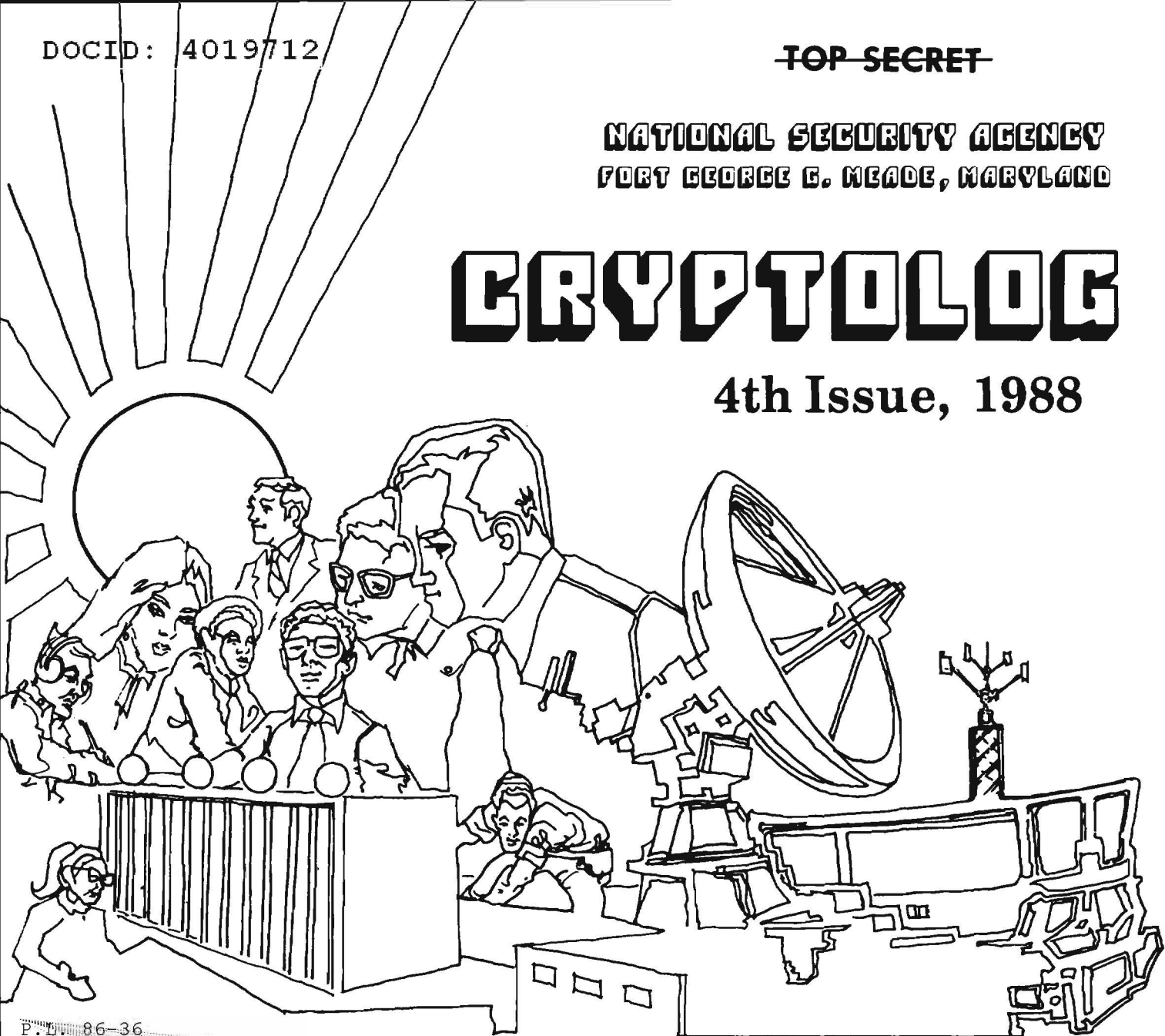


NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

4th Issue, 1988



P.T. 86-36

PROJECT RELOAD	[REDACTED]1
HOW TO MAKE A MORSE OP.	[REDACTED]5
BULLETIN BOARD	[REDACTED]6
LOTUS 1-2-3: A FANTASTIC RESEARCH TOOL	[REDACTED]7
THE NEW CRAYONS: AN ALLEGORY	[REDACTED]	12
RESUMES AND JOB APPLICATIONS	[REDACTED]	14
THE QUESTION OF LEADERSHIP	[REDACTED]	15
SCRIBE	[REDACTED]	17
SOFTWARE REVIEW: RIGHTWRITER	Leroy Ferguson	18
CONFERENCE REPORT: AMS CENTENNIAL CELEBRATION	David Harris	20
QUOTE WITHOUT COMMENT	28
LETTERS	28
FROM THE PAST	34
BONUS PUZZLE: MINICRYPTS	Bill Lutwiniak	35
NSA-CROSTIC (plus) No 67	[REDACTED]	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

P.L. 86-36

VOL. XV, No. 4..... 4th Issue 1988

PUBLISHER..... [redacted]

BOARD OF EDITORS

- Editor [redacted] (963-1103)
- Computer Systems [redacted] (963-1103)
- Cryptanalysis [redacted] (963-5238)
- Cryptolinguistics [redacted] (963-4740)
- Index [redacted] (963-4814)
- Information Science [redacted] (963-3456)
- Information Security [redacted] (972-2122)
- Language [redacted] (963-3057)
- Mathematics [redacted] (963-5566)
- Puzzles [redacted] (963-6430)
- Science and Technology [redacted] (963-4958)
- Special Research Vera R. Filby (968-5041)
- Traffic Analysis Robert J. Hanyok (963-4351)
- Illustrators [redacted] (963-4989)
- [redacted] (963-3738)
- [redacted] (963-6423)

NSA'S BLACK HOLES

A recent theory about the universe holds that there are little black holes, like worm holes, in our universe leading to other universes. It must be right. We have evidence right here at NSA.

There's one worm hole between Fort Meade and FANX. If we ever get into that universe we'll find reams of memos that never got to their destinations. There's another worm hole just outside of SAB 2 that captures bundles of CRYPTOLOGs on their way to the intended recipients. There's even one, just a pin prick, to be sure, between HQS building and Ops 1, that attracts proof sheets of CRYPTOLOG articles.

Strangest of all, NSA's black holes don't go in for junk mail. You know the kind, when every employee gets a memo (after the fact) stating that 25 December is a legal holiday. Curious, isn't it?

Of course, there are those who attribute the disappearance of mail to a virus, the same kind that affects the US Postal System.

We don't know which of the two is the right explanation for the missing mail. Or if there's still another cause. We hope that somebody can find out soon and do something about it.

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.

Tg.

Contents of CRYPTOLOG may not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

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.

PROJECT RELOAD



illustrated by the author

P.L. 86-36

P.L. 86-36

[Redacted] P04B

~~(FOUO)~~ Project RELOAD was launched in March of 1985 to improve the U.S. SIGINT System (USSS) support to national decision-makers and military commanders. This was to be done by upgrading the SIGINT production capabilities and missions of field sites, in particular those operated by the services. The initial objectives were to restore technical health in the field and to enhance analysis and reporting in the field, thus ensuring the wartime survivability of the USSS.

[Redacted]

(U) About the time the basic RELOAD Findings and Recommendations report was released, the results of three other major studies became known, and the recommendations cited therein significantly influenced the course of follow-on RELOAD actions. These studies are:

(U) In the earliest stages, the project concerned developing short-term solutions to site-specific endemic problems identified during field surveys made in late 1985 of 55 collection sites. These surveys gave mission management at the sites an opportunity to document their perceptions, problems, and needs. The findings formed the basis for, and provided the spirit upon which RELOAD strategies were subsequently built. Problems unique to each site were addressed by appropriate Agency elements which provided quick fixes to pressing problems. In fact, some 325 corrective actions were implemented by late 1986, resulting in some improvement in front-end production.

~~(FOUO)~~ A Study by the Director's Blue Ribbon Panel, consisting of high-level NSA executive-consultants. It reviewed the USSS in its entirety to determine the state of its technical health and its ability to accomplish its assigned mission now and in the future. It concluded that technical health in the field had to be strengthened; the practice of giving the military (the SCEs) virtually robotic tasks had to cease; and that NSA had to share the high tech duties with the field -- not just to enhance the field's capabilities, but to allow the time and talent of the NSA work force to be directed toward keeping up with the vast expansion taking place in all aspects of SIGINT. Systemic deficiencies were evident within NSA as well as in the field, for different reasons.

~~(G-000)~~ However, by the time the final RELOAD assessment was approved by the Director in April 1986, it became evident that certain problems in the USSS were systemic deficiencies requiring the development of long-term institutionalized solutions.

[Redacted]

~~(G-000)~~ The Future SIGINT Capabilities Study (FSCS) which examined the capability of the USSS to handle the rapidly increasing volume of signals in the environment as well as its ability to cope with our targets' advances in signals technology. It pointed out that the seriousness of the rapidly advancing technologies of our targets poses serious problems requiring strategic action if the USSS is to maintain superiority in intelligence

~~CONFIDENTIAL~~

gathering.

(U) Through all of this there has been a very vivid perception on the part of NSA, the field, and the SCEs that RELOAD has had, and continues to enjoy, the strong backing of DDO and the Director.

(U) The Director of NSA charged the key components and the SCE commanders with identifying specific people to work with the RELOAD Project Management Office to implement the findings and recommendations of the various studies. A tiger team approach was selected, as the effort is and will continue to be a corporate one. The players involved are DDR, DDT, DDA, ADT, DDO (A, B, G, P, and W), CMC, ESC, INSCOM, and NSG.

~~(C)~~ The working groups chosen to meet and implement near-term (less than a year), mid-term (two to five years), and long range (beyond five years) solutions to the issues have contributed immeasurably to the accomplishments of RELOAD, as have the innovative suggestions of field sites. The SCE HQ are represented on *all* working groups, with the Cryptologic Manning, Collection, and Processing Working Groups actually being chaired by INSCOM, ESC, and NSG representatives, respectively. RELOAD is broader than just the working groups and the initiatives do not come from the working groups alone. Nor do initiatives come just from the SCE Headquarters; they can come from any element in the process, and often spring from the field sites themselves. RELOAD has brought about a better bonding between the front end and the back end of the system with the common goal of doing it more efficiently and effectively.

FOLLOW-ON ACTION

(U) Because three of the four studies focused on operational matters under the Operations Directorate, it seemed reasonable that follow-on action should be undertaken by that Key Component. Since Project RELOAD had done so much on the study initially and was most familiar with the problems, it was given the corporate go-ahead to attack the systemic problems plaguing the system. The nature and breadth of the RELOAD program changed drastically as it shifted from problem study to problem solving. The reconfiguration and modernization of the entire USSS seemed to be necessary. Consequently, the scope of Project RELOAD has expanded, as has the original list of systemic issues.

(U) RELOAD continues to use quick-fixes to problems wherever practical, but is following up with long-term corporate (NSA-SCE) institutionalized programs, serving as the means by which organizations are brought together to fix their own problems. It provides the forum and the opportunity through the working groups to actively pursue solutions to problems with the RELOAD banner serving as the driving force. A corporate entity has been created in which all of the parts recognize essentially one goal: to equip and to educate the work force to acquire the skills required to cope with the challenges of tomorrow.

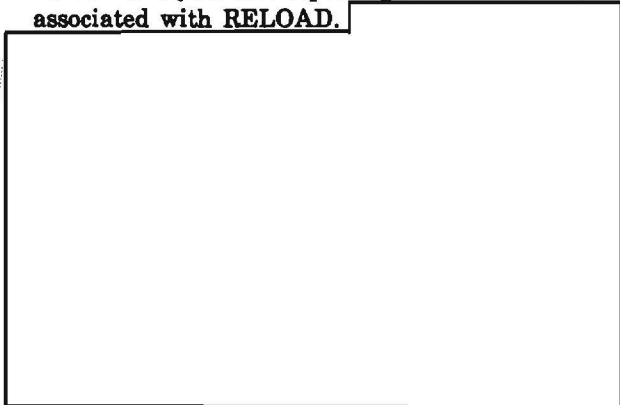
~~(C)~~ By the end of 1987, RELOAD had blossomed into a widespread brainstorming

~~CONFIDENTIAL~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CONFIDENTIAL~~

effort with fresh ideas emanating from many NSA and SCE sources. The effort has already yielded some degree of improved field technical health, has upgraded target assessment and reporting, and has made genuine progress toward expanded front-end crisis response and self-sufficiency capabilities. The emphasis continues to focus on improving technical health through enhancing the skills of the work force. As a consequence, certain RELOAD initiatives traverse the entire USSS, and impact on both the military and civilian work forces. The achievements recorded in 1987 are many and attributable to the hard work, vision, and cooperative efforts of numerous personnel at various field and headquarters elements.

~~(S)~~ During the past year, the technical health concerns and issues documented in the RELOAD findings report of April 1986 drew the corporate working groups that were examining the topics into a scope beyond the narrow analysis and reporting structure earlier associated with RELOAD.

