know which of the following you have experience in: [redacted] UNIX operating systems, programming languages, machine familiarity.

P.L. 86-36 P.L. 86-36



An Overseas Tour

P.L. 86-36

A PERSONAL CHRONICLE

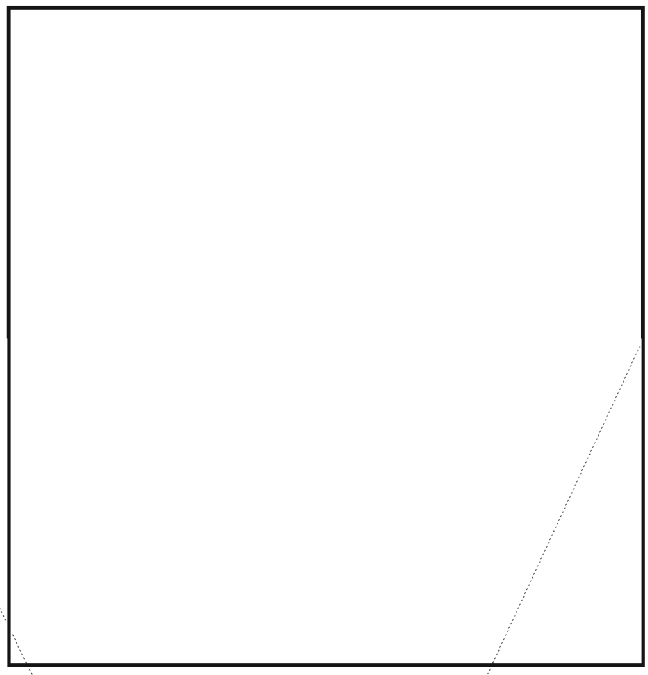
[redacted] *N2*

(U) I am writing this paper not only as a personal chronicle, but also as a means perhaps of convincing others to apply for an overseas tour. I am writing with mixed emotions because if I do a good job in convincing more people to apply, I may not be able to go again myself. I am not sure whether the circumstances that allowed me to finally get an overseas tour were unusual or not, but I have not heard of anyone else having the same experiences that I had.

GETTING THERE

~~(C)~~ With that in mind, I will get on with chronicling the events which finally culminated in an overseas tour. I had worked in B Group as a cryptanalyst for quite a few years and although overseas positions were advertised, there never seemed to be any for cryptanalysts. In 1980, a field announcement was circulated with a position for a cryptanalyst [redacted] It looked like an opportune time to get some experience in another aspect of the Agency. I filled out my application and sent it to the required offices. I also made appointments to talk to various people who would be making the selections and also to people who had been [redacted] either TDY or PCS.

(U) I decided that this was the job for me. The selection committee narrowed the candidates down to two people, me and the person who eventually got the job. All was not lost, though. Because I had expressed a lot of interest, the Chief of B5 asked me to consider transferring to B5 as the replacement for the selectee in order to have an inside track when the overseas position again became available. As it turned out, this was probably the ideal solution for B5 and for me.



~~(C)~~ This course is long and arduous but worth every minute. There were only three people in the class, all destined to be part of the [redacted] This included the future [redacted] the future computer and systems analyst, and myself. As in most language classes, morning dialogs and conversations were the norm. I can really appreciate the saying "you can run, but you can't hide". Pre-class preparation was a must and participation was required. Fortunately, our instructor, a native speaker, had the patience of Job and a sense of humor. I really think that the class was as hard on her as it was on the students.

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

(U) This part of the pre-departure preparation is probably the most difficult and brings the most complaints from people going overseas. The reasons for the complaints are many – not only do you have to go to class everyday and all day, you also have many administrative things to take care of at the same time, like: getting passport pictures, being inoculated, being briefed on security by various elements in M and N, finding out about financial and medical benefits or lack thereof, changing from one payroll system to another, learning your cover stories, trying to find out when you will be leaving, what your flight schedule will be etc., and the list goes on and on.

(U) As you get on with this you can only wonder whether it's worth it. Nothing seems to be organized, and there doesn't seem to be enough time to get everything done before departure. Patience is definitely what you need. After going through the process, I can empathize with the people in personnel, security and travel. They really have their tasks cut out for them. It is a thankless job for which they receive little credit when they should. So be patient – things always seem to work out eventually.

~~(S-CCO)~~ Finally, the big day came. All the paperwork was completed, I had my orders, passport, and tickets; my housing and hold baggage had been shipped and I was ready to go. Sometime before I left, the chief of the site sent a welcome card and an orientation package so that culture shock would not be too great. I was also very fortunate in that I had had an opportunity to meet her several months prior to my departure made it possible to meet some counterparts during their visit to NSA. All in all, the principals kept us informed and gave us the opportunity to meet everyone and anyone who might be able to give us insight to our assignment.

~~(C)~~ Be prepared for culture shock when you go overseas. No matter what anyone has told you about the country, you never really know what it is like until you get there. When I finally arrived the first thing I noticed was the heat. Hot and really bright sunlight. As in most places, people make lasting impressions and can either make a job memorable and enjoyable or absolutely unbearable. Well, fortunately in my case and I think for almost everyone else who has been in it started off on the right foot. The person whom I was replacing met me at the airport Welcome, and brought flowers. He took me to my hotel, checked me in and then took me out to our working spaces, which were located outside of metropolitan

~~(S-CCO)~~ I was introduced to all the team members and to personnel I would be working closely with for the next two years. Fortunately, there was almost a two week overlap before my predecessor's return, so he saw to it that I got to meet and associate with at the very beginning. I was not required to jump into a pond and sink or swim. Everybody at our station was helpful. The administrative officer made sure I liked where I was staying (initially most people stay in a hotel for several days before their apartments are ready), inquired if there was anything I needed, sent a message to my daughter to let her know that I had arrived safely, and did lots of little things that I personally probably wouldn't have thought of.

~~S-CCO)~~ The chief met me again and gave me a briefing on everything that went on and stressed that if there was anything she could do to help or answer any questions, anything at all, just let her know. I got the feeling right away, that this was like a family – everyone tried to help everyone else feel at home. The Ambassador also played a role in making new personnel welcome and comfortable by inviting new people to attend a country team meeting where he introduced them to his staff. Few analysts at the Agency have the opportunity to meet people at this level, but I did in this case. The Ambassador was very appreciative of the benefit and information derived through SIGINT and the assistance that our office provided him.

(U) All of this in the first two weeks. I had trouble believing it, but it was all happening. During this time I had settled in for an almost three-month stay in a hotel. Some people would think that this would be a real inconvenience, but as I was there by myself, and as the hotel personnel was very cordial and congenial, I found this an excellent opportunity to meet the people in a non-work environment. The

hotel management was quite friendly and I now number some of them as good friends. They found that if they treated the guests as a family, the stay was much more enjoyable as well as being just good business sense. This was also a good opportunity for me to start practicing [redacted]

WORKING THERE

[redacted]

~~(S-CCO)~~ This was evident soon after they were given a C/A course using the IBM pc. The Assistant Director of Training sent two very competent people to teach it and I acted as translator/interpreter and assistant instructor. As soon as the course was completed, I was getting questions on how to work specific problems; these were from the cryptanalysts and even the traffic analysts had found useful applications for the course.

[redacted]

HOW TO GET OVERSEAS

1. Keep track of the overseas jobs in the announcements as they come out.
2. Find out where you want to go.
3. Talk to people who have been there.
4. Talk to the selection official.
5. If you really want to go, apply and make yourself known to the people who can help you get there.

Unclassified

[redacted]

ADVANTAGES OF A FIELD ASSIGNMENT

1. Money (differential pay)
2. Travel
3 Experience
4. Career enhancement
5. Promotions
6. Meeting great people

Unclassified

~~(S-CCO)~~ As an advisor, I found that [redacted] respected the knowledge and experience I had and would listen to what I would tell them. I realized right away, though, that if something needed to be changed or improved or suggested, it was certainly better to do it in a manner in keeping with their culture. I could just not walk into an office and say such-and-such had to be changed because it was wrong to do it that way. Even though NSA furnishes much of the things they use, we are still their guests. I don't think you would call it a con job, but common sense.

~~(S-CCO)~~ [redacted] Well, remember the C/A course I mentioned before. I suggested that the C/A people who now knew something about using the PCs, type out their new systems on a disk in a format I had already put on the disk. This saved me and them a lot of time. They could make corrections, enter the system into their data base, and give the system to me in a short period of time. In turn, I could transfer their input onto a disk in message format, enter the correct date and message number, and give the disk to the our comm center for transmission to NSA.

[redacted]

~~(FOUO)~~ Going TDY was also an excellent opportunity to see other parts [redacted] Usually after the workday was finished, the site personnel would want to show you "their part" of the country. They would take to you to famous temples, important landmarks and tell you where to get the best food at the cheapest price and what the specialty of the area was. If you like sea food or strange exotic dishes, this is the time to try it. I had one soup that had animal organs in it that I did not recognize, and I was a biology major in college. I ate it anyhow and it was quite good.

~~(C)~~ I was lucky to have worked with a really good bunch of people, from the chief of the field site [redacted] It was more like a family working together to make things happy. If anyone had a problem, any problem, someone would help. Everyone covered the job responsibilities of team members if they were going to be TDY, on annual leave, etc. You always knew that any information to or from NSA would get to the right office. All of the different teams helped each other. When a shipment of equipment arrived and it had to be unloaded, everyone turned out to help.

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

[redacted]

P.L. 86-36

LIVING THERE

[redacted]

POSSIBLE DISADVANTAGES

- Possible loss of visibility (in your old office)
- Time difference for solving problems
- Looking for a place to work on return

Unclassified

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

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

[redacted]

(U) Living is fairly inexpensive and you can get bargains of almost any kind. Those who are interested in antiques can find an abundance [redacted] If you see an "old thing" you really like but the price is more than you want to pay, you can try to bargain for a reduction (I would recommend this avenue first) or you can probably find someone who can make it for a fraction of the cost. Clothes are another item that are good bargains. Tailor-made or ready-made, natural materials or man-made, they can all be found here.

(U) I really appreciated one of the benefits of an overseas tour and that is the R/R. I picked [redacted] It is really nice to have someone else pay for a plane ticket.

(U) As for the [redacted] people, I cannot say enough good things about them. They are friendly and truly are a smiling people. Not a lot of things appear to bother them and almost all are willing to help. They really make you feel at home.

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

RETURNING TO HQS

~~(C)~~ After I was in [redacted] for six months, I was asked whether or not I wanted to extend for additional 1 or 2 years. After discussing this with the chief of the field site, I decided not to extend for professional reasons. Also, after six months, I really did not know whether to stay or go. More about this later. About six months or so before I was ready to return, I found out that I had a job offer from a non-DDO organization, thanks again to a great boss who on her own had looked for a good job that would further my career. Actually as it turned out later, I had a pick of two positions.

(U) I also knew who my replacement would be so we had the opportunity to correspond with each other. During this time I tried to fill him in on what to expect, what to bring, who to see and anything else that I thought might help him and his family enjoy their tour. Unfortunately, we had no overlap to discuss problems and allow me to introduce him around to his counterparts.

~~(S-CCO)~~ After all the out-processing is done – you have to clear with Embassy housing, bank, commissary, and a lot of other places – you get your orders and plane tickets. I was seen off at the airport by my colleagues, [redacted]

(U) On return to CONUS, I was given 14 days of home leave and enough admin leave to more than cover the time needed to readjust and take care of personal and professional business. I had to check through different elements of M and N for personnel, security and finance. Some of this is a hassle, but necessary. I got a physical from the medical center. I also made it a point to stop in my old office to see how my replacement was doing and give them a debrief of what was going on when I left.

(U) There are some things I would like to see changed, from both a professional and personal point of view. They include:

a. the selection process: it takes too long

b. out-going processing: it is too confusing and time-consuming

c. the time (six months after arrival) when you have to decide whether to extend your tour: it is unrealistic. You really can't make a rational decision in six months. Just finding your way home at night might still be a problem.

d. scheduled overlap of for replacements – this should be a requirement.

e. upon return to NSAW, a two-week period should be spent in the office associated with the field site, not as only as a courtesy, but principally to inform them of how things were going when you left. It will also help your replacement if he or she has a problem.

f. return processing, especially for payroll: there should be an electronic way to transfer personnel from one payroll system to another without have to redo all the paperwork.

(U) All in all, I would say if you are looking for adventure, career enhancement, a lot of personal satisfaction, and a chance to meet new people, take a chance. Apply for an overseas tour, but not the one I want, thank you! □

STU III: The New Telephone System

V

~~This article is classified CONFIDENTIAL in its entirety~~

Three years ago NSA set out build a low-cost secure phone. We hoped to put practical secure telephones into the hands of hundreds of thousands of personnel handling classified and sensitive information. (See "NSA's Initiative on Secure Voice" CRYPTOLOG, Jun-Aug, 1985.) Today, as contractors are shipping out the first of the production STU-IIIs – Secure Telephone Unit III, pronounced "stew three" – it seems that our goal will be reached. In the process of achieving this goal, we have also created a device with the potential to change completely the nature of our entire telephone system. What this eventually will mean for us at NSA is replacing the black, grey, and green phones with a single handset.

In the coming year we will deliver approximately 50,000 STU-III's. Our options/add-ons to the present contracts will bring the total up to 80,000 by mid-1989. In addition, each of the three major services has identified a requirement for approximately 300,000 STU-IIIs each, and they have started programming action to fund these buys. All of these STU-IIIs will interoperate with one another. This secure network will be larger, by more than several orders of magnitude, than any secure network ever created. And it may grow even more if the volume of secure communications generated by a million interoperable secure phones creates a demand for more. To understand how all this may effect us, we need to know how our present phone system works and how the STU-III differs from it.

Currently most secure phone users communicate within and between secure areas. We encrypt calls only when communicating with a distant location comparable equipment. Usually some telecommunications organization takes care of encrypting, multiplexing and switching the calls and operating the secure trunk communications lines. The average user is not involved in this process at all. The present system is "user-friendly." You use it just like a "regular" phone. This system has some drawbacks, however:

- For the most part, you can call only locations with comparable systems.
- The system is "system high" so you can talk on it only to people who are cleared at least as high as you are;
- It is cost effective only in relatively large installations.

Unlike the present system where cryptography is separated from the phone instruments, the STU-III contains its cryptography in the handset. Though secure phones containing their own encryption devices have been around for years, the STU-III is different in cost, interoperability, and the keying scheme. The first production run of STU-IIIs has an average unit cost of $3828. Although this price would probably keep the STU-III out of the average home, it is almost five times less expensive than its predecessor the STU-II (KY-71), which sold for $18,136.

As the vendors make additional production runs of the STU-III, economies of scale will drive the unit cost down even more. Devices acquired from the options to the present contracts will cost only $2655. It is difficult to predict the final unit cost, but the trend is clearly

downward. Given advances in manufacturing and large productions runs, the unit cost of the STU-III may well drop to less than $1000 per phone.

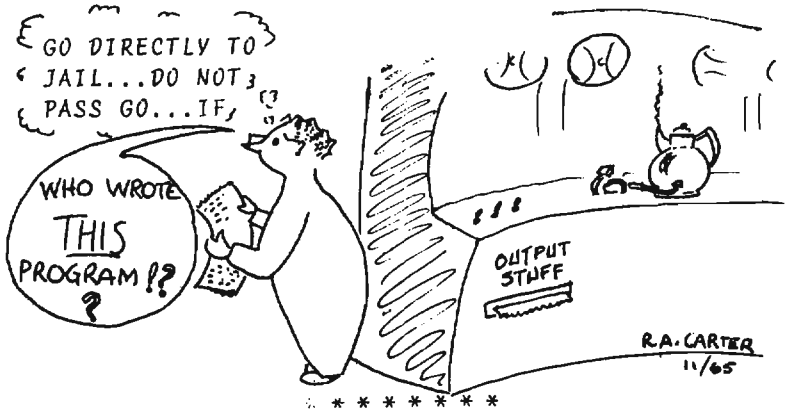
The STU-III enjoys a degree of interoperability that is truly revolutionary. It can be used anywhere there is a standard analog phone line simply by unplugging the present handset and plugging in the STU-III. While the earlier generation STU-II also enjoys the flexibility of using standard commercial phone lines, it does not have the STU-III's multilevel security capability. The STU-III can be used for all calls from unclassified to Top Secret Codeword. The secret of the STU-III's multilevel security is its keying scheme.