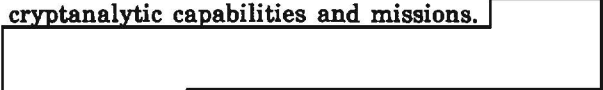


(U) The present scope of RELOAD actions becomes evident from the following summary of highlights:

~~(S)~~ Traffic Analysis - The focus has been on increased training, responsibilities, and documentation. Site technical exploitation initiatives are flourishing. Corporate skill standards have been introduced to assist the training and assignment processes and major revisions to existing career pathing and development schemes are under consideration. The traffic analysis and SIGINT reporting skill standards were subsequently combined into a SIGINT analyst skill standard. Certain field sites have assumed increased target responsibilities and new technical studies (e.g., ITNs) are resulting. Mission managers are refocusing duties to capitalize on available experience and skills and as a consequence

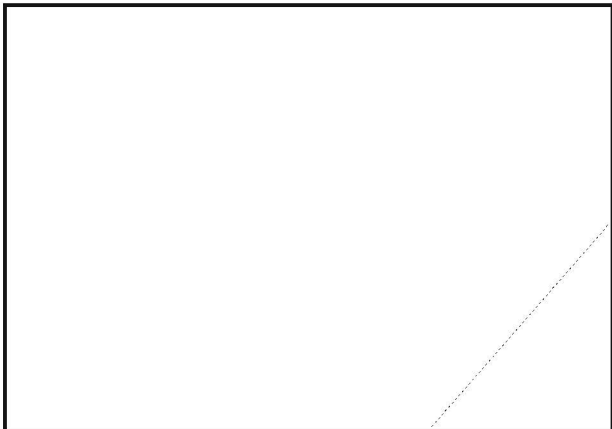
analytic proficiency is on the rise. A working group TA Focus Plan calling for a broad range of reforms to strengthen career field/discipline mechanisms is in final coordination and appears to have overall management/command backing.

~~(S)~~ Cryptanalysis - A host of SCE field stations have now reacquired basic cryptanalytic capabilities and missions.



Two courses were conducted to teach cryptanalytic techniques and acquaint analysts with target cryptanalytic histories and profiles. Stations have been given appropriate software and data base access where possible to aid local exploitation efforts. Early results are most promising. Productivity at some sites has markedly increased, processes producing monthly keys for some targets have been accelerated, and most important, local target identification and warning methods have been upgraded.

~~(S)~~ ADP/Data Bases - One achievement in this area has been the development of a means for all sites to request access to data bases, by approaching one office (T52) with their justification. Group A has developed and fielded procedures to provide access to information requested, which also satisfy need-to-know controls. This system will now be applied to other data bases, and made applicable to more field sites. Access to data bases from field sites will remain a function of the capacity for communications paths to support it. Other aspects being worked are a directory of information managed by T52 which can deliver a listing of data bases, provided by target offices, designated for access to field sites, and an up-to-date listing of software that has been developed either in NSA or in the field and is available for acquisition.



~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

[Redacted]

[Redacted]

[Redacted]

(U) **Manning** - With the aim of getting better skills-to-job matches, the SCE HQs are now geared to push their current manpower systems to the maximum. One universal method employed was the drafting of better job skill requirements statements and the rollover of these expressions into TDs. Also to be employed in this process will be the RELOAD-drafted and corporately approved three-tier skill standards. Attention is being devoted to tracking and assigning skilled personnel including the addition of trailers to occupational codes to identify specially trained and uniquely capable personnel. Most important, SCE managers are striving to implement improved career pathing schemes to enhance the cryptologic development of personnel; NSG's A & R plan is a trend setting example.

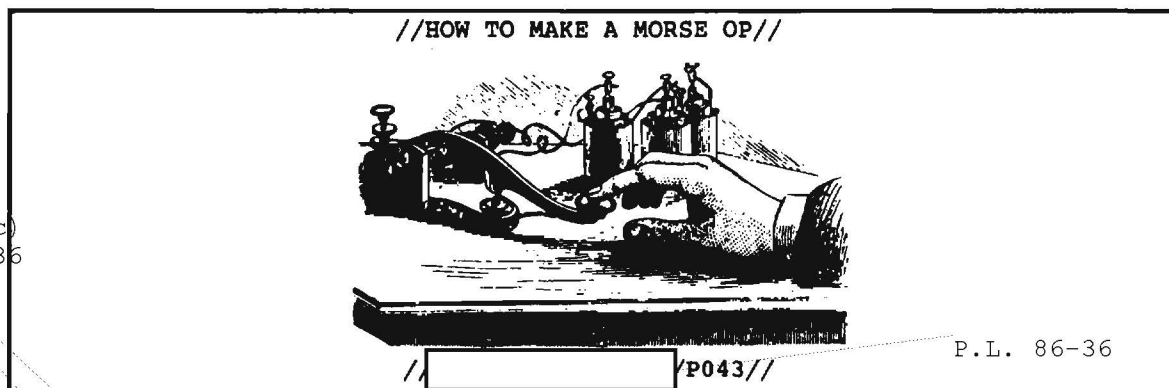
(U) **Language** - This newly established corporate working group has established as its goal a commitment by managers to fix long-standing problems in proficiency, maintenance, retention, assignments, and training. It held its first meeting in December 1987 and will interact with SCE and NSA management to gather essential information to form a baseline of existing linguistic proficiencies from which to build realistic requirements that will lead to improved language competencies in the field and at NSA.

(U) The challenges of the combined studies have driven what has been done under RELOAD and continue to direct what is yet to be accomplished. The Field Stations and SCE HQ are most enthusiastic and have been the key players since the results of the initial site surveys developed into positive actions. The producer community is now convinced that RELOAD is not just a fad that will go away. The front-loading effected by RELOAD will continue; it will continue because there is now an understanding of the scope of the problems and an understanding of what must be accomplished under the umbrella of RELOAD. The concerted effort includes reaching outside the USSS to obtain reviews and reconsiderations of procedures affecting the very heart of SCE skill acquisition and maintenance, to wit, training and assignment.

~~(S-CCO)~~ **Processing** - The main thrust in this area was to make collectors cognizant of why certain signals were important and what the plans and strategies were for future field exploitation

[Redacted]

SECRET



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

~~(S-CCO)~~ NSA was asked to prepare SIGINT training [REDACTED] several years ago. The OPI, [REDACTED] solicited input from several sources for material and training, including E23 (now E54) for help with training new Morse operators. The following is based on a memo prepared by one of my NCS colleagues at the time and to which I contributed. We never learned whether our recommendations were adopted or used. But we think it worthwhile to publish our findings on what it takes to make a Morse operator. The statistics and conclusions are based on our experience at NCS in training morse operators.

THE RECOMMENDED PLAN

(U) It usually takes a Morse operator trainee approximately twenty weeks to achieve a code copying speed of twenty groups per minute. (This is not full time -- not all of the 800 hours are spent copying code.) To achieve 13 GPM usually takes about 165 hours.

(U) The usual progression for a Morse trainee is that after about 110 hours the average student can copy eight groups per minute. From this level, the student will progress rapidly, usually attaining 13 to 15 GPM after an additional sixty hours of work. At this point a plateau is reached, after which it will take another 150 hours of copy to progress to 18 GPM. By the term "plateau," we mean the level at which the student can copy at his highest speed accurately and with relatively little trouble. The next higher speed, on the other hand, seems to present the student with an inordinate amount of trouble. That is, at the plateau the error rate will be at or under 2%, while the error rate at the next higher speed usually starts at about 15% and gradually diminishes. The plateau speed

varies from student to student, but as we said above, it usually ranges from 13 to 15 GPM.

(U) This plateau is apparently the transition point at which Morse code copying becomes a psycho-motor response rather than a cognitive translation of the sounds to symbols. After the transition is made, code speed acquisition again rises steeply with a gradual flattening of the curve as the natural limits of the students' abilities are approached. It will take approximately 400 to 500 hours of copying Morse for an average student to attain a code speed of 20 GPM.

~~(C)~~ In designing a course for an intercept operator, material other than morse copying of course is taught. In designing a course combining Morse training with the academic material required, we recommend that the subject matter is scheduled so that the first two weeks are devoted to learning the Morse alphabet. After this, most of the time should be spent on the academic material, gradually increasing the amount of time spent on Morse until the final weeks, when copying Morse is full time. The conditions under which the students work, particularly during the last weeks, should be as realistic as possible. This could be accomplished by introducing recordings of actual target transmissions, or perhaps by assigning the student an actual mission which is duplicated on cover.

(U) Morse learning is a very individual thing with students progressing at different rates, reaching their plateaus at different code speeds, spending different amounts of time on their plateaus, and so forth. A student who appears to exhibit good potential, then, should not be dropped for failure to achieve average progress.

SECRET

~~HANDLE VIA COMINT CHANNELS~~

~~SECRET~~

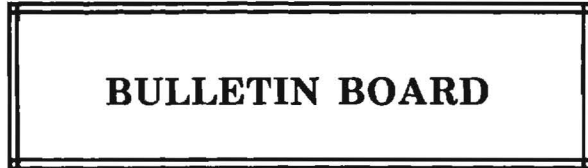
(U) One feature of Morse is that accurate copy is much easier if (and when) the student learns to stay behind the character being sent. Three to five characters behind is what the average high speed operator manages, but accuracy is nearly impossible if the operator is working right on top of the character being sent. This should be stressed by the instructors from the time the students have mastered the alphabet all the way through the course.

effort on operational material and the rest either speed work, if still needed, or introduction to other alphabets.

(U) From a training perspective, it will take twenty weeks or more to make a Morse operator. Most people will tell you that at least a year actually doing the work is necessary to produce a competent operator, but that's another story that can be told some other time.

SUGGESTED TIMETABLE

(U) The end of week nine, by which time the students would have had 159 hours of Morse training most of the students should be working on 15 GPM or thereabouts. Whatever speed they are on, it is likely that most, if not all, will be at their plateau level. Here is the time to start to bear down and increase the time spent in the training day on Morse.



UNIX BROWN BAG SEMINARS

~~(C)~~ The end of week fourteen, after approximately 300 hours of Morse training, striving to achieve higher code speeds will be getting old. A break here will, in some cases, provide better results in the long run and in most other cases make little or no difference. That is, there is a good chance or benefit and little chance of loss by taking a break from the Morse at this point. The next two weeks, we recommend, should be devoted to classroom training in intercept procedures. When Morse training is resumed after that, all appropriate logging and copying formats should be incorporated.

~~(FOUO)~~ At the February session of the brown bag seminars on UNIX sponsored by CRYSCOM, [redacted] CRI/T335, will speak on [redacted] analogies and CA applications. In March [redacted] T335, will give details on data configuration using SCCS/MAKE, especially in regard to the UNIX/UNICOS Software Exchange Proposal. Date, time and place for the February and March meetings will be announced later. For further information please call or write the CRYSCOM Exec, [redacted] Ops 1, P13, 963-3405.

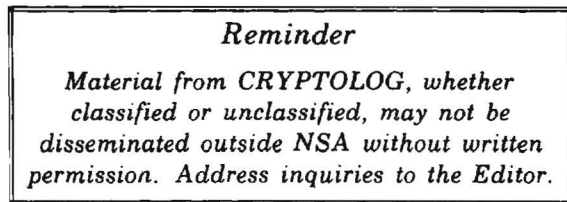
CRYSCO '89

P.L. 86-36

(U) By the end of week 18, some 330 to 350 hours of Morse training will have been given.

~~(FOUO)~~ Planning for CRYSCO '89 is underway. The sessions will take place the week of 19 June in HQS 9A135, the Old Director's Conference Room. Suggestions for topics are solicited. Contact one of these people: [redacted] CRYSCO '89 Chairman, 968-8141; [redacted] CRYSCOM Exec, 963-3045, or [redacted] CRYSCOM Chairman, 963-4681.

~~(S-CCO)~~ Starting with week 19 or thereabouts, code speed practice should be interspersed with recording or target activity or, if resources are available, [redacted]. Additionally, students who have achieved the required code speed and are apparently gifted operators can be introduced to barred letters and special characters beyond what they will have learned as routine. [redacted]



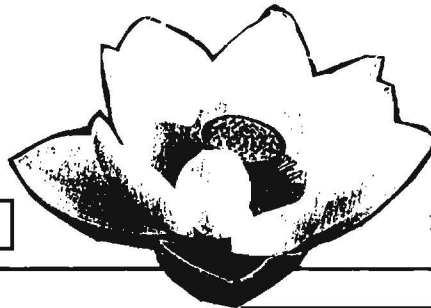
(U) The remainder of the course, probably through the 23rd week or beyond, should be full-time Morse with about two-thirds of the

Lotus 1-2-3: A Fantastic Research and Intelligence Tool

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

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

P.L. 86-36



P3 Technical Assistant

~~(C)~~ Lotus 1-2-3 is a commercial software package its creators say was designed for accounting and financial analysis. But its integrated spreadsheet, database, and graphics components also make it an ideal piece of software that can be used in the Agency by traffic analysts (net identification, analysis, and query counting), engineers, mathematicians, typists, and managers.