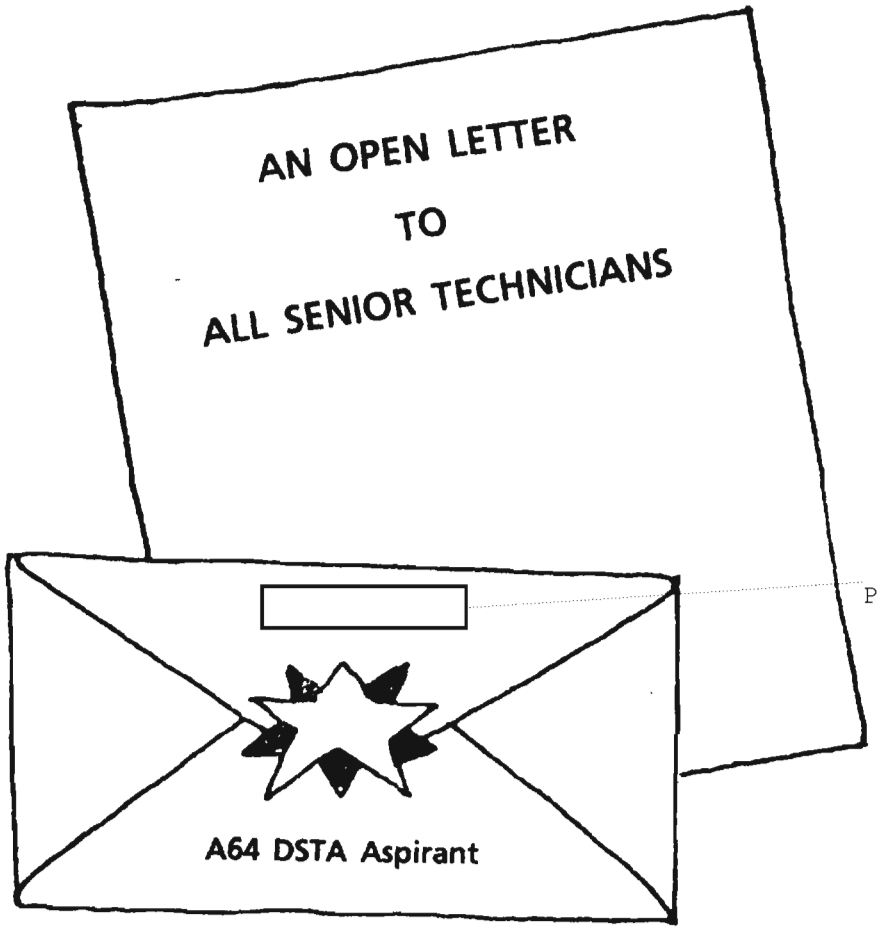
Unlike earlier generations of secure phones, the STU-III does not depend on an external source of keying material. The two phones in contact generate their own key with each call. They automatically and securely authenticate calls at all classification levels. Thus someone with access to a Secret level STU-III can call someone with a Top Secret level STU-III and talk securely at the Secret level. A display panel on each phone displays the highest common classification level *for that particular call.* A vast community that has not been able to contact us before will now be able to call us securely.

For the next decade we will be in a transition from our current secure phone system to a new system based on the STU-III. Meanwhile, operating both systems in parallel will demand an efficient interface between the new and the old secure phone systems. We have a large investment in equipment, expertise and emotion in the current system. Although sunk and hidden costs, such as segregated secure and non-secure cable plants and wideband circuit leases between installations, make a comparison difficult, placing a STU-III on every desk is not yet clearly cost-competitive at existing large fixed plant installations such as NSA Headquarters, CIA, and the Pentagon. Eventually, as the unit price of the new secure phones goes down, we can replace today's large fixed plant phone systems with a single instrument and a much simpler system to handle all of the functions of today's grey, green and black phones. □

GOLDEN OLDIE

Reprinted from:
bits & bytes
C4 Machine Processing Infomation Bulletin,
Vol I, No. 6, October 1965





Editor's Note:

A6's (voice language) technical track provides for post-professionalization certification in quality control (QC). The Branch Senior Transcriber/Analyst is expected to provide training and technical leadership on all branch projects and to provide technical advice to branch management. The Division Senior Transcriber/Analyst (DSTA) is to do the same on all or most division projects. At Office level the Senior Linguist should be capable of doing the same for selected projects in all divisions.

This article originally appeared in the Fall 1987 issue of Vox Topics. *It is reprinted here with the kind permission of the Editor.*

During a recent meeting of the A64 Technical Track Advisory Group the discussion centered on the tech track in general and specifically, on some of the perceived problems within the tech track. Two of the problem areas which surfaced during this discussion were:

(a) that some individuals were not staying current with the people and projects in the branches where they toured for certification in quality control, and

(b) that after certification many individuals were not paying back to the branches the learning time spent there as aspirants.

I would like to spend a little time discussing these two problems.

One of the areas that senior technicians are rated on when it comes time for performance appraisals has to do with technical leadership. This is a broad area that includes at least the willingness to perform on those projects where we have been QC-certified, as well as the requirement to take part in promotion boards, Career Development Review Boards, Quarterly Management Reviews, Branch Management Teams, Division Management Teams, etc. I don't feel that we can be considered to be properly performing in a technical leadership role unless we are willing to function in these areas.

In order to be able to provide adequate input to the groups mentioned above, it is necessary to know the work of as many people as possible. I believe that the only way to gain that knowledge is to spend some time each year in each of those areas where we are QC-certified. When I finally achieve certification as a DSTA, I will be QC certified in A641, A643, and A644. Since I enjoy chasing airplanes around the sky, I will probably make A643 my home. I do, however, intend to spend one month each year in each of the other branches in order to stay current, not only on the projects in those branches, but also to get to know the workforce so that I can better represent them. I would like to suggest that other titled senior technicians consider doing the same.

The process of becoming QC-certified on the projects necessary for becoming a titled senior technician is looked upon by some of the aspirants as nothing more that a ticket-punching exercise. Spend as little time as possible on a project, get certified, and immediately move on to something else seems to be the way many aspirants view the program. I believe that this is very short-sighted as well as selfish. The managers of each project we work on spend a good deal of time training us and getting us to the point where we can be considered to be QC-certified. It seems to me that the least we can do is to pay back a little of that time after we achieve that certification. The amount of time to be paid back should be negotiated between the aspirant and branch or project manager. I personally think that a pay-back of 20-25% is a good figure to aim for and, as a DSTA aspirant, this is what I am suggesting to the management of those branches where I receive QC certification.

Again, I suggest that other titled senior technical aspirants give this serious consideration.

The technical track provides those in the workforce who do not feel comfortable as managers and who are better technicians than managers with an avenue in which they can channel their efforts in a meaningful way. It is up to all of us who have chosen the tech track as our career path to make it the best it can be. To this end I offer these comments. □

BULLETIN BOARD

NEW ISO STANDARD FOR CYRILLIC

(U) The International Standards Organization has just published ISO 9, "Transliteration of Slavic Cyrillic Characters into Latin Characters." This is intended for "international communications." The new standard leaves every country free to adopt a *national* standard for its own internal use.

(U) ISO 9 provides Latin-alphabet equivalents for 52 characters, adequate for transliteration of Bulgarian, Byelorussian, Macedonian, Serbo-Croatian, and Ukranian.

~~(C)~~ At NSA, however, the authority for SIGINT purposes is USSID 406, "Standard Transliteration of Foreign Writing Systems." The individual annexes for specific languages treat special problems unique to that particular writing system. Address your questions about USSID 406 to [redacted] P044, 963-5577.

P.L. 86-36

ATTENTION: POLEMICS

(U) CRYPTOLOG seeks permission to reprint two items from POLEMICS, a cartoon and a mini-article. Would the appropriate person please send a note to Norm saying yes or no?

BACK FROM THE FIELD?

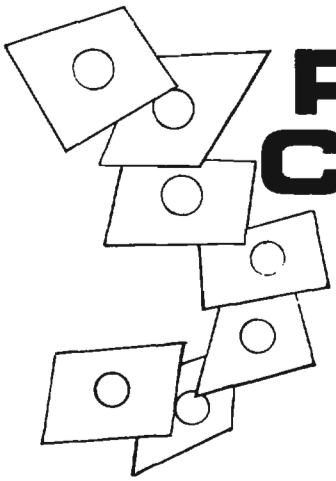
(U) Yes, you can catch up on issues of CRYPTOLOG published while you were away! Available on a loan basis is a volume titled *While You Were Away* ... which contains issues published in the last three years or so. Address your inquiries to the Editor, P1, HQS. Please do not call.

ATTN: CRYPPIES WHO PROGRAM IN C

(U) E53 is looking for unclassified examples of C-language code that perform unclassified CA techniques, and also some sample I/O (e.g., bit manipulation). The examples will be put in a booklet that will be given to students in C-language courses. Send your submissions to P1, HQS, for classification review. POC is [redacted] E53, ITB, 968-8007.

P.L. 86-36

FOR PC USERS



PERSONAL COMPUTER SECURITY

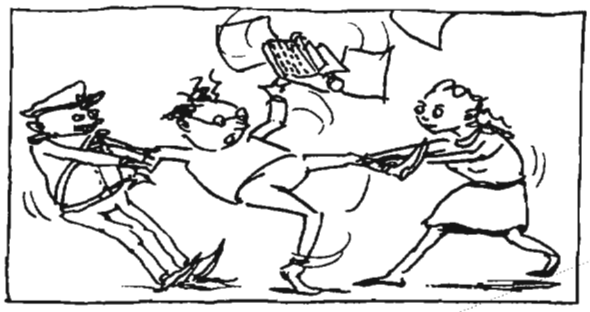
FLOPPY DISKS

Care and Keeping

- KEEP DISKS IN THEIR PROTECTIVE JACKETS WHEN NOT IN THE DRIVE UNIT.
- KEEP DISKS STORED UPRIGHT IN THEIR BOXES.
- KEEP DISKS CLEAR OF ERASER CRUMBS, DUST, AND SMOKE PARTICLES.
- USE A FELT TIP PEN WHEN WRITING ON THE DISK LABEL. PENCIL OR BALL POINT PRESSURE CAN DESTROY FLOPPY PRECISION.
- *MAKE-UP COPIES. THEN STORE THEM IN A SEPARATE FACILITY FROM THE ORIGINALS.*
- DON'T TOUCH THE DISK SURFACE. IT'S EASILY CONTAMINATED, SO SOMETHING AS MINOR AS A FINGERPRINT CAN CAUSE ERROR. ON A DRY DAY, YOUR FINGER COULD HAVE ENOUGH ELECTROSTATIC CHARGE TO DAMAGE THE DATA PERMANENTLY.
- DON'T USE ALCOHOL, THINNERS, OR FREON TO CLEAN THE DISK. CHEMICAL FUMES CAN ENDANGER THE MAGNETIC COATING, SO DON'T EXPOSE IT TO SOLVENTS LIKE NAIL POLISH OR DUPLICATING MACHINE FLUIDS.
- DON'T EXPOSE THE DISK TO MAGNETIC OR MAGNETIZED OBJECTS. DATA CAN BE DESTROYED, SCRAMBLED, OR WIPED OUT COMPLETELY. A COLOR TV, CRT, ELECTRIC MOTOR, OR OTHER DEVICES CAN DESTROY DATA INTEGRITY. SCREWDRIVERS, PAPER CLIPS, CAR KEYS, OR ANY METAL OBJECT MAY ALSO BE MAGNETIZED.
- DON'T PUT A TELEPHONE ON TOP OF A DISK, THE DISK DRIVE, OR A BOX OF DISKS. ONE RING CAN CAUSE DAMAGE.
- DON'T EXPOSE DISK TO HOME POWER SUPPLY UNITS.
- DON'T BEND, FOLD, OR USE RUBBER BANDS OR PAPER CLIPS IN THE DISK. ANY WARPING CAN LEAD TO MISTRACKING.
- DON'T REST HEAVY OBJECTS ON THE DISK. IT CAN CAUSE A CRIMP THAT WOULD LEAD TO MISTRACKING
- PROTECT YOUR FLOPPY AT LEAST AS WELL AS YOU WOULD THE DATA THAT'S ON IT.

NATIONAL COMPUTER SECURITY CENTER

LETTER TO THE EDITOR



P.L. 86-36

To the Editor:

(U) [redacted] letter [CRYPTOLOG, 4th Issue 1987] praising interns matches our experience. We value their energy and ability, and could not get along without their help. But experience counts, too.

[redacted]

(U) Succesful analysis depends not only on intellectual ability, but on some knowledge of what came before. The former without the latter is not enough. Particularly in this Agency we must place high value on experience, and create an environment in which experienced analysts (who may well have been 'bright young' interns in *their* day) can prosper and whose contributions are recognized. Only by remaining in the technical fields might they, one day, perform some the magic related above.

(U) The example I gave is simplistic, but the principle has broad application. Let's not denigrade the need for experienced analysts and look only to the 'bright young' interns.

[redacted]

P.L. 86-36

About

[redacted] *A538/P13*

~~(FOUO)~~ The first annual Cryptanalytic Software Conference (CRYSCO) was held in April 1984. The Cryptanalytic Software Committee (CRYSCOM) organizes and conducts this conference where super-computer users can share ideas and information and discuss plans and problems. The purpose of CRYSCO is to provide organizations using supercomputers with a better understanding of the plans and progress of cryptanalytic software used by other organization in the supercomputing community. CRYSCO also addresses long-range hardware and software plans and problems.

~~(C)~~ The week-long conference is attended by cryptanalysts and programmers from NSA and also from Australia's Defence Signals Division (DSD), Canada's Communications Security Establishment (CSE), the United Kingdom's Government Communications Headquarters (GCHQ), and the Institute for Defense Analysis (IDA).

~~(C)~~ Speakers are experts from NSA, [redacted] and outside people as well. CRYSCO presentations and workshops take place in the Friedman Auditorium and in a conference room.

~~(FOUO)~~ During CRYSCO, recommendations are forwarded by the cryptanalytic super-computing community, which are then reviewed, prioritized, and implemented by CRYSCOM.

(U) This year's conference, CRYSCO-88, will be held 23-27 May. Specifics on the program will be announced later. □

Review: FOUR WORKS ON CRYPTOLOGY (U)

Reviewed by: [redacted] *P11*

Analysis and Design of Stream Ciphers. by Rainer Rueppel. Sproinger-Verlag. Berlin, New York, Heidleberg, 1986. [TK5105. R83]

~~(C)~~ Though cryptologically naive, Rueppel has developed a great deal of shift register theory and has presented it in a very attractive way.

~~(U)~~ Rueppel is a Swiss national. Much of his book is taken from his doctoral thesis, written under the direction of Jim Massey, an American, at the Swiss Federal Institute of Technology in Zurich. Rueppel has had contacts in useful places. He mentions Borer Electronics of Solothurn, Switzerland; he was at one time an employee of a popular Swiss manufacturer of cryptologic equipment; he has designed a cipher system for the European Space Agency. He was recently visiting at the University of California, San Diego, in the Department of Electrical Engineering and Computer Science.

(U) Most of the work done by academic cryptologists has been in the development of "block" cipher schemes, for which a plaintext element (and a ciphertext element) is a unit of a preassigned (large) number of bits. Rueppel instead studies "stream" ciphers: text elements are single bits. As usual, there is the obvious, but universally acknowledged to be much less important, generalization to fields of more than two elements.

~~(C)~~ Rueppel begins with the usual definitions and carefully develops the algebra associated with polynomial rings over a finite field. He mentions the synchronization problem for stream cipher generators, and discusses briefly the advantages and disadvantages of "self-synchronizing" stream cipher generators, known to us as CTAK machines.

~~(C)~~ Chapter 4 is concerned with the "linear complexity" of a sequence (the length of the shortest shift register which will generate the sequence). [redacted] He shows that the linear complexity of a "random" n-long sequence is near to n/2; in fact the expectation of the complexity is asymptotic to 1/18 (9n + 4 + (n mod 2)) and the variance is asymptotic to 86/81.

~~(C)~~ It should be pointed out that Rueppel allows shift registers which produce tails (coalescent registers) and that a similar theory can be developed [redacted]

~~(S)~~ Using a recursion devised by Massey, Rueppel was able to calculate inductively the exact distribution for the function $N_n(L)$ = the number of n-long sequences which have linear complexity L. The work that he does is closely related to the mechanics of the Berlekamp-

Massy algorithm known to us as Zierler's algorithm, after its inventor.

~~(S)~~ Chapter 5, which takes up 88 of the book's 230 pages, deals with the analysis of nonlinear combiners which produce key from a linear shift register. Here the important result is the Paige-Blankinship Theorem, and Rueppel worries about when the (upper) bound of this theorem is in fact not attained. We know (and he does to) that such an occurrence is rare. Though the book was published in 1986, there is already an update to the material of Chapter 5: "Products of Linear Recurring Sequences with Maximum Complexity" by Rueppel and Othmar Staffelbach, in the 1987 IEEE Transactions on Information Theory.

~~(TSC)~~ In the 1984 IEEE Transactions on Information Theory, Siegenthaler defined the "correlation-immunity" of a function to be of order m if the output is independant of any m input variables. We would express this differently: the bulges of all linear approximators of density $\leq m$ are 0. It turns out that for a memoryless system one cannot have both large correlation-immunity and large linear order, since their sum is bounded by the number of input variables. This can be corrected by allowing a single bit of memory in the combiner, as Rueppel notes in his Chapter 9 (apparently an afterthought, as it logically should follow Chapter 5).

~~(TSC)~~ Rueppel goes on to define the Walsh (Handamar, Fourier) transform of a binary function and to develop its most elementary properties. This has been done before, but Rueppel goes on to make a connection with cryptology. He discusses the Data Encryption Standard (DES) and calculates a Walsh transform of one of the 6-input 4-output S-boxes. We already knew (this was announced by Adi Shamir at a CRYPTO meeting) that there exist strong linear approximations to some of the S-box functions.

~~(S)~~ Chapter 6 is one of the poorer chapters of the book. Rueppel notes that changing the timing of a register (operating the register d times as fast as the system clock or, equivalently, decimating the output of the register by d) yields a different stream. He proposes a random sequence generator as follows: Take two (or possibly more - he's vague on the implementation in that case) shift registers of different (say, relatively prime) lengths $L < M$, with primitive feedback polynomials. Form key as $k_i = \sum_{i=1}^{L} x_i y_i$ mod 2, where x_i and y_i are the contents of the L low-order stages of the registers. Optionally, add in some y_j for $j > L$. He seems to think he gains something by varying the speeds of operation of the registers.

(U) In Chapter 7, Rueppel introduces the notion of a cipher system based on the knapsack (subset-sum) problem. Initially this idea was devised by Merkle and Hellman, but the Merkle-Hellman knapsack has been shown by Shamir to be weak. Rueppel laments the reputation which has befallen the knapsack concept. The idea is that N positive integer weights $w_1, w_2,...,w_N$ are chosen and then a "test" integer T is given; the challenge is to find a subset of the weights which sum to exactly T mod Q. This problem is well known to be difficult (when N is large) for most choices of T.