[Redacted]

(U) Since Lotus is an integrated package, any menu option can be used either independently or together with other options on the same data.

IMPORTING DATA INTO LOTUS FOR DATABASE OR MAP DISPLAY PURPOSES

[Redacted]

Its ready availability on IBM PCs, XTs, and ATs that are widely distributed throughout the agency, the low cost, and compatibility with new upgrades of Lotus make it a cost-effective analyst's tool, especially welcome in these days of tight budgets.

~~(FOUO)~~ Lotus can import into its spreadsheet any ASCII textual or numeric file from any Agency database if it has 240 characters or fewer on a line and can be stored on a diskette. That means that reports from the field with mixed narrative and tabular information can be processed through LOTUS to pull the tabular information together. Then that tabular information can be parsed, as required, by any parameter. The parsed results can then be sorted by any parameter or saved to another file for database querying.

(U) The menu options include:

▶ **FILE IMPORT-** Inputs to a Lotus spreadsheet any ASCII numeric or textual file up to 240 characters per line; inputs to other spreadsheet files (DBII & DBIII, Visicalc, word processor files).

(U) If new reports require similar parsing, you need set up only one parse line, store it, and use it for the new data. Once all the necessary data are extracted and stored on separate files, these files can be read back into the spreadsheet, and combined and sorted as a single file. The data can also be queried for specific criteria and the data matching the criteria can be extracted for any purpose, such as input to the Lotus map display spreadsheet.

▶ **PARSING-** Allows user to separate any line(s) of text into separate columns of numeric or alphanumeric characters. The parsing line can be stored for reuse on new data.

PARSING

▶ **DATABASE-** Allows sorting of columns and rows of data; permits querying the database using criteria to extract information.

~~(FOUO)~~ If you have old alphanumeric textual files you've created with a word processor or on a terminal such as COASTLINE and you want to create a database without retyping the data, Lotus parsing is for you. Figure 1 shows how

▶ **STATISTICS-** Finds sums, averages, and standard deviations for data entered into the spreadsheet.

▶ **GRAPHICS-** Displays Bar, Pie, Line, XY plots on the screen using spreadsheet-entered data; [Redacted]

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

parsing works on a message where the parameters are separated by / marks, and zulu time, latitude and longitude are wanted for the database.

(U) Lotus tries to up a parse line (first line in Figure 1) where L=label, * = space, and >

means continue the label until a new symbol appears. If the parse line doesn't meet your criteria, you may modify it, as shown in Figure 2 where S in the parse line = space. Lotus then parses the data automatically and lets you store the parsed data anywhere you want on the spreadsheet, as in Figure 3.



Fig. 1. Original Parse Line and Data

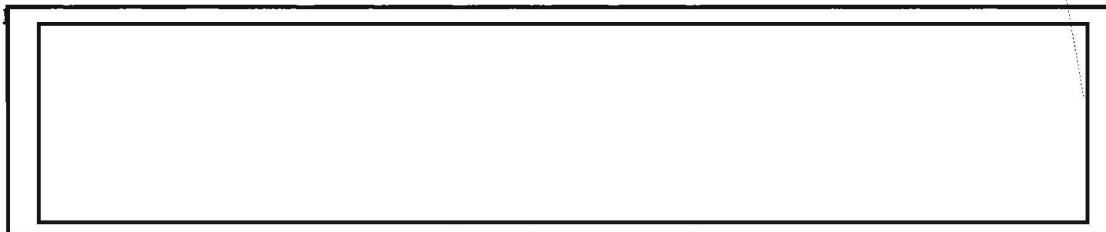


Fig 2. Modified Parse Line and Data

(U) The data in Figure 3 is arranged in three columns and can now be sorted using Lotus' database sort option, combined with another file having similar data previously extracted the same way, or input to my Lotus Elint Display spreadsheet for plotting.



Fig. 4. Database

(U) In Figure 5 the database is sorted with the "from" column as primary sort.



**DATABASE SORT AND QUERY
AND DATA TABLE SETUP TO COUNT
DATABASE DATA**

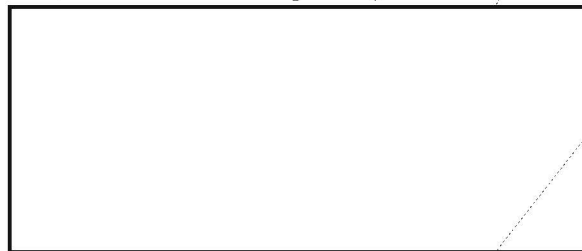
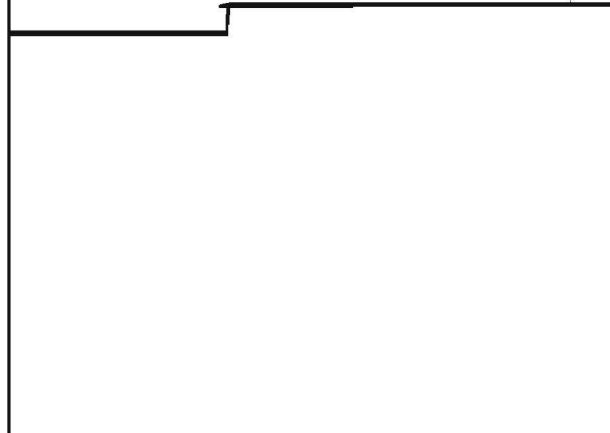
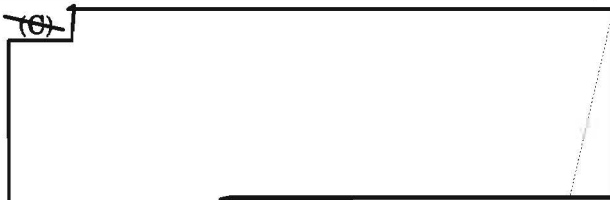


Fig 5. Database of Fig. 4 sorted by "from" as Primary column and "to" as Secondary column.

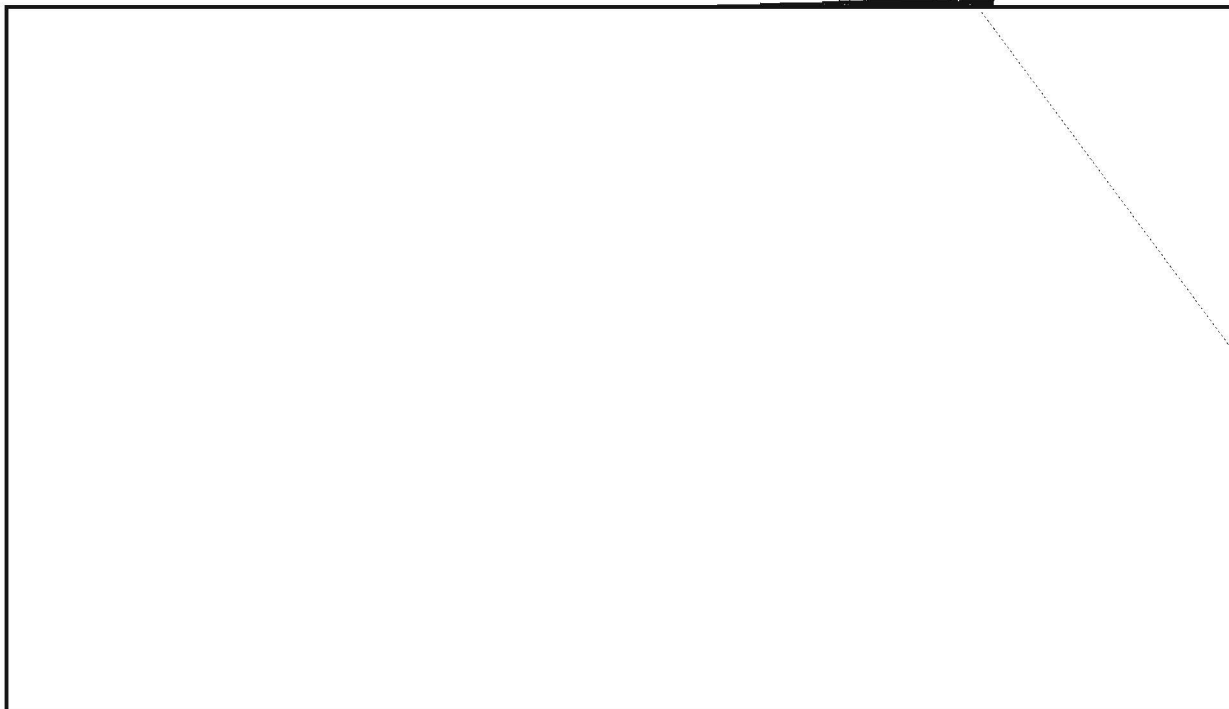
(U) Figures 6 and 6a show how the database is queried for information. Lotus requires setting up a criteria and output header with the same titles as those for the database. Criteria are input in the criteria line for any of these header parameters. Results matching the criteria are then displayed on the output lines.





(U) These steps are continued for all parameters in the Data Table until it is filled. Analysts can then scan the Data Table to determine who talks to whom and how many times, thus establishing relationships very easily.

~~(C-CCO)~~ I have just touched the surface of what Lotus can do. For example, curve-fitting techniques can be developed on a spreadsheet, and the input curve to be matched displayed together with the calculated curve; message editing hard to do on Coastline can be input to Lotus where paragraph-justifying can be easily done and the results passed back as a Coastline file. Files too large to transmit to a

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

field site via Coastline can first be read into Lotus, split into segments and then transmitted via Coastline. At the field site the segmented files are read back into Lotus, recombined, and saved as the original file.

(U) It is also possible to convert any program binary file into an ASCII hexadecimal file, split the file into segments, and transmit it to the field site. The field site then recombines the file in Lotus and reconverts it to a binary file and uses the program. This saves sending new application programs by mail to the field.

~~(FOUO)~~ The field can also transmit programs not working correctly to NSA where they can be analyzed and transmitted back. This saves mailing time (usually 3 weeks per mailing), updating time, and uptime for using the program. Bar, pie, line or XY charts can be developed in a spreadsheet, displayed, and plotted. The data for these charts could be imported from a diskette, keyed in by hand,

extracted from a query from a database setup in the spreadsheet or a sort of the data, or entered from a parsed message.

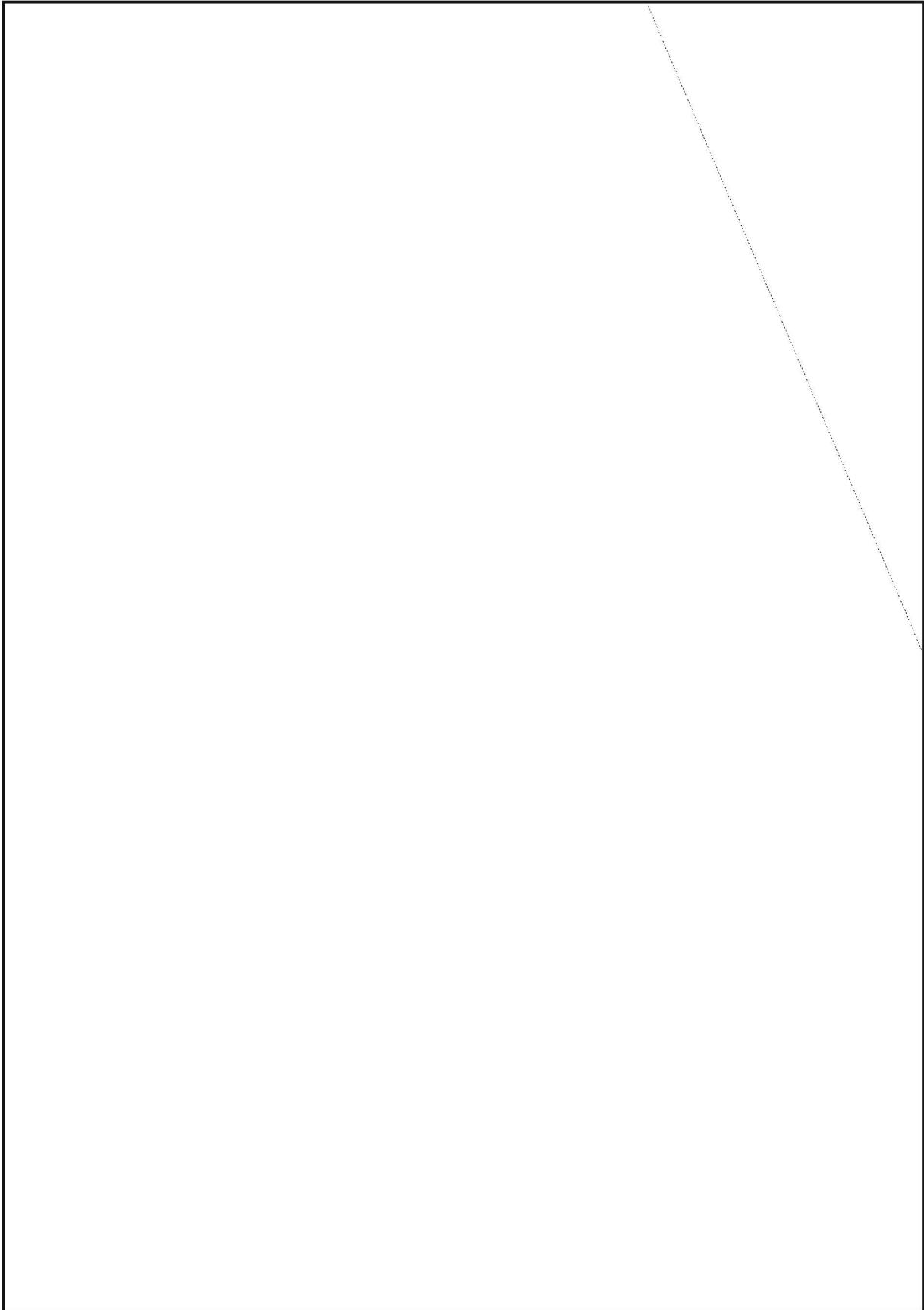
(U) In summary, this article shows that Lotus can handle many intelligence chores without special programming. Before your organization buys sophisticated hardware or software to accomplish a task, check into Lotus spreadsheet capabilities. You'll be surprised at the power available. Try it...you'll like it.