~~(C)~~ In Chapter 8, "The Hard Knapsack Stream Cipher" Rueppel introduces an entirely new approach to knapsack design. This is the system proposed for the European Space Agency. This is not a public-key system; the weights are not available to the analyst. Rueppel employs an N-stage primitive register and a set $\{w_1, w2_1, ..., w_N\}$ of weights. He calculates an N-bit number $k = \sum_{i=1}^{N} x_i w_i$ mod Q, where x_i are the fills of the register and Q is a number equal to or just less than 2^N. The number k, expressed in its binary representation, provides N bits of key for encipherment. Recognizing that weakness may

exist in the low-order bits, Rueppel suggests shortening k by lopping off a few bits. He also recognizes that the regular single stepping of the device could lead to an attack, and proposes the multiple (but still regular) stepping of the register.

~~(TSC)~~ This seems quite a sensible proposal, and [redacted] Apparently Rueppel's design has appeared elsewhere, for Don Coppersmith of IBM has announced an attack [redacted] in a paper dated March, 1986. Coppersmith also refers to a paper by Gander and Bader. Coppersmith's [redacted]

~~(TSC)~~ The book sells for $47. I own only two books (each of two volumes) for which I've paid that much, but perhaps it's the changing times. I don't think Rueppel's book is worth that much. Certainly for us there's little that's new. He has a few problems with English, but none of the errors are troubling; he writes very well. [redacted]

Primality and Cryptography by Evangelos Kranakis, Yale University. Wiley-Tuebner. Stuttgart, Chicester, New York; 1986. 235 pp. $41. [TK 5102.k66]

(U) This is another book of cryptologic significance. It does not deal with mainstream crypt topics, as Rueppel's does, but prepares the reader to study with understanding the recent papers on cryptologic systems which are based on the difficulty of mathematical (especially number-theoretic) problems. I found nothing novel in Kranakis' book, but it certainly is a convenient collection of number-theoretic facts which one needs to know to understand contemporary academic cryptology.

~~(TSC)~~ One of the papers for which Kranakis prepares his readers is the interesting "A Simple Unpredictable Pseudo-random Number Generator" by Lenore Blum, Manuel Blum, and Mike Shub, from the 1986 SIAM Journal on Computing (pages 364-383). An internal (G44) paper "The x2 mod N key generator" comments on the article.

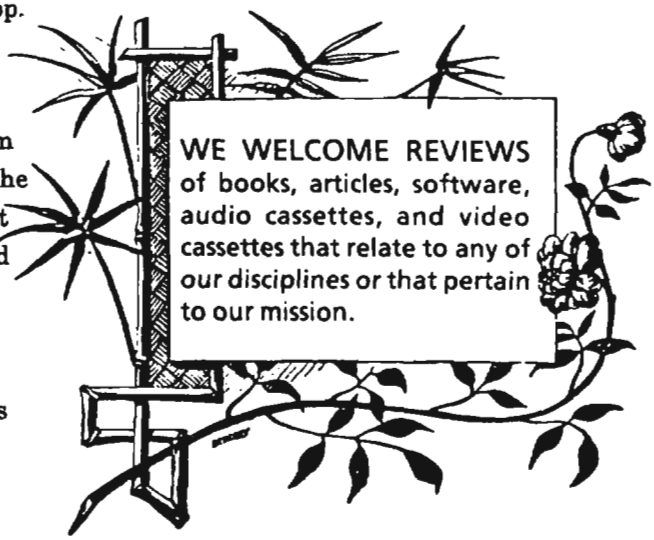
Two Issues in Public-key Cryptography: RSA Bit Security and a New Knapsack-Type System by Ben-Zion Chor. MIT Press. Cambridge (Mass), London. 1986. 78 pp. $20. [TK 5102.5 c478]

(U) This book represents the author's doctoral work at MIT under Ron Rivest. The Chor-Rivest knapsack was introduced at CRYPTO '84. A description should be in the Proceedings of that conference (available at the NSA library).

~~EO 1.~~ 4.(c)
P.L. 86-36

"Knapsack-type Cryptosystems and Algebraic Coding Theory" by Harald Niederretier. *Problems of Control and Information Theory* [a Hungarian journal] 1986, pp 159-166. [In NSA Library.]

(U) This Austrian was the co-author of an excellent book on finite fields. In the article he carefully compares his system with the Chor-Rivest Knapsack. No prizes for guessing the winner!



Technical Literature Review

Joseph L. Gastwirth, "The Statistical Precision of Medical Screening Procedures: Application to Polygraph and AIDS Antibodies Test Data" (with Comments by D. H. Kaye, J. C. Kircher and D. C. Raskin, Janet Wittes, J. D. Goldberg, Seymour Geisser, and Beth Gladen). *Statistical Science*, Volume II No. 3, August 1987, pp. 213-238.

Reviewed by: David Harris, R513

This article should be of interest to anyone concerned with either government polygraph or government drug testing policy.

The problem is the statistical analysis of the false positives and negatives when these tests are applied to populations in hopes of detecting rare phenomena. Suppose a test is 90% reliable in the sense that if a person has the disease, there is a probability of 0.9 that the test will give a positive response, while if he does not have the disease, there is a probability of 0.9 that the test will give a negative response. Suppose only 1 person in 5000 in the population being tested has the disease. Then, in any 5000 people tested, there will be about 500 positive responses to the test, but only one of these people will in fact have the disease. Gastwirth takes this standard analysis further in showing that in such situations, it is extremely difficult to analyse accurately how reliable the results of the test are. Thus, we may not even be able to draw reliable inferences on how much faith we should have in the test as a guideline to who is diseased and who is not.

The implications of this for the proper use of drug tests and polygraph tests are clear. Employers who give people a single polygraph test, and then either fire people or refuse to hire people on the basis of this test (a common practice in industry) are likely to be doing grave injustices to hundreds of people for every one true risk they expose. This is especially serious when the victims have no legal recourse against employers who advertise the results of polygraph or drug tests to the community at large. Such use of testing in screening a large population is clearly believed improper by all the experts. Repeating the test may or may not protect against injustice, depending on whether the false positive is for a causal reason, resulting in correlation between the incorrect results of consecutive tests.

Two guidelines are generally accepted by all the experts. First, if advanced screening has been applied so that the population tested has a reasonably high likelihood of being infected, then the problem of false positives is much less severe. Testing for AIDS in a high risk population is more reasonable than testing for AIDS in the population at large. This, of course, has implications for drug testing especially. Second, even when a trait is low probability in the population tested, there are proper ways of using the results of the test to guard against abuse. In particular, failing a polygraph or a drug test should not in and of itself disqualify an employee, but passing a test can be taken, in the absence of further reason for suspicion, to be grounds to trust the employee.

Polygraphs and drug tests can thus be used as money-saving devices. If an employee passes such a test, we may reasonably cut back on other checks of his character. If an employee fails the test, then he should get special attention of some sort. Since relatively few people in the population fail the test, we can concentrate our efforts on them. But, when screening a largely innocent population, we should remember that most of the people who fail the test are innocent. Thus, in AIDS testing, if someone fails the ELISA screening test, the proper approach is to explain the situation to him unhysterically, and go on to more sophisticated tests to settle the matter.

That there is general agreement among the experts on the proper technique for screening a broad population is impressive. □

CRASHING THE SYSTEM

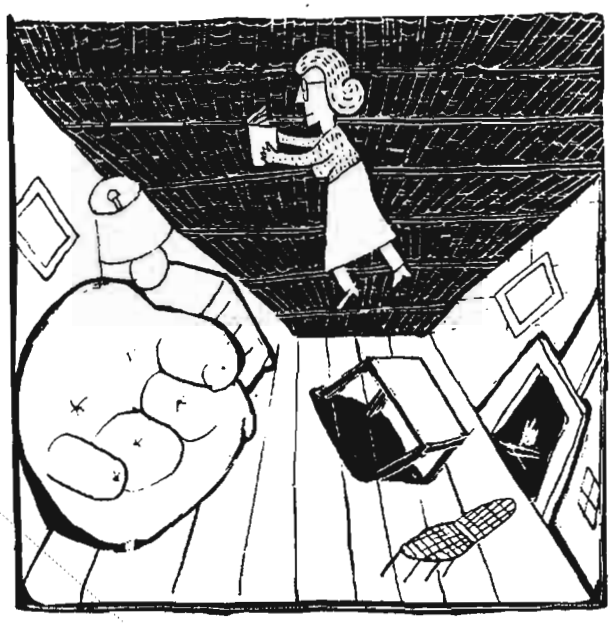
by [redacted] *C11*

(U) System crashes have become commonplace in this high-tech world. All kinds of things can cause them, from power failures to innocent mistakes by a (perhaps inexperienced) user. The latter variety are ones that operating systems try to prevent, but as with most things done by human beings, they are subject to mistakes. I can recall my own experience crashing the system.

~~(FOUO)~~ The object of my attack was RYE, and I used it infrequently enough to need the cheat-sheet (a three-by-five card, actually) that Carolyn Palmer had taped to the terminal. Carolyn had used a red pencil when writing the card; the first element of the first command line was the priority, a digit from 1 to 7, but the digit we were to use was a 3. Carolyn had made a slight goof when she started writing; maybe she was thinking of something else; at any rate, she started off with a single vertical stroke, which she tried to erase. Marks made by red pencils don't erase easily. Her "3" was abutted to a partially-erased vertical stroke, looking for all the world like a "B."

~~(FOUO)~~ Maybe you can guess what happened. Logging onto the system, I typed the "B" that I thought I was seeing and proceeded with the rest of the command. Too late, I remembered that the first character should have been a digit. About an hour later I got a call from the System Administrator [redacted] as I recall), wanting to know why I had logged on with the Director's priority. It seems that 7 (the highest) was reserved for the Director, and it threw everybody else off the system. But I hadn't asked for a "7"—I had asked for a "B".

~~(FOUO)~~ In what is good programming practice in other situations, the system tested for a "greater-than-or-equal-to" 7, rather than just testing for "equal-to" 7. On that system, alphabetic characters were numerically greater than digits. So to the system I looked like a surrogate for the Director. I think they fixed that little bug after that.



The Lingala Code. by Warren Kiefer. Random House, New York, 1972.

Reviewed by: [redacted] *P16*

(U) Why report on a 16-year old novel? Because I just ran across it by chance when my local library rearranged its holdings.

(U) It is an adventure story abounding in steamy jungles, spies, and bureaucratic infighting. There's lots of atmosphere. It's a good yarn, clearly written by someone who was there at such at time and who participated in events similar to those described.

~~(FOUO)~~ But the reason for reporting it here, however belatedly, is that the author describes an ingenious cipher system, the invention of "Eddie Ryan," a code clerk working with "Mike Vernon," a CIA agent in Africa. It seemed plausible to me, and even more so after reading the description of Lingala beginning on page 24.

~~(FOUO)~~ This book certainly would have been acquired for the Crypt Collection back in those Olden Days—which become ever more Golden with the passing of time. The Collection included fiction that had descriptions of crypt systems, especially home-made ones, just in case they popped up somewhere.

(U) (Say, whatever happened to the novels that once were in that collection?)

(U) Let "Mike" describe the Lingala code:

Ryan's system had the supreme virtue of looking exactly like several hundred other obscure African dialect written phonetically. Yet it was not. It was, as Ryan said, gibberish. Only when broken would it become a piece of intelligible information.

The Lingala Code worked on some of the oldest cryptographic and theological principles available to Eddie Ryan. Its basis was a missionary grammar which had fascinated him, and which he then showed me. The book was the product of a Protestant evangelical conference in Ubangi in 1931. I leafed through it.

. . . . . .

As I said, Ryan had talent. The Lingala Code answered our simplicity requirement. And it was secure, as Washington later discovered. The following day I sent it off to the States without the missionary grammar. The Agency failed to crack it, computers and all. That was because machines do no have Ryan's imagination, let alone his perception. When I sent the Agency the book finally, it still took them a few days to break the code. They did not realize that the underlying key was the way of the Congo: simple tings were often simpler than they looked, until you turned them inside out and found they were not, quite. The Lingala Code never attracted attention because it looked and sounded like a bone-fide African language. Everyone thought it was.

Lingala is a tonal language. That was one of the keys to the code's success. Lingala had never been written by the people who spoke it until the missionaries came. For their schoolrooms and their prayer-learning, Lingala was necessary, and by missionary standards, it was equally necessary that the local tribesmen become literate in what was essentially a spoken tongue. The wrong tone in Lingala could turn the word for "shield" into the word for "nut." So the phonetic system was full of traps.

The last sentence of Ryan's coded page read "Kobana yu aya yosa yu mumu."

Read that sentence aloud to the average African and he will not laugh. It was total nonsense. But the average African is polite, and language is language. There are so many dialects that it can pass as just another. I tried the Lingala Code on two eminent professors at Louvanium University, men learned in tongues of African origin. They were unable to make any sense of it, but they sagely agreed, because of its presumed source, that it was an interesting variation on one or another esoteric tribal speech. Bullshit. It was a variation on Ryan's ingenuity.

If one read the sentence, as Ryan suggested I read it, in reversed word order, it took on a recognizable, halting African rhythm: "Mumu yu yosa aya yu kobana." But it was still gibberish.

Then he showed me his simplified table of ten letter substitutions. It contained four vowels and six commonly used Lingala consonants. The list looked like this:

a=u, e=i, i=o, u=l, l=k, k=n,

n=b, t=m, b=y, and m=l

With the substitution, the new sentence read "Tata na biso oyo na likolo." A quick reference to the missionary grammar, and I came up with a literal translation of "Father from we is of heaven . . ." or "Our Father Who art . . ." etc. Ryan pronounced me a genius.

"Now sir" he continued patiently, "in our word assignments, suppose we designate 'Father' our man in Stanleyville and we assign 'heaven' as the code name for Kamina base. The message is quite clear."

LANGUAGE BRIEF: LINGALA

by [redacted]

(U) Lingala was originally the speech of the Bangala, a tribe living between Lisala and Nouvelle-Anvers in northwest Congo. First through the trading activities of the Bangala up and down the Congo River, and then through their services as mercenaries of the Belgians, Lingala became a lingua franca spoken on both sides of the Congo River from Kinshasa to Kisangani. Under the Belgians, it was the usual language of laborers, clerks, riverboat and railroad employees in the whole central and northern part of the Congo.

(U) It is one of the four official native languages of the Congo and, along with French, the official language of the Congolese National Army. It also appears to be known by all major government figures. Most Congolese have learned Lingala as a second language, but nowadays many urban dwellers, particularly in Kinshasa, learn it as a primary tongue. It is

~~(S-CCO)~~ This article was originally published in the November 1969 issue of The Quarterly Review for Linguists (QRL) where it was to be the first of a series of briefs on "the more exotic languages" prepared by linguists working in those languages. In fact, only one other brief was published, on Uzbek, in the May 1970 issue.

~~(S-CCO)~~ The idea for language briefs was presented by Prescott Currier in his article, "Data for the Language and Linguistics Section of the Country Reference Book" in the May 1968 issue of QRL. The Country Reference Books were to be a series "designed to provide useful technical information in ready-reference form on each of the target countries of NSA." That project never got off the ground.

~~(C-CCO)~~ We invite linguists to contribute briefs on low-density languages as well as on "exotic" ones. You may wish to consult the outline suggested by Capt. Currier. For a copy write to: Editor, CRYPTOLOG, P1, HQS.

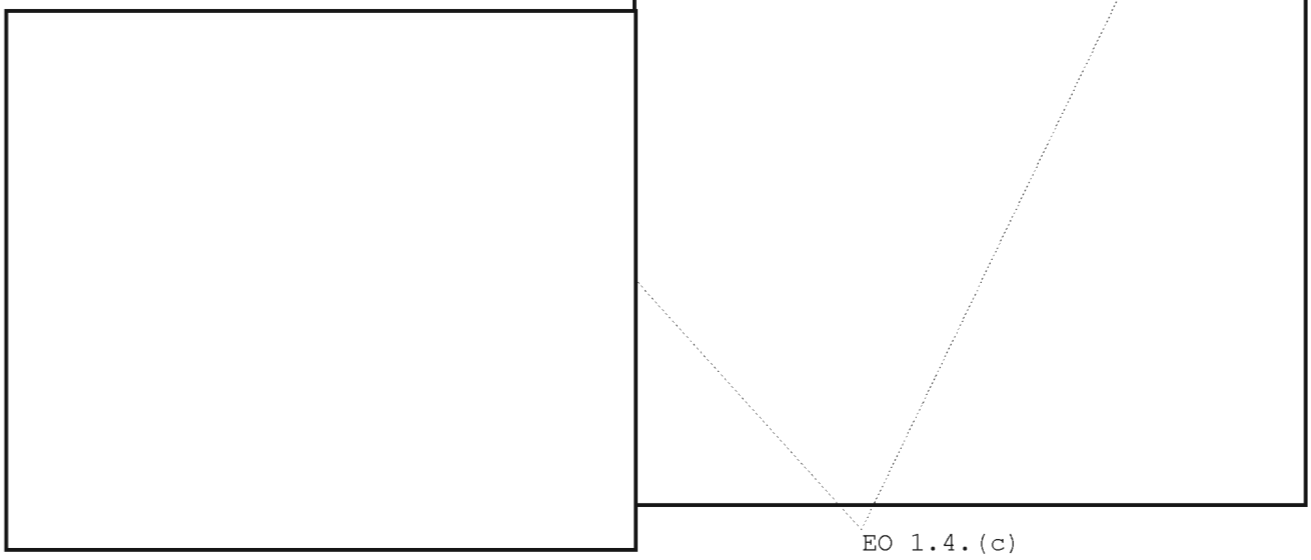
probably the most useful of the Congolese languages for a foreigner to learn; it is also an excellent starting point for the study of Bantu languages.