Editor's Note:

We are advised that ASPIC has replaced Lotus 1-2-3 as the standard spreadsheet software with SuperCalc4, but the latter does not have parsing capability and lacks other features necessary for the applications described in this article. Lotus 1-2-3 can still be ordered as non-standard software with justification.

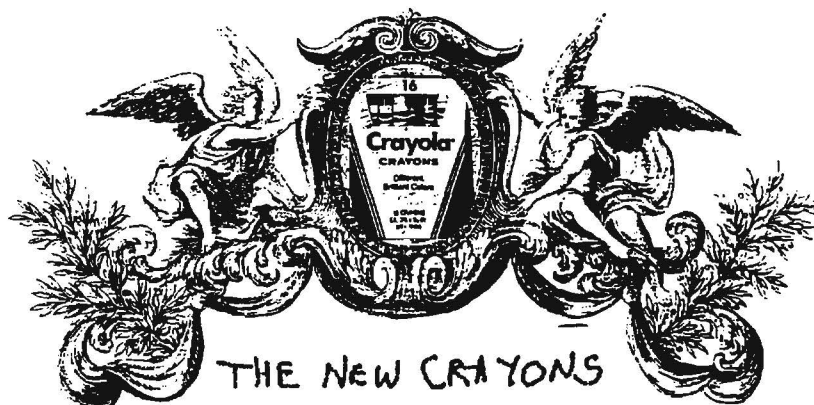
~~CONFIDENTIAL~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CONFIDENTIAL~~



~~CONFIDENTIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

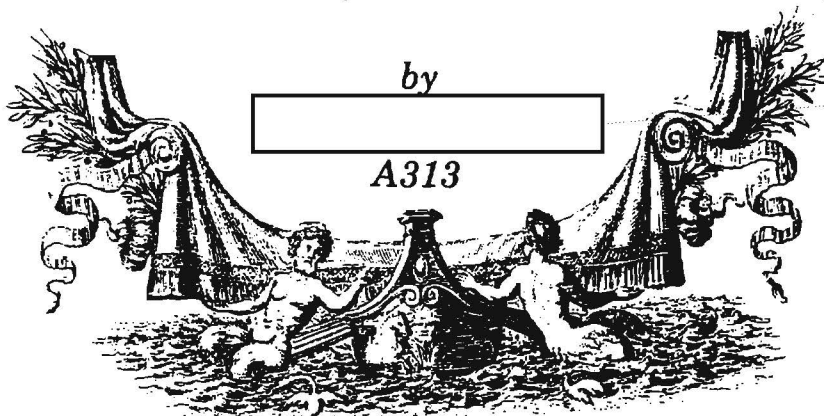


Once upon a time there was a special school for young artists. Only the most promising students were allowed to attend. The school had several boxes of crayons for them to use. Each box contained eight fine colors. The school did not have enough boxes to give one to each student, so the children had to share. But most of the time that was okay. While they were waiting for their turn to use the crayons, they could rub their drawings with tissues to make them look smoother, or they could think about what they would draw next. Sometimes they wished they could have more crayons, but they managed to make do. The children learned to make wonderful pictures with their simple tools, and people began to come to look at their masterpieces hanging in the school's own gallery.

The schoolmaster was very proud of the gallery. He wanted to help the students produce more and better drawings for the visitors to admire. So he decided that each child should have his own box of crayons. He arranged to buy more. The new crayons would be thinner, so the young artists could draw finer lines. There would also be 16 colors in each box, so the children's pictures could be even more wonderful than before. These new, improved crayons were expensive, so the schoolmaster could buy only a few boxes at a time. But nobody worried too much because they knew that one day everybody would have his own.

When the new crayons began to arrive, the children discovered that the boxes had room for 16 crayons, but two colors were missing from each box. The crayon makers had not yet been able to make new, improved versions of blue and purple crayons. But they promised to make them soon and send them to the school.

As the months went by, the students were given more of the new crayons. Finally, there was one box for each student. Some had the old ones, and some had the new. The new 16-color boxes still had no blue nor purple. So the children with new crayons had to borrow the old ones when they wanted to use blue or purple in their pictures. The children with old crayons had to borrow the new ones so they could



P.L. 86-36



draw finer lines and use some of the fancy colors. The new, improved, thin crayons were easier to break, so everyone had to be more careful. And, of course, everybody had more crayon sharpening to do.

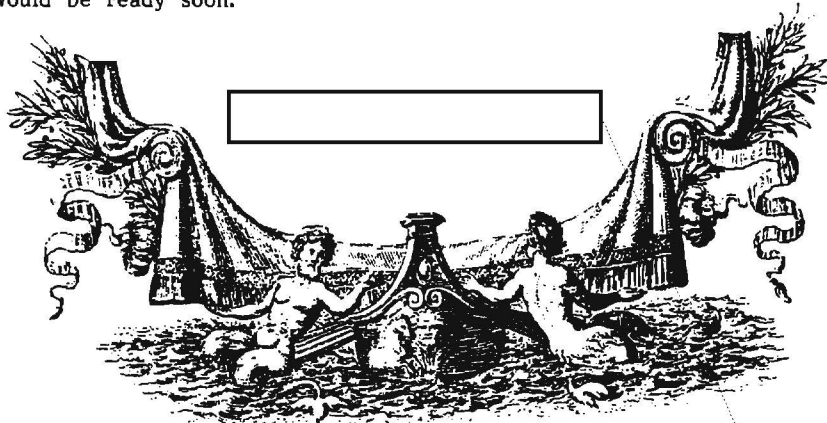
The schoolmaster declared, "Now that we have one box of crayons for each student, you can draw more pictures faster to hang in our gallery."

"No," the children explained, "We cannot. We do not really have enough crayons for everybody to use at once. We still have to share. We also must spend more time taking care of the crayons."

The schoolmaster thought the children were ungrateful and greedy. He refused to buy any more new crayons unless the children agreed to trade in the old ones. He did not want to make the school board angry by having more boxes of crayons than there were children in his classrooms. But the children insisted that they could not give up the old crayons because they needed blue and purple to complete their pictures.

Soon the children were spending less time drawing and more time trying to explain their crayon needs. Yet the schoolmaster would not change his mind: the boxes of crayons must not outnumber the children. But he promised to provide new, improved blue and purple crayons, even if he had to make them himself; then they would no longer need the old ones. The children were not convinced, but agreed that it would be just fine if he could really do it. Then they could see about getting a complete set of new, improved crayons for everybody. They just wanted to make sure they had the new blue and purple crayons before giving up the old ones.

Meanwhile, the crayon salesman said that there would soon be no more 16-color boxes of crayons. Instead, he would be selling boxes of newer, more improved crayons in 24 colors. Well, at least there would be room for that many. The crayon experts were still working on the red and orange ones, but the salesman assured everyone that these would be ready soon.



P. L. 86-36

**RESUMES and
JOB
APPLICATIONS**



▶ Office symbols and organizational designators

Also, although the terms COMINT, ELINT, SIGINT, etc., when associated with NSA are considered FOUO, you must be careful when associating them with job titles, duties and performed functions.

As stated elsewhere, indications of one's foreign language capability in connection with NSA duties are considered classified; this creates problems in writing a resume. Association with languages in an academic or training context is permitted, but specific languages should be listed only in the academic section of the resume. Specific foreign language ability, e.g., native speaker, self-taught, etc. should be listed only in the summary of qualifications or miscellaneous section. You may show any and all language training courses as unclassified. You may not associate your language capability with the duties of your position.

During our employment with the National Security Agency, many of us will prepare or have already prepared, one or more resumes or job summaries in which we must explain, in unclassified language, what we have done and are doing on the job at NSA. This often is a difficult task, since much of what we handle tends to be classified.

All resumes, detailed job applications, student co-op reports and the like must be reviewed and approved for release as unclassified. The Classification Advisory Officers (CAO's) throughout NSA have been authorized by Q43 to review and release these resumes, applications, and reports. The five CAO's within the Operations Directorate are listed at the end of this article.

Any document intended for public release, such as a resume, may not contain classified information. The following additional information also may not be released:

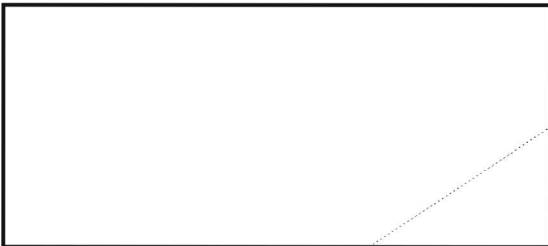
- ▶ NSA missions and functions
- ▶ Employee names (names of supervisors are releasable; employee character references should not be attributed to NSA employment, but to U.S. Government employment.)
- ▶ Project names and covernames
- ▶ Salaries (other than the originator's)
- ▶ Number of people employed by NSA

As far as clearances are concerned, you may indicate that you are cleared for TOP SECRET Special Intelligence (TS/SI) without further elaboration or detail. You may not include any additional specific accesses. Revealing that you hold a TS/SI clearance may actually be helpful, even if the position sought may not require a clearance. The fact that the government granted the clearance speaks well for the honesty and integrity of the applicant.

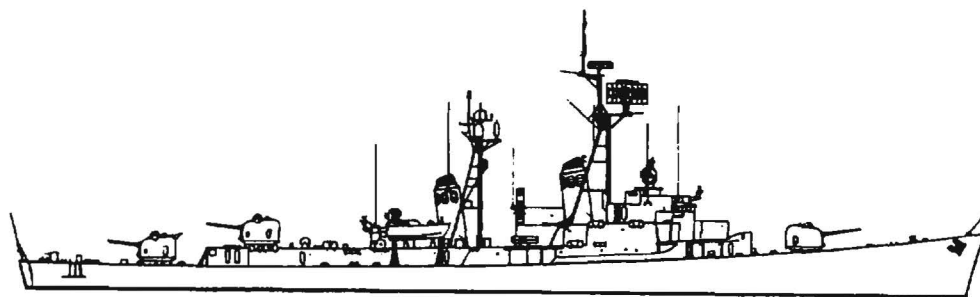
The following is an updated listing of the Classification Advisory Officers (CAO's) within the Operations Directorate. Please contact the appropriate CAO whenever any assistance is desired or needed concerning proper classification of information or materials, or for review and release of a resume, applications, etc.



▶ B/CAO Dick Sylvester, B03, 4053s
2S010-2



THE QUESTION OF LEADERSHIP



P16

P.L. 86-36

~~(FOUO)~~ During the early 1950's I was assigned to the staff of Commander, North Atlantic and Mediterranean for duty with Communications Unit 32D (COMUNIT 32D). I was assigned to various destroyer division staffs where I taught ELINT countermeasures to radiomen and radar operators aboard three different destroyers. All three destroyers had similar missions and almost identical manning.

(U) At that time Greece and Turkey were going through a very unsettled period, so one mission assigned to the Navy was to show the flag in Greek and Turkish ports - usually spending three to five days in a port or lying offshore before moving on to the next. Observing the difference that leadership made on the effectiveness of officers and crew in carrying out their missions gave me some insights into the practical effects of leadership. It may have been only coincidence that leadership varied so much from one ship to another, but the magnitude of variation made the picture very clear.

(U) Taking the leadership of the first destroyer (USS *GYATT*) as a baseline, the officers and crew seemed to be of average competence, and morale was about average for ships in the Mediterranean at that time. Command reacted to problems of training and morale rather than anticipating and controlling them. Reaction was quick enough to avoid major problems, and well guided enough to get the job done.