(U) Lingala is a member of the Bantu family of languages which dominates almost the whole southern part of Africa from the lower edge of the Gulf of Guinea across to the Indian Ocean below Somalia. It shares with other Bantu languages the characteristic of noun classes (of which it has seven) distinguished by prefixes and agreement of other parts of speech with the noun by means of concordial prefixes.

(U) Through its widespread use as a lingua franca Lingala has become simplified. Rules for concordance are not strictly observed; many adjectives are invariable and in everyday language the use of verb prefixes showing person and number is limited. The genitive particle -A normally appears only in the forms -NA and -YA, the two highest-frequency words in the language.

(U) The consonants used in Lingala are b, d, f, g, k, l, m, n, p, s, t, w, y, and z. The letter r does not occur (in foreign words it become l). U often occurs as a variant of o; dz, dj, and z frequently interchange. The nasalizing consonants m and n are sometimes dropped before another consonant.

(U) Tone is of some importance in spoken Lingala, but since there are no tonal markings in the standard written language, context has to be the prime determinant of meaning. The frequent inclusion of the French words in Lingala texts can often be an aid to understanding.



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

More Letters

To the Editor:

I refer to [redacted] letter in CRYPTOLOG, 3rd Issue 1987.

Amen!

Vera Filby, E4

To the Editor,

Just a note to say that I enjoyed [redacted] [redacted] article on traveling very much.

I can't match his experience by a long shot, but it did bring back some of my memories of trans-Pacific MATS flights in the middle and late 50's (crash trucks and Hawaiian lay-overs then, too) and of travel to the Middle East (special baggage searches, unattended baggage concerns).

I wonder if Kermit ever went through body searches in the Far East? South Korea lacked electronic gear in 1959, so there were separate male and female search rooms.

Again, thanks, Kermit, for taking the time to write that article.

[redacted] *G*

To the Editor:

I was intrigued by your note on the British Diplomatic Cipher of 1783 [4th Issue 1987]. This cipher looks a great deal like what is most frequently referred to as the "Beale Ciphers". Basically a source document is chosen. The words are then numbered starting with the first word or some previously agreed upon starting point. To encipher the plaintext, a word is chosen at random from the source document which has the same first letter as the plaintext and the number of that word is written down as the first cipher character. Hopefully, the encipherer will also mark through each word in the source document to prevent a unilateral substitution. In this case, a source document of 4000 or more words is needed since numbers in the 3900's appear. Finding the source document is no easy matter but even a second grader can solve the problem if the source document is in hand.

Sir Arthur Conan Doyle described this system in "The Valley of Fear". The Beale ciphers appeared in 1820 as documented in a 1964 paper by George L. Hart published by the Roanoke, VA. Public Library. The first mention of such a system may have been by a French mathematician named M. Michel Chasles who flourished around the time of the French Revolution.

Many man-hours have been spent by the American Cryptogram Society and the Beale Cypher Association in the unsuccessful attempt to decipher the two unsolved 1820 Beale messages, which indicates a certain degree of security of the method.

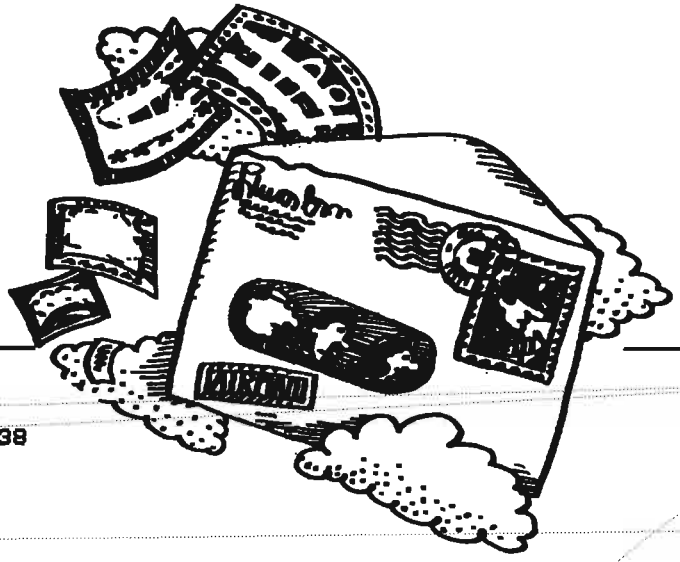
[redacted] *R223*

To the Editor:

Another "well done" on your 4th Issue 1987, with very valuable tips in the articles on writing.

I'm circulating my copy throughout C1!

[redacted] *D/Chief, C12*



CLASSIF
ZCZCRKA746DAR535
RR [redacted]
DE [redacted] #3043 0210838
ZNY MMNSH
R 210838Z JAN 88
FM GCHQ
TO [redacted] MD
ZEM
~~C O N F I D E N T I A L~~
QQQQ
[redacted]
CLASSIFIED
CRYPTOLOG NO 4 1987 - BRITISH CIPHER OF 1783
1. CODE BEARS CLOSE RESEMBLANCE TO TWO WE HOLD IN CIPHER MUSEUM DATED 1809 (R/R) AND 1820 (T/T). BOTH ARE TWO-PART WITH 4200 GROUPS, OF WHICH 102 ARE INSTRUCTION GROUPS (EG TAKE ONLY THE FIRST SYLLABLE OF THE PRECEDING NUMBER). COMMON GROUPS HAVE TWO OR OR MORE ALTERNATIVES (19/19 FOR WHAT IS EFFECTIVELY END SYLLABIC SPELL, 4/4 FOR FULLSTOP, 5/5 FOR A). VALUES ARE OFTEN COMPLEX, EG HUR,RICANE, T,FUL,RY,RIED.
2. CODE T IS ESSENTIALLY A HATTING OF CODE R IN SMALL BLOCKS OF GROUPS (2/3/4) - PROBABLY BY SHUFFLING DECODE TYPE CASE. FCO IS KNOWN TO HAVE TWO EARLIER VERSIONS: Q/G OF 1806 AND N/N OF 1795. SHALL BE CHECKING THESE ON FRIDAY 22 JAN. THERE IS A POSSIBILITY THAT ONE MAY WORK AS PARIS IN 1772/3 HELI K/K THRL P/P (SEE KAHNS CODEBREAKERS PP 173-174). WILL LET YOU KNOW RESULT.
#3043

United States, within the meaning of the Espionage Laws, Title 18, ...ion to an unauthorized person is prohibited by law.

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

CLASSI
ZCZCRKA240DAR965
RR [redacted]
DE [redacted] #3212 0251628
ZNY MMNSH
R 251628Z JAN 88
FM GCHQ
TO [redacted]
ZEM
~~C O N F I D EN T I A L~~
QQQQ
[redacted]
CLASSIFIED
FURTHER MY 210838 JAN 88
1. NEITHER N/N NOR Q/G WORKED THE ORACLE. YOU MAY CARE TO PASS ON THAT GROUP RANGES AS FOLLOWS (ALL 2-PART):
N (1795) 1-4200
Q (1806) 1001-5200
R (1809) 1-4200
T (1820) 301-4500
INSTRUCTION VALUES ALL THE SAME.
2. POSSIBLE THAT PUBLIC RECORDS OFFICE MAY HAVE SOMETHING. WILL ASK FOR NON-PRIORITY LIBRARY HELP.
#3212

...within the meaning of the Espionage Laws, Title 18, ...nor to an unauthorized person is prohibited by law.

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

NSA -CROSTIC #66

The quotation on the next page was taken from an article that appeared in an NSA publication. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS

A. Learned

B. Injuriously

C. Travel

D. Use

E. Attic quality

F. Coined

G. Fascinated

H. Blood condition

I. The act of exploding

J. Compels obedience to

K. Plumbing fixture

L. "The ——— Show"

M. Anna Pavlova used it

N. Know by instinct

O. Cape preamble

P. Miss Dunham

Q. Scurries

R. Barnyard speech

S. Terminator

T. Shade

U. Encourage

V. Serpentine

W. Hairy spider

X. A motley crowd

Y. Pertaining to birds

Z. Gravity gradient

a. Where meteorites fall

WORDS

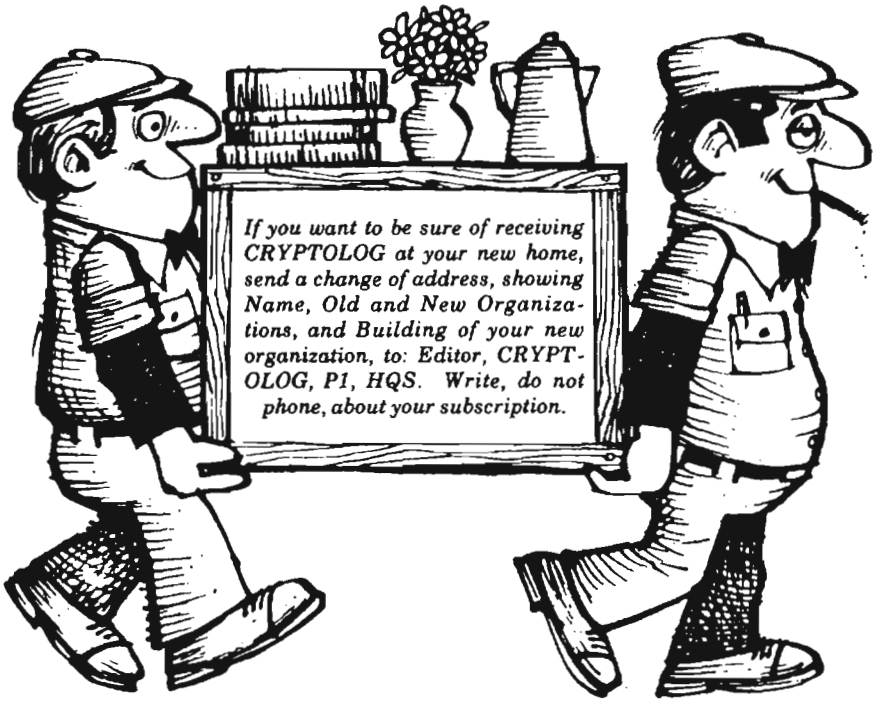
175	141	131	125	159	52	82	118	169		
128	105	19	196	34	66	92	187	123		
197	142	77	151	114	183	3	170	46	9	
178	137	144	103	108	56					
147	163	80	139	68	181	190	182	10		
107	90	31	130	106	186					
180	88	55	42	47	198	122	104	100	69	
74	51	5	143	22	12					
2	40	11	28	48	195	65	124	96	78	24
121	185	17	173	75	84	132	165			
167	39	21	37	97	13	194	161	172		
81	67	91	119	49	98	32				
44	14	89	136	176						
1	27	150	83	30	171					
25	201	133	112	153	61	87	71	93		
120	23	85	4	38	193	164	149	174		
20	62	115	16	36	45					
157	50	79	72							
152	86	156	200	54	168	155	18			
166	146	60	199							
154	127	29	7	192	140	64				
148	110	134	53	160	189	58				
135	8	15	59	158	177	184	145	191		
116	70	94	6	138	162					
26	179	102	63	35						
113	43	73	202	126	188	57	57	95		
117	33	109	41	99	101	111	129	76		

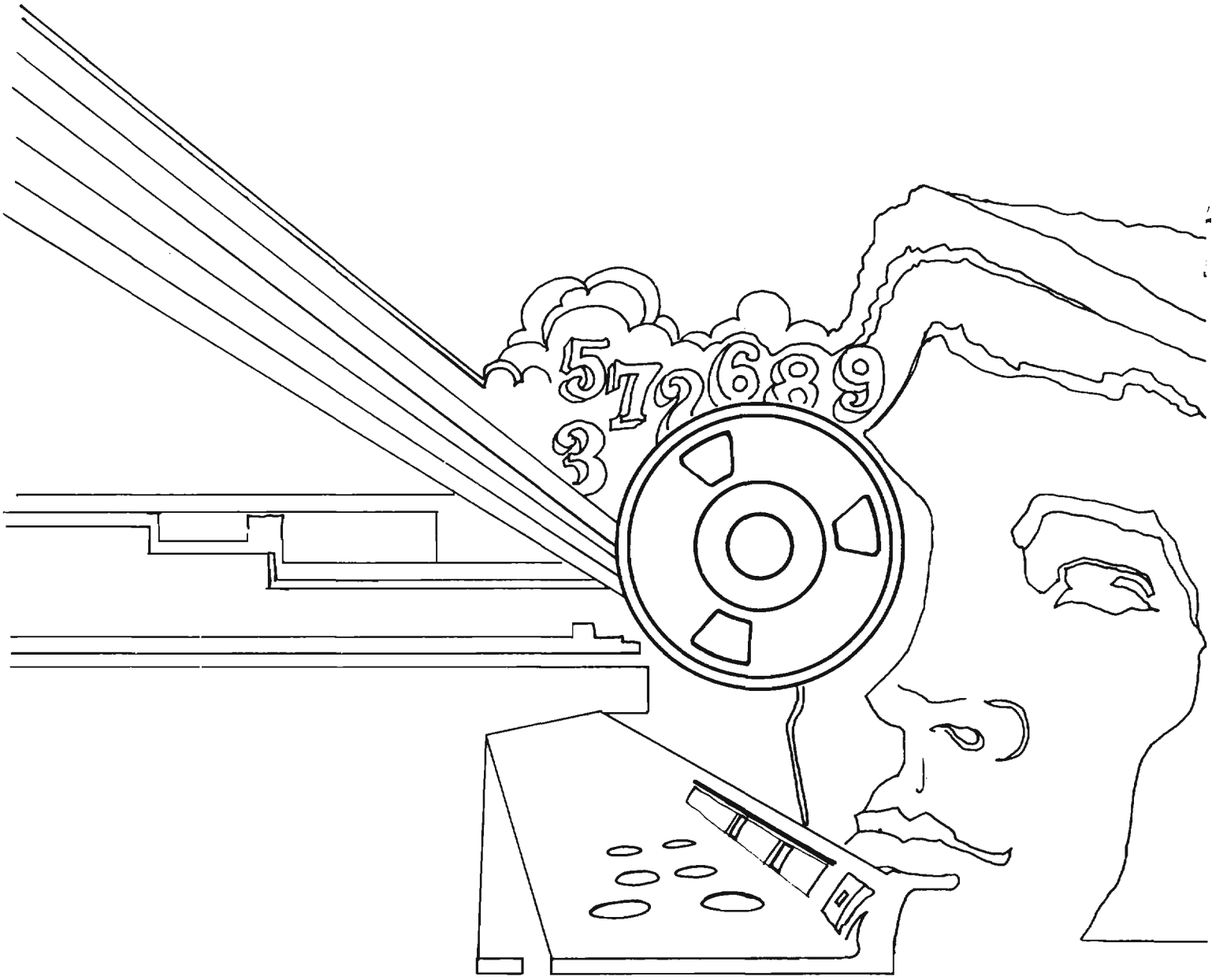
HOW TO SOLVE A DOUBLE-CROSTIC

Using the Definitions, fill in whatever Words you can. Then copy each letter from the Words into the corresponding square of the grid below. Scan the text in the grid from time to time; from the recovered fragments you may be able to complete the word in context. Copy the new entries from the grid into the Definitions, where the fragments there might suggest a complete Word, and so on, working back and forth. Also, scan down the first positions of the Words as you recover them, for additional clues.

1 N	2 I	■	3 C	4 F	5 H	■	6 X	7 U	8 W	9 C	10 E	11 I	12 N	13 K	14 M	15 W	■	16 Q	17 J	■	18 S
19 B	20 Q	21 K	22 H	23 F	24 I	■	25 O	26 Y	27 N	■	28 I	29 U	30 N	31 F	32 L	33 a	34 B	35 Y	■	36 Q	37 K
38 P	■	39 K	40 I	41 a	42 G	43 Z	44 M	45 Q	■	46 C	47 G	48 I	49 I	50 R	51 H	52 A	53 V	■	54 S	55 G	56 D
57 Z	58 V	■	59 W	60 T	61 O	■	62 Q	63 Y	64 U	■	65 I	66 B	67 I	68 E	69 G	■	70 X	71 O	72 R	73 Z	74 H
75 J	76 a	■	77 C	78 J	79 R	80 E	81 I	82 A	83 N	84 J	85 F	86 S	87 O	88 G	89 M	■	90 F	91 L	■	92 B	93 O
94 X	95 Z	96 I	97 K	98 I	■	99 a	100G	■	101a	102Y	103D	104G	■	105B	106F	■	107F	108D	109a	110V	■
111a	112O	113Z	■	114O	115O	116X	117a	■	118A	119I	120F	121J	122G	123B	■	124J	125A	■	126Z	127U	128B
129a	■	130F	131A	132J	■	133O	134V	135W	136M	137D	138X	139E	140U	■	141A	142O	143H	144D	145W	146T	147E
148V	149P	150N	■	151O	152S	■	153O	154U	155S	■	156S	157R	158W	159A	160V	161K	162X	163E	164F	165J	166T
■	167K	168S	169A	■	170O	171N	■	172R	173J	174F	175A	176M	177W	■	178D	179Y	180G	181E	■	182F	183O
184W	185J	186F	■	187R	188Z	189V	190E	■	191W	■	192U	193F	194K	195I	196B	197O	198G	199T	200S	201O	202Z

MOVING?




5726893