(U) The Commanding Officer (CO) was not known by the average crew member except as an authority figure. He relayed all instructions

and commands through his Executive Officer and down the chain of command. That is the norm throughout the Navy, and works well when exercises are large and diverse enough to leave little slack time. It does not work as well when a great deal of time is left unoccupied, while supplies are at low levels from lack of replenishment opportunities, and recreational facilities during port calls are minimal.

(U) The second destroyer was USS *OHARE*, which we boarded in Gibraltar where she arrived after a stormy Atlantic crossing during which an accompanying destroyer was overrun and sunk by an aircraft carrier. Our small detachment was very favorably impressed on our first visit to USS *OHARE* to survey our working spaces. The crewmembers on the Quarterdeck (the area aboard the ship at the end of the gangway) were noticeably sharper and more courteous, and the ship was cleaner and in better repair than *GYATT*, in spite of the rough crossing.

~~(FOUO)~~ We left Gibraltar and returned immediately to the Eastern Mediterranean. On the day before our first port call in Greece aboard *OHARE*, the CO mustered all hands on the fantail (the open stern of the ship) and delivered an interesting talk on the area that included local points of interest as well as historical highlights and a brief on local customs. He emphasized the point that we (the crew) were to be ambassadors of good will, and desired that we make a good impression on the local population. He saw to it that sightseeing

tours were organized for those interested in them, and arranged for sporting events (softball and soccer) for others. The difference in crew conduct ashore and in our (COMUNIT 32D) perceptions of this port were radically different from our two visits aboard *GYATT*.

(U) During that visit and subsequent ones to other Greek and Turkish ports, all preceded by talks delivered by the CO or another of the officers. I do not recall a single serious breach of discipline. We had been used to seeing at least a few fights and/or drunk and disorderly incidents on previous visits of *GYATT*. We soon became aware also, of the reason that the ship was in such good repair and clean condition. The CO and his officers had fostered a spirit of friendly competition between the two leading Boatswains Mates (those Petty Officers responsible for repair, upkeep, and seamanship) which resulted in fast, efficient repair and cleaning of anything in their areas of responsibility. A spirit of pride in their work and friendly cooperation existed among the other departments of the ship also, resulting in the award of several E's (official awards for excellence) to the ship.

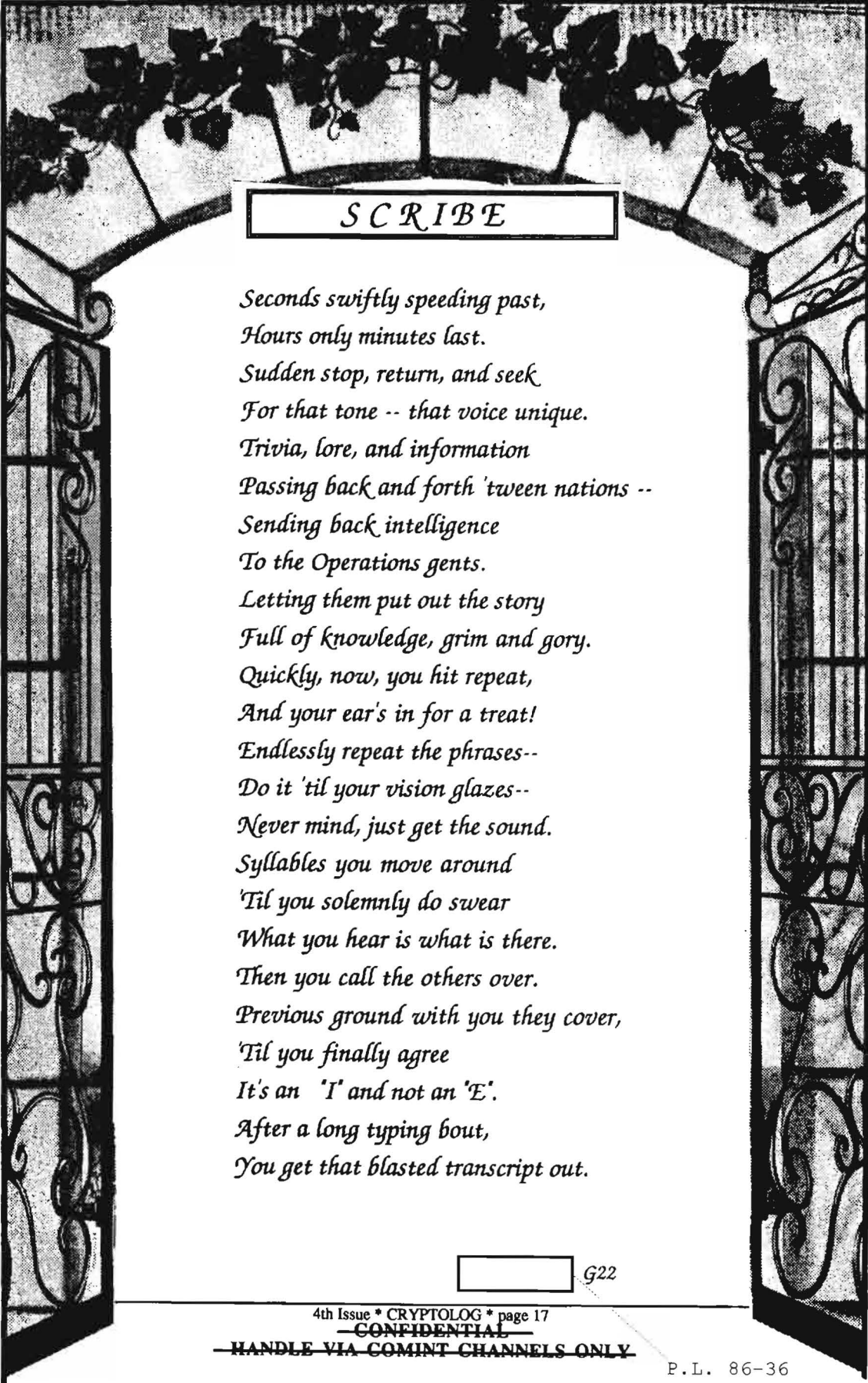
(U) After such an enjoyable tour aboard *OHARE*, we were ill-prepared for our introduction to USS *KNAPP* on a miserable, rainy day in Plymouth, England. The *KNAPP* sent a whaleboat to pick up our unit, and when the Coxswain (the Petty Officer in charge of the whaleboat) discovered that he was to take aboard equipment as well as crew, he refused to do so. After some discussion with *OHARE*'s Officer of the Deck, he agreed to take both equipment and crew, but we were offered no help in loading or unloading. When we finally got aboard *KNAPP*, we found that our assigned work spaces had no usable antenna connections, and the antennas that had been installed some time before were not in operating condition. We had to do all of the repair and installations ourselves.

(U) It came as no great surprise after that to see the large number of crewmen returning aboard drunk from liberty in Plymouth, and other places later. There was rivalry between factions of the crew of *KNAPP*, but it was not the friendly rivalry we had observed in *OHARE*; *KNAPP*'s crew often were involved in drunken brawls between factions.

(U) I cannot recall ever having seen the *KNAPP*'s CO, but his reputation was well known to all of the crew. He was said to prefer drinking with some enlisted crewmembers to spending time with his officers, by whom he was not well regarded. He was alleged to have been arrested for drunken driving by Military Police in Rome, where he had driven a jeep which had been assigned to *KNAPP* from a Navy motor pool in Trieste for use by ship's officers. It seemed to us in COMUNIT 32D that the poor crew discipline and *KNAPP*'s generally rundown appearance and condition were a direct result of the negative influence of the CO.

(U) Differences in leadership in the three destroyers was also evident from the examples of seamanship that we observed while aboard. *GYATT* was generally competent, and did a good job of maintaining station and maneuvering during exercises and while coming alongside a tender or tying up to a dock or pier. *OHARE*'s crew distinguished themselves by the precision of her movements, whether maneuvering in restricted waterways or tying up to a dock in tricky winds and tides. *KNAPP* generally was able to maneuver competently under favorable conditions, but her crew was not able to deal well with unfavorable circumstances.

(U) One remarkable example illustrates the great difference between *OHARE* and *KNAPP* - the ships with the two most widely different commanders. Both spent two weeks in a course at the Antisubmarine Warfare School in the Foyle River near Londonderry, Ireland. During the course, each had to refuel at the dock in the Foyle River. The river at that point is rather narrow and the current swift. The maneuver required an upstream approach, a 180-degree turn, and ended with coming alongside the fuel dock from upstream. *OHARE* made the upstream approach and dropped her port anchor when about two ship-lengths upstream of the fuel dock, reversed one engine and swung around the anchor (like a child around a lamp post) and ended in perfect position to back upstream against the dock. *KNAPP* made her upstream approach and turned without using her anchor, which left her drifting into the fuel dock as she attempted to back alongside. Irish linehandlers on the dock were forced to scramble quickly to avoid *KNAPP* as she tore up six to ten feet of the pier before stopping. □

~~CONFIDENTIAL~~


S C R I B E

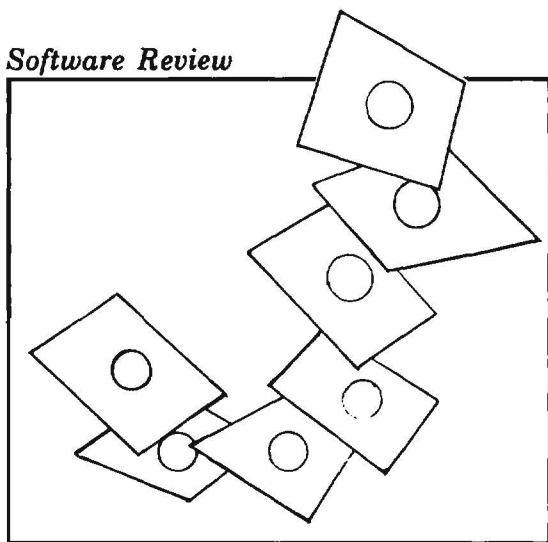
*Seconds swiftly speeding past,
Hours only minutes last.
Sudden stop, return, and seek
For that tone -- that voice unique.
Trivia, lore, and information
Passing back and forth 'tween nations --
Sending back intelligence
To the Operations gents.
Letting them put out the story
Full of knowledge, grim and gory.
Quickly, now, you hit repeat,
And your ear's in for a treat!
Endlessly repeat the phrases--
Do it 'til your vision glazes--
Never mind, just get the sound.
Syllables you move around
'Til you solemnly do swear
What you hear is what is there.
Then you call the others over.
Previous ground with you they cover,
'Til you finally agree
It's an 'I' and not an 'E'.
After a long typing bout,
You get that blasted transcript out.*

G22

4th Issue * CRYPTOLOG * page 17

~~CONFIDENTIAL~~~~HANDLE VIA COMINT CHANNELS ONLY~~

Software Review



RIGHTWRITER, by Rightsoft, Inc. 2033 Wood Street, Suite 218 Sarasota, Florida 34237

GSA price \$56. Upgrade, \$5. additional.

Reviewed by: P13

P13 has been reviewing recent software that DDO analysts might consider buying.

One of these is RightWriter, which evaluates a document for grammar, style, usage, and punctuation. The program creates an output file consisting of the original text interlined with comments and suggestions. It provides an overall critique, a measure of the grade level of the writing and the "strength of delivery." It flags jargon and clichés and concludes with a list of words in the document that should be reviewed. There is also an option to provide a frequency count of all words in the document.

The manufacturers claim that the program is compatible with most word processors including

OfficeWriter, the agency standard. Output files match the format of the input files.

We found the program easy to use, with a better-than-average user's manual. It is designed as an aid for business and technical writing, and we highly recommend it for that purpose. The writing hints in the user's manual would benefit other writers as well.

In summary, a good buy.

Note: the passage delineated by lines was run on RIGHTWRITER. The results are shown on the facing page.

System requirements:

- ▶ Minimum Internal Memory: 384K RAM
- ▶ Minimum Disk Configuration: Two dual sided diskette drives or one diskette drive and a hard disk
- ▶ Operating systems: PC-DOS, Version 2.0 or higher; MS-DOS, Version 2.0 or higher; OS/2
- ▶ Computers: IBM PC, PC-AT, and PS/2, and all MS-DOS compatibles. (Special versions are available for DOS earlier than 2.0 and for memory sizes smaller than 384K.)



Output from RIGHTWRITER

<< ** SUMMARY ** >>

Overall critique for: D:\RIGHT\soft2.txt
 Output document name: D:\RIGHT\soft2.OUT

READABILITY INDEX: 8.87

4th	6th	8th	10th	12th	14th
**** **** **** **** ****					
SIMPLE		----- GOOD -----			COMPLEX

Readers need a 9th grade level of education.

STRENGTH INDEX: 0.92

0.0	0.5	1.0
**** **** **** **** **** **** **** **** ****		
WEAK		STRONG

The writing has a strong style.

DESCRIPTIVE INDEX: 0.60

0.1	0.5	0.9	1.1
**** **** **** **** ****			
TERSE		----- NORMAL -----	
			WORDY

The use of adjectives and adverbs is normal.

JARGON INDEX: 0.00

SENTENCE STRUCTURE RECOMMENDATIONS:

15. No Recommendations.

<< WORDS TO REVIEW >>

Review this list for negative words (N), jargon (J), colloquial words (C), misused words (M), misspellings (?), or words which your reader may not understand (?).

RightWriter(?)	1	compatible(?)	1
critique(?)	1	evaluates(M)	1
interlineated(?)	1	jargon(N)	1
reviewed(?)	1		

<< END OF WORDS TO REVIEW LIST >>

<< ** END OF SUMMARY ** >>

CONFERENCE REPORT



The American Mathematical Society
Centennial Celebration, August 1988,
Providence, Rhode Island

Reported by: David Harris, R51

Several Agency personnel attended the Centennial Celebration of the American Mathematical Society. The celebration featured invited talks by eighteen prominent mathematicians surveying the present state of American mathematics. It also featured some discussion of where mathematics is going, a discussion generally dominated at this conference by the applied types interested in improving the ties of academic mathematics to the users of mathematics in the real world, be they DoD, physical and social scientists, or industry. The left wing of the academic world, winner in last year's referenda on relations with DoD, was conspicuously quiet.

The managers of the society were apparently minded to try to undo some of the political harm from last year's debates by advertising and supporting better relations with applied math and its sponsors. The world of mathematics nearly always has known some conflict between applications-driven mathematicians (say Herman Weyl) and purists (say Bourbaki). Some of the best math now is being done by non-mathematicians. Organizers of this conference made an apparent effort to sell applied areas as a source of good math and good problems. Applied scientists can be a source of wisdom on what problems should be

worked on, as well as an inspiration. But traditionalists resist. The establishment was clearly trying to show that it realizes applied science has a role to play.

EVALUATION

I think that conferences like this are a convincing argument for the importance of having Agency people travel to at least selected conferences. I would hope the Agency would continue to try to keep our program of attending outside conferences alive, despite the budget crunch. In my view, it is foolish to spend money on supporting academic research, and fail to gather up the material that is presented to us at conferences for such relatively low cost. It would be self-defeating to let our ties to the outside atrophy for lack of money. All our previous efforts and expense would quickly be wasted.

SUMMARY

The technical highlights of the conference included an excellent minicourse by Gene Luks on Groups, Graph Theory, and Computer Science and a related talk by Aschbacher on recent developments in group theory exploiting the classification theory, very interesting talks on the interaction of physics and mathematics by Jones, Kac, Uhlenbeck, and especially Witten; a talk by Gross on modular forms and elliptic curves; a somewhat disappointing minicourse by Assmus and Key on Coding Theory and Finite Geometries; and talks by Caffarelli, Diaconis, Fefferman, Freedman, Friedman, J. Harris, Howe, Majda, Peskin, Sullivan, Tarjan, Thurston, Bott, and Lax.

In my personal opinion, the most awe-inspiring talk was Witten's on the relationship between quantum field theories and the future development of mathematics. He argued convincingly that many of the recent breakthroughs in math can be understood in terms of quantum field theories, and that theoretical physics can serve as a guide to new directions for mathematics. This possibility was illustrated by Jones' talk on knot theory, Kac's talk on modular forms, and by Donaldson's work on 4-dimensional manifolds. For details of the technical talks, please see my trip report.

Perhaps equally important was the political side of the conference. The political talk at the meeting was for once generally pro-DoD, and

anti the usual academic mathematical establishment. Especially outspoken were the talks by Peter Lax, a former president of the AMS, and Edward David, otherwise known as head of a commission that helped to convince the government to increase its support for academic mathematics. They both had many critical things to say about the lack of effort by academics to help deal with the current and future crisis in recruiting more American-born mathematicians.

David stressed the dangers of getting involved in politics. Once the math world declares itself political on any issue, politicians will cease to view its opinions as based on expertise, and will instead judge it as a political ally or enemy. This has heavy long-term consequences for mathematics support by government. David mostly gave the academics the bad news that they are failing to do their share of the job, and that they had better get out of politics and get to work in preserving mathematics as a profession. The mathematicians were repeatedly told that math is in competition with welfare and housing the poor. So, mathematicians must expect to be held to meeting their social obligations if they expect funding.

Lax gave what the president of the AMS called a blunt speech roundly criticizing many in both the pure and the applied mathematics communities. The anti-DoD resolutions of last year have clearly left much hard feeling, and the establishment was keeping its mouth shut to try to avoid making further trouble.

Another interesting event at the conference was a JPBM-sponsored meeting on the MS 2000 program and the abuse of MAs as teachers in academia. It was never quite clear however whether the intent was to deplore the practice of exploiting masters holders by using them as underpaid temporary help without benefits, or whether the intention was to educate department chairmen on the best way to do exactly such exploitation!

As usual, we engaged in a considerable amount of informal discussion with academics, both for purposes of improving our general image, of finding out what is going on in academic mathematics, and of ultimately aiding recruitment.

POLITICAL SPEECHES

Opening Ceremonies

Perhaps one could look on this opening ceremony as indicative of the lack of understanding by laymen of what professional academic mathematicians do and how they view themselves. Neither the governor nor mayor showed up for the opening ceremonies, despite the fact that AMS is an employer in Providence. The governor sent his policy advisor, Valerie Southern. The mayor sent Joseph Almagno, the Superintendent of the Providence School Department, apparently under the mistaken impression that the members of AMS are teachers. Brown University. sent Phillip Stiles, Dean of the Graduate School/Research.

The London Math Society and the MAA exchanged presents with AMS. SIAM accepted a present from AMS but gave none that I know about (in keeping with the general skepticism by applied mathematicians throughout the meeting about the attitudes of the pure mathematicians of AMS.)

President Reagan sent a letter, indicating his staff has some awareness of AMS's activities, and stressing the role of mathematical skills in maintaining "...our domestic prosperity, our national security, and our competitive stance in the world marketplace... That's a challenge I know you're ready to meet." Not if the members of the AMS can help it!

Governor DiPrete could not come because of the National Governor's Conference. His aide showed little appreciation of the noble role pure mathematicians assign themselves. She spoke of the 50% high school drop out rate in Providence, of the remaining students that cannot really read or write, and want less technical schooling. DiPrete opposes this, and wants more engineers, biomedical workers, scientists. The members of AMS are the role model for them. DiPrete wants to forge a partnership to guide our children and society. President Mostow reacted by calling this a message we rarely get, but appreciate (i.e., don't call us about such a partnership, we'll call you.)

Next, Joseph Almagno spoke. He said, we need you to help public education. The public is losing confidence in our product. We need to retool, reshape, and find better methods. He

apparently thought he was addressing an audience interested in education. He did not understand the role of the AMS as inventors of the truth of pure mathematics. Instead, he hoped they could help him with the problem of non-English speaking students, largely Hispanic and Southeast Asian. How can we teach them? Apparently, the differential geometers and algebraic topologists should show the way.

Phillip Stiles from Brown spoke of the long record of collaboration between AMS and Brown. Brown reaffirms its commitment to math and its outstanding math library (by which he meant they had recently bought a large collection of ancient mathematics manuscripts.) Brown University Mathematics Dept. was conspicuous by its lack of active participation as such at the meeting. For example, there was no effort to encourage mathematicians to visit the department. A search on foot allowed me to locate the Brown Mathematics Department building, in an outwardly unprepossessing old Victorian house. This was rather in contrast to the Applied Math and Engineering buildings, or for that matter the History of Mathematics Dept. quarters.

After the Presidents of AWM and the London Math Society had congratulated AMS and given it some gifts, Bill Gear of SIAM spoke. Math is the infrastructure of our future progress. SIAM and AMS must work together. We are all developing countries, and mathematics is at the heart of the process. We must have a literate population applying math to the problems of the real world. The distinctions between engineers, scientists, and mathematicians should be blurred, and we should all work together, unlike the traditional disdain of mathematicians for all these others.

In particular, funding is now in the hands of democratic institutions, which means that sciences must work to inform the public if they want money. Show that math is significant to the public. Integrate math into the world. All these points were repeatedly made by the applied mathematicians at the conference, but are distinctly distasteful to the true mathematicians. They are at variance with the sentiment expressed in the overwhelming support for the anti-DoD resolutions of the AMS last year. The organizers of this conference, however, did seem to stress by their

choice of talks precisely the importance of non-mathematicians to the future of mathematics.

Finally President Mostow spoke. He said that math today is so diverse that no one person can describe it all. Few people know the breadth and depth of the influence of math. The computer revolution shows, if anything, the invisibility of math in the world at large. The educated public does not share our enthusiasm for the subject. We must make efforts throughout education to find opportunities to expose people to real mathematics. AMS must get involved in this. Math will be permeating the world. So we are feeling our way towards a solution.

Future textbooks on the history of ideas should give mathematics its proper place. This will encourage youth to go into math. The role these textbooks give math is totally opposed to the role most academic mathematicians would like to have, and are willing to fill! How do you keep this from turning off those students you have educated on the role of mathematics in the real world?

Edward David "Renewing U. S. mathematics: An agenda to begin the second century."

The highlight of the political activity at the meeting was the address by former Presidential Science Advisor, Edward David. He is remembered as the leader of a committee that wrote the David Report (see my Trip Report on the AMS Meeting in Louisville 5 years ago.) David was helpful in selling the government on increasing funding for mathematics drastically. Now he has come back to AMS to lecture the mathematicians on their failures as citizens and professionals.

He started by expressing his concern about how mathematics deals with its customer activities. After five years of pushing how have we done? Substantial progress has been made, but there is a long way to go, and the hour is late. Frank talk is needed. In the last five years, math support has increased considerably. You have been winning in the fixed sum game over your competitors such as housing for the poor and aid for the starving. But the major issue was renewing mathematics, and enabling it to sustain itself. That issue is more pressing than ever. In 1983 there were 800 new Ph.Ds. Now

there are 700 a year, and half of those are foreign.

The increase in funding has been almost equally from NSF and DoD. NSF gave high priority to support for grad students and post docs. Unfortunately, they did not help senior investigators. But the problem is bottoming out, salaries are skyrocketing, and this may change the common perception that the world does not want any more mathematicians.

The David Report asked for actions from universities in support of mathematics, but has gotten little such support from them. To the Universities, mathematics is not as worthy as other subjects if it does not bring in as much money. Mathematicians must unite to educate the world on the value of math and on its needs. The world thinks math exists; there is no need for any more mathematics, just teach the math already known. Ken Hoffman's lobby has been quite good at fighting this attitude. [Of course, Ken Hoffman's lobby has also taken a lot of heat from the Thurston branch of AMS precisely for selling math as useful to the real world, in ways that many mathematicians oppose.]

Next David addressed reform of education. Two boards of the NRC are currently working on school curriculum reform, and informing mathematicians of opportunities for cross-fertilization. This is the MS2000 project. But there are very tough political realities. There are budgetary restraints. Federal R&E is already 25% of the nondiscretionary budget. Math is competing with social programs, like housing and welfare. Science has incredibly been winning in this competition. But math cannot expect another 84% increase in the next five years. The highest priority is of course sustaining the quality of math research. There should be an update of the David Report every five years to document progress, evaluate university instruction, and overview research opportunities in the view of mathematics users. It should discuss how math should be supported. A mechanism for such an update is needed.

David said AMS must overcome last year's combative attitudes and recommit itself to its goals in Washington. Micromanaged, programmed government-sponsored research is inevitable. As at Bell Labs, perhaps government can choose the research field, but let scientists determine the direction of the

research. There is a need to know what problems both the math and the user world think are important. What do your results mean for these *other* people. This may be done post hoc rather than ad hoc. Do the research, then look for how it may be sold to the outside world as useful.

AMS must work on its relation to the public - if only out of concern for keeping its share of the discretionary budget. We need political sophistication and cohesiveness, and must consider our responsibilities to society, and how we look to society. David said he is not calling for overcoming political activism. Mathematicians may offer advice to government in statesman-like ways. *But, mixing science with politics is poison. In Washington, if you try to use the prestige of mathematics to decide nonmathematical political issues, you will be treated as enemy politicians, and all your views will be rejected as political.*

Mathematicians must find better ways to attract young people to our field - NOT as currently, take it or leave it. The young have been leaving it in droves for adjacent fields. Even those in adjacent fields are appallingly ignorant of what mathematicians really do. Most students think we aim at winnowing out the weak and grinding down the ungifted. [They are right. Most outstanding mathematicians view the world differently from David, *not* a mathematician. There is only a comparative handful of people in any generation capable of making important breakthroughs in theoretical pure mathematics. They are of interest to us. The rest are a waste of our time.] Academic education should be a pump, not a filter.

David says we must improve mathematics education in our schools. We are a part of the educational crisis. The country is failing to educate youth in mathematics. We should help - and if we do, it will be appreciated. Twenty five million kids take mathematics in school; that gives mathematicians a big responsibility. [Elsewhere at the conference the "New Math" efforts of mathematicians to reform curriculum were discussed. These lead to doubts on this point. If mathematicians seek to make pure mathematicians out of the masses, they may end up messing up math education even worse. What is needed is an effort to talk with the masses in ways they will understand and find

convincing. It is rather doubtful that there are many members of AMS wanting to do this.]

In conclusion, David said our success in renewing mathematics has been mixed at best. We need new doctorates, and we must give them reason to believe that going into mathematics will give them a reasonable future. This will require the members of AMS to interact with schools, other disciplines, etc. Are they willing?

AMS BUSINESS MEETING and STEELE PRIZES

There was an amendment to the bylaws, voted without controversy, to change the way that dues are computed for institutional members. The effect is to break the connection between dues and the number of published articles from the institution, to the probable detriment of non-academic institutional members like the Agency. Several long-time employees of AMS were thanked. Then the Steele Prizes were awarded. Sigurdur Helgason won the prize for exposition. Gian-Carlo Rota won the prize for a fundamental research paper, for his work on the use of the Mobius function in combinatorial theory, and Deane Montgomery of IAS won the prize for cumulative influence on the profession. Paul Nevai, with whom I have had some interactions on the subject of orthogonal polynomials, got a job on an AMS committee. Mel Hochster, whom I knew in college, is one of the candidates for Vice President. William Browder will become the new President of AMS in December.

At the MAA Business Meeting, Steven Galovich and Bart Braden won Carl Allendoerfer Awards. James Epperson and Stan Wagon received Lester Ford Awards. Dennis Luciano, Gordon Pritchett, and V. F. Rickey won George Polya Awards. Seven Certificates of Meritorious Service were presented.

MISCELLANEOUS

AMS was organizing tours of the AMS Headquarters building in Providence. While I did not go on these tours, I did manage to go to the headquarters building to take a look around on my own. Not nearly as interesting as the wonderful little Rhode Island School of Design Museum of Art. I also recommend walking tours of College Hill and Federal Hill

to see the interesting architecture. My wife spent much of her time in nearby Newport.

There was an AMS short course on chaos and fractals that I did not attend.

There was a daily newsletter throughout the conference, featuring such information as that Rhode Island was the first state to attempt to tax sexual intercourse. They also advised, when driving in Rhode Island, "never ever beep your horn at black Cadillacs with blackout windows."

INVITED TALKS

Michael Aschbacher (Cal. Inst. Tech.)
"Representations of finite groups as permutation groups" (introduced by Daniel Gorenstein)

"The classification of the finite simple groups in 1981 changed the landscape of finite group theory and led to an increased effort to describe the structure and representations of the simple groups. Together with the classification, this effort has made possible unexpected applications of finite group theory in other branches of mathematics." In 1860, the French mathematics society offered a prize for the best research on the following problem: what are the possible indices m of subgroups of the symmetric group of degree n , and for such an m , what are the subgroups of index m ? Several great men published work on the problem, but understandably made little progress, and no prize was actually awarded. The purpose of Aschbacher's talk was to show that finally we are beginning to be able to do this problem, and to illustrate how to use the classification theorem.

Luis Caffarelli (Inst. Advanced Study) "The geometry of solutions to nonlinear problems" (introduced by Louis Nirenberg)

Persi Diaconis (Harvard) "Sufficiency as statistical symmetry" (introduced by Gian Carlo Rota)

Charles Fefferman (Princeton) "Problems from mathematical physics" (introduced by Felix Browder)

This session covered two problems in mathematical physics. The first is from quantum mechanics and concerns how close our current state-of-the-art will take us to explaining why a roomful of hydrogen gas can

happen. The answer is quite close. The second is from general relativity and concerns a proof that some small enough initial disturbance will not become a black hole. As such it deals with a quite difficult analysis of the possible nature of solutions for a PDE.

Michael Freedman (UC-San Diego) "Working and playing with the two-dimensional disk" (introduced by William Browder)

Harvey Friedman (Ohio State) "The incompleteness phenomena" (introduced by Saunders MacLane)

Benedict Gross (Harvard) "Modular forms and elliptic curves" (introduced by John Tate)

This session surveyed some major developments in the theory of elliptic curves, the theory of heights, and rational points. Gross is married to Jill Mesirov, whom some of you may remember. According to Tate, they had a child two weeks before this conference.

Joseph Harris (Harvard) "Developments in algebraic geometry" (introduced by Phillip Griffiths)

Roger Howe (Yale) "A century of Lie theory" (introduced by George Mackey)

Vaughan F. R. Jones (UC-Berkeley) "A von Neumann algebra excursion: from quantum theory to knot theory and back" (introduced by Joan Birman)

Victor Kac (MIT) "Modular invariance in mathematics and physics" (introduced by Nathan Jacobson)

Upon hearing this talk I remarked that some deep mysterious truth was going on here. Witten's talk later explained to me what it is! Kac began by asking us all to sign the petition on behalf of Soviet emigrés available at the registration desk (a partial reminder of the role of immigrants in this celebration of math in America!)

Andrew Majda (Princeton) "Mathematical fluid dynamics: the interaction of nonlinear analysis and modern applied mathematics" (introduced by Peter Lax)

Majda advertised the importance of an interdisciplinary approach to applied math problems. These problems are too difficult to

be handled by any one method, but can be reasonably well dealt with sometimes by combining attacks via new computational methods to guide research, experimentation (with physical models for example), suggestive rigorous theoretical analyses of simplified mathematical prototype models, etc.

Thus fluid dynamics is governed by a complex system of nonlinear PDEs with features of all kinds of PDEs. The key new ingredient allowing the interdisciplinary approach is the use of computer simulation to guide research and test models and conclusions when experimentation is unreasonable. This situation is a paradigm for even worse applied problems, such as oil recovery, combustion, elasticity, and magneto-fluid dynamics. This use of gas dynamics dates back to ideas of Lax.

Charles Peskin (Courant Institut.) "Mathematics and computing in physiology and medicine: Biomathematics from Hearts to Molecules" (introduced by Cathleen Morawetz)

Peskin gave yet another talk on the advantages of mathematicians working on applications rather than pure math. Here the problem is the mathematical modeling of functioning human organs, and in particular the designing and testing of heart valve replacements. Several articles of this sort are in the latest engineering journals. Similar problems arise in constructing oil rigs that have parts subject to both slow and fast vibrations. Also, molecules undergo slow and fast vibrations.

Peskin described the problems of modeling heart valves, and illustrated with films done by computer simulation showing how hearts with various kinds of replacement valve would in fact function. Several possible valve designs can be studied this way, and dismissed as defective, or improved.

One molecular chemistry problem being modeled is how large molecules like DNA control the production of RNA, which creates protein enzymes, which in turn control the reproduction and action of the DNA. The "Genes in Action" model is by no means done, but is already being used to study the mechanics of molecules. Again the so-called stiffness problem, caused by the differing time scales within which nerve impulses and DNA operate, is the difficulty in doing the modeling.

Dennis Sullivan (CUNY Graduate School) "Progress on the renormalization conjectures in dynamical systems" (introduced by Stephen Smale)

Robert Tarjan (Prof. Computer Science, Princeton) "Mathematics in computer science" (introduced by Ronald Graham)

After a general introduction to theoretical computer science, and the development of effective algorithms, Tarjan spent most of his time talking about his work on trees and operations on trees. He introduced rotation as a mechanism for balancing trees and keeping searches cheap. He argued then that balancing is not in practice a good idea. A possible answer is splaying (Sleator-Tarjan 1983).

William Thurston (Princeton) "Three-dimensional geometry and topology" (introduced by Lipman Bers)

Bers introduced Thurston with glowing praise. The talk he gave merited the praise.

Karen Uhlenbeck (Texas) "Instantons and their relatives" (introduced by S. S. Chern)

Edward Witten (Prof. Physics -Inst. Adv. Studies) "Quantum field theory and Donaldson polynomials" (introduced by Clifford Taubes)

To me at least, Witten's talk was the high point of the entire conference, giving a glimmering of where the grand synthesis will come from that Uhlenbeck, Kac, Jones, Tarjan, Thurston, etc. are looking for in their work. The point is that much of traditional mathematics can be looked at as related to 1-dimensional quantum field theory. The recent work of Jones and Donaldson are the first inklings of 3- and 4-dimensional quantum field theories. The Kac and Bott talks, as well as work by Gromov in Thurston's talk are inklings of a 2-dimensional theory. So, there is at least the possibility of inspiration for vast new areas to develop in mathematics out of this connection to quantum field theory. Witten's talk was a sketch of this connection.

Raoul Bott (Harvard) "The topological constraints on analysis" (introduced by Andrew Gleason)

Peter Lax (NYU) "Mathematics: Applied and Pure" (introduced by George Mostow)
Alternative titles from Lax, "The Flowering of

Applied Math in America" or "The Deflowering of Pure Math in America".

Mostow summarized Lax's talk as 'blunt'. It was. He said a lot of impolitic things that ought to have been said. This talk was part of the continuing counterattack by the applied people against the disdain for applied math by the academics. Lax started by mentioning the Bourbaki attitude that once dominated pure math, calling for math isolated from the rest of the universe, and internally guiding its own future growth. Lax said the great mathematicians of the past would have been horrified. Math and Applications are equal partners, feeding each other [controversy in the audience!]. Before 1945 applied math was treated shabbily in math departments despite some great examples.

Lax launched into a survey of recent work in applied math. Equal to the gains from computing caused by improved hardware has been the gain from clever software, algorithms, code, discretizations, etc. Computing forms an additional bond between pure and applied math. Integer programming, dynamic programming, optimization problems, and simulated annealing have become major fields. Lax described simulated annealing at length, especially attacking the traveling salesman problem via the Metropolis algorithm. He mentioned FFTs, the simplex method, fast matrix multiplication, Karmarkar's algorithm, and Knuth's book as major subjects.

Lax then described Sarnak's work on network design, which is done using the theory of automorphic functions and the Ramanujan conjecture. Then he talked of Smale's work on average case complexity, although he acknowledged that there are not many answers yet in computational complexity.

Lax then lambasted AI and catastrophe theory. He said AI set its goals preposterously high and exaggerated its achievements. He was particularly hard on Herb Simon's talk on BACON at the AMS meeting at Louisville (I worked over that talk myself in a trip report.) Lax cited several other skeptics on AI. He had similar harsh words for the advocates of catastrophe theory. Lax is a believer of sorts in the theory as such. But, the hostility of many is caused by stupid attempts to oversell what catastrophe theory is.

Zeeman was an honored guest at this conference, representing the London Math Society. Lax quoted Zeeman at length on the virtues of catastrophe theory as a breakthrough, and then tore the quote apart. For example, he pointed out that the study of shock waves for PDEs dates back to Riemann, and is older than AMS or even the London Math Society of which Zeeman is president. He expressed skepticism that Zeeman did not know this.

The methods of applied math are sometimes rigorous (when this is practical, which is far from always). Otherwise, it must rely on asymptotics, experiments, simplifications to inspire intuition for further research. In the days before computers, these simplifications may have helped cause the bad reputation of applied math, and the unwillingness of pure mathematicians to work in this area.

World War II demonstrated the importance of math to the real world, which led to support for both applied math and math in general. The US Government provided this support, at first through ONR, then AFOSR and ARO, then through DOE (the successor to AEC). NSF took over much of this funding later on. The AMS proposal to reduce DoD funding is offensive to many of us. It implies we are doing something wrong when we accept government money to fund our work. We object.

Immigrants to the United States were responsible for pushing applied math in the old days. To them, it was inexcusable not to look to the applied world for advice on what problems math should be confronting. For example, von Neumann and Weyl were dominant figures in American math that felt this way.

Finally, Lax spoke of the need to change our educational system. As for calculus, he said he was one of the "doubting Thomases" (groans at the pun!) Lax thinks we should replace calculus by a new style calculus course oriented towards applications. UMAP can serve as a source for such.

Saunders MacLane (Chicago) "Some major research departments of mathematics" (introduced by Leonard Gillman)

MINICOURSES (*I attended two of the seven.*)

"Contributions of algebraic coding theory to finite geometry" E. F. Assmus (Lehigh) and J. D. Key (Bryn Mawr).

[Handout, surveying parts of the course, is available.] This minicourse suffered from the ravages of the MAA support personnel. They changed the room for the course without telling half the participants. As a result, half of us missed the first half of the course. The second half of the course had all the students, but was held in a ludicrously hot and unfavorable classroom environment. After an hour, Key wilted to the extent of not being able to go on. After another hour, Assmus was soaked to the skin. Why the originally scheduled, air-conditioned room was not used I do not understand. The course served as an introduction to linear codes and their connection to designs and finite geometries.

"Groups, graphs, and computing" Eugene M. Luks (Oregon).

[Handout, rather incoherently surveying parts of the course, is available. In addition to the handouts that were supplied at the course, Luks mailed us a better version, one representing properly the various overlays he used with his overheads, as well as a reprint of an article, "Isomorphism of Graphs of Bounded Valence Can be Tested in Polynomial Time" that led to some of this work, and that originally appeared in August 1982 in *Journal of Computer and System Sciences*.]

Though it was given in the same impossible environment as the second half of the Assmus course, this course went splendidly. The classroom was not quite as unpleasant. But, mostly, this was because of the presence in Luks of a true expert, lecturing about the state-of-the-art of an important subject that he clearly loves. The course dealt with a paradigm for solving computational group theory problems, together with many examples. Ultimately the goal is to come up with ways to use the classification of finite simple groups, and divide-and-conquer, to improve computer algorithms. The role of the connection between group theory and graph theory is central to how Luks suggests doing this. □

QUOTE
WITHOUT
COMMENT

Extract from

BANANA, The Story of a Fruitful Diagnostic Enterprise, G42 TSR05-88, March 1988

by [redacted] G424

Cryptologic diagnosis is not an activity for the insecure. It may be thought of as a mental wrestling match against an opponent who is assumed, not known, to have some weakness. The diagnostician must be prepared for a long, possibly futile struggle. He must have enough confidence in his abilities to mount a relentless attack even though the referee may be the opponent's mother. Rather than give up in a particularly tiring match, he merely takes time out to face other opponents, only to return with some new moves.

Unlike most other members of the cryptanalytic community, the diagnostician is not armed with the hard knowledge of his opponent's game plan—no sacred diagrams. He must possess an even more thorough knowledge of principles and techniques than his non-diagnostic colleague in order to seize the advantage on his adversary. To add insult to injury, his successes seem trivial to those who have never been in his shoes. Diagnostic success is often shrouded in secrecy, making it even more difficult for the diagnostician to enjoy the cryptanalytic limelight. With his chances of fame and even respect somewhat limited, the diagnostician presses on secure in the knowledge that he is working in the most difficult and creative area of cryptanalysis.

~~FOUO~~



To the Editor:

(U) In response to your editorial in the 3rd Issue 1988, I wanted you to know that at least one Key Component, T, has a "Yellow Pages." Here's a copy for you. Others can be had for the asking.

Jim Devine, A/DDT

The Editor replies:

(U) Thanks! And, dear readers, some of the pages are yellow!



To the Editor:

P.L. 86-36

~~(FOUO)~~ [redacted] article on the language programs (2nd Issue 1988) was very good. My experience with the language reserve program leads me to believe that it should be more widely advertised among the managers, not just the retiring linguists. I also sense that most managers and linguists interpret the wording "the director can call upon in emergency situations" to mean crisis or almost warime situations. In my case, in G Group, it was a critical shortage in the field and the need to fill the spot for a longer than average TDY period, e.g., several months.

~~(FOUO)~~ Thanks to the willingness of the linguist, the perseverance of the managers, and assistance from P16, we were able to overcome the initial hesitancy from some quarters to defining our language problem as fitting the criteria of emergency and of requiring directorate approval. It was a successful endeavor.

(U) [redacted] perceptions as SUSLO-2 were very interesting also.



LETTERS



P.L. 86-36

To the Editor:

I recently received a copy of the article, "A Reform in Need of Reform" by [redacted] published in *CRYPTOLOG*, 2nd Issue 1988. Some of the things I read truly amazed me, and I would appreciate an opportunity to offer a moderately vigorous rebuttal. The points with which I wish to contend are synopsized below:

The author believes that the current NSA software acquisition methodology is hindering software acquisition, that our software customers are well aware that the process is not working, that the finance people know we are paying more for less, and that our Office and Group Chiefs feel weak and uncomfortable because all they can do is throw their hands up and go for a quick-response solution. In a curious contradiction, the author acknowledges "that the software being delivered today is cleaner and easier to maintain than in the past, but . . . in terms of costs . . . the trade-off is unacceptable."

The article states, "Incontrovertibly, contractor-developed software comes at a much higher cost than in-house developed software . . . software developed out-of-house is costing the Agency perhaps four to nine times what it might otherwise cost."

The author proposes that we produce software using a method loosely patterned after a level of effort contract. As I understand from the article, software developers should be assembled into small groups, and assigned small portions of a large system. The software developers will get a general idea of the customer's problem, produce some software that they think is approximately what the customer wants, and demonstrate it to the customer. If the result is not exactly what the customer wants, the developer will simply rework the software until the customer is happy. If the customer or the

developer happens to think of something else the software should do, the developer will just add it in. Conferring continually with the customer, the teams will carry on, adding functions as knowledge is gained, correcting course as necessary, and documenting as little as possible until the team and the customer agree that the job is done. The article suggests that if we follow this formula, the software developers will be productive and happy, the customers will be undisappointed, and the "malaise" that has so cruelly afflicted our Office and Group Chiefs will be forgotten as they busily reallocate something like seventy-five to eighty-nine percent of their software acquisition budgets.

The method..that the author proposes to replace current software acquisition policy seems laissez-faire to an extreme. Nothing could be planned more than a few weeks in advance, because the customer might change his mind or there could be a dramatic technological breakthrough that will redirect the whole project. Without a plan, there is nothing to schedule; besides nothing is ever going to get done on schedule anyway. It would be wasteful to document before the software is finished, because there are no firm requirements, and no one really knows what the finished product is supposed to do. Never mind that the software developers, unstifled by the need to document and uncontrolled by firm requirements, may strike out on some wild tangent that comes to a deadend, and may need to reestablish what was done two weeks earlier, but cannot remember how they did that last tricky little algorithm that got altered during the wild tangent. Just continue this....method.., and one fine day the project will be finished.

In his article, [redacted] impeached for reasons of greed or self-interest any witness who supported NSA software acquisition methodology. Before I try to counter some of

the positions taken in the article, let me defend myself against the charge of greed. I am never enriched by prolonging a project. I write no textbooks. I teach no courses. I am a software acquisition manager, and my rewards, such as they are, depend upon my ability to acquire software within cost and schedule. I confess to the charge of self-interest in this matter, but because of that self-interest, I am strongly motivated to transfer allegiance to any doctrine that promises to help me develop software within cost and schedule limits.

If there is a known method by which we can produce software on schedule at one quarter the cost of acquiring it under contract, I am willing to adopt that method instantly. Maybe the author is correct and we have been wasting three-quarters of our software budget. I certainly do not have figures to refute this estimate; does anyone know an accurate overhead rate or an authentic productivity figure for NSA software developers? Maybe the author can help me out here. Could I possibly see the research data that was developed to support this estimate

Perhaps the author will be surprised to learn that many of the contractors I have dealt with recently stand four-square on his side. If the contractors are being enriched by our methodology and documentation requirements, they are almighty ungrateful; the cry against NSA documentation requirements is almost universal among contractors. Most contractors have their own way of doing business, and are eager to demonstrate that their way "meets the intent of NSAM 81-2 and NSAM 81-3." They want us to accept their standards and practices, precisely because they are familiar with them, and we probably are not. They object to the amount of documentation we require. Usually they cite prohibitive cost, but I suspect they balk for the same reasons government developers do: they do not want those nosey parker software managers telling them what to do.

According to the article, the NSA acquisition policy reduces the productivity of our newly-hired software producers. These people have had the benefit of the "formalized" experiences of their predecessors, and are "far better prepared than their predecessors to analyze, design, implement, test, and document", yet they chafe under the yoke. They are stifled; the documentation requirements are

"stultifying" and the methodology is "demotivating" (sic). They yearn to be free from the oppression of the wearisome NSAMs, which expect from them either too much or too little, depending on how you read the author's remarks. On one point the author is clear: "Agency [...] methodology is [...] in flagrant disregard of [...] Maislow, Herzberg, and Argyris."

I fail to see how our methodology violates the teachings of all the Management Hall of Famers. Using it, software managers can provide software developers with clear direction, unambiguous measures of progress, and frequent indications of accomplishment and success. All of these are Good Things, according to the Management Meisters. It seems to me that drifting through a project, with no clear indication of immediate or long-term goals, continually trying to patch new requirements into the software, with no real sense of accomplishment and no end in sight, would demoralize the new-hires more than having to document their work. I agree that today's developers are trained to "analyze, design, implement, test, and document". NSA software acquisition policy provides a framework of discipline that guides them while they do what they are trained to do.

If so much is wrong with our policy, and if so many people, including the newly hired, the contractors, the Data Processing customers, the financial people, and the author of this article, object to it, why does it remain in place? Who supports NSA software acquisition policy? I think most software acquisition managers do. I think the software support managers do. I hope and trust that my upper management does. Among us, we may often hold spirited and enthusiastic discussions concerning the proper interpretation of finer points in 81-2 and 81-3, but we have in common certain beliefs: software acquisition requires firm discipline; Life Cycle Support requires documentation; the NSAMs offer a way to achieve both. Whether it is perfect or not, our current methodology allows us to define and bound the software project, divide it into discrete tasks, estimate cost and schedule much more accurately, measure progress throughout the project, predict cost and schedule variances, and react decisively when such variances occur. As it happens, much of the documentation produced as tools with which to *manage* software

production also serves another purpose: it helps the poor devils in Life Cycle Support organizations who must patch and mend the result for the next ten years. These people have one of the toughest jobs in the software world; ask them if it costs too much to produce clean maintainable software and the documentation to go with it.

Most of all, I hope our Data Processing customers support methodology and discipline in software the acquisition. As a result of front loading software acquisition efforts, the customer has reasonable expectations about what he is buying, how much he is going to pay for it, and when it will be ready. Reverting to desultory software acquisition is almost sure to result in a lot of disappointed customers. Without goals or requirements, without discipline and method, we cannot predict or plan events; if we cannot predict or plan events, we cannot estimate cost. The customer will never know what he is going to get, when he is going to get it, or how much it will cost, until after the project is over.

So I guess I am one of the author's axe-grinders. The axe I must grind remains the same whether contractors or govies turn the stone: accountability. As a software acquisition manager, I am responsible for producing useable, maintainable software and the proper documentation on time and within budget. Therefore, I want control, or at least the illusion of control, of the software development process. I want to know what work is to be done, how much money is going to be allotted to the task, who is going to do the work, how the work is going to be done, how soon the work is going to be finished, how progress is going to be measured, and how success is to be declared. No additional work will be done without a written requirement, accompanied by a certified check, more people, or schedule relief. Furthermore, I want current information concerning how much work has been done, how much money has been spent, how much work is left to do, when we are going to finish, and how much it will cost in the end. In writing, please. NSAMs 81-2 and 81-3 provide guidelines and methods for managing software projects, and I need all the help I can get. Some software producers may find the process onerous, but for the most part, these people are professionals, and understand

the need for a disciplined approach to software development.

The author of this article presented several other viewpoints that I would like to address. Some of his points are actually supported by the 81-2 and 81-3 philosophy, but he states those points so casually and offhandedly that one can easily overlook the implications of his reference. For example, he states that the critical ingredients of a successful project are "simple design", "prototyping", "incremental development", "small, tightly organized teams", and "minimal formality".

Aren't "tightly organized" and "minimal formality" antithetical? Still, I think I get the point: a small group of people working together without having to deal with outsiders, and without a lot of tiresome management types asking how things are going.

No argument from me about "incremental development". Paragraph 2.1.2.2 on page 2-3 of NSAM 81-3/DOD-STD 1703, dated 15 April 1987, is the definitive work on this subject, as far as I am concerned. The same goes for "prototyping", which is actually a subset of incremental development. Sorry, but the projects I see these days just do not yield to "simple design". Apparently all the simple software has already been written, and the only projects we have left are devilishly complicated.

The author offers a solution to the complex software project ("If a project is large, it should be broken into smaller projects."), and likens the process to a diner eating steak. Strangely, he then leaves the subject and says nothing more about the tremendous system engineering effort required to implement the Sirloin Approach. The process of breaking a large project into smaller projects is the design process, and it is simpler said than done. The procedure is described in Paragraph 1.4, page 1-9 of DOD-STD-1703, which defines the design activities during software development. Traditionally, these activities consume forty percent of the total acquisition effort. Developing software is not very much like eating steak. It is a process of defining the basic parts of a system, manufacturing the parts according to specification, and assembling the parts into a working system. It requires thought, planning, organization, cooperation, discipline, and a lot of hard work. It requires

a lot of formality, too. Somebody has to document the requirements assigned to each segment of software, the input each expects, and the output it provides, because eventually all those segments must fit together to form a system that works.

The author does recognize the importance and difficulty of system integration, and masterfully reduces a task of imposing proportions to an elegant understatement: "Of course, the interfaces amongst the teams must be clearly defined, and the coordinator must do his job skillfully." You are only too right, sir. The "coordinator" may even have to introduce a little more formality, meaning an Interface Control Document, and a Software System Integration Plan. And a Configuration Management Plan; otherwise those highly-motivated software developers, in a high flush of "esprit de corps", will "respond dynamically to new requirements" and produce only "minimal adequate informal documentation while development is fluid", and put the ICD and the Integration Plan down the sewer. And of course the "coordinator" needs to know when each piece of the software is going to be ready, which means ... a Schedule! Here is Formality of the meanest sort, with assigned tasks, and deadlines, and people's names, and all like that so They know if you don't do your work. But not to worry, more than likely at least one other tightly organized team, unburdened by formality, is going to get tied up interacting with the customer and assimilating knowledge gained into the product, and will blow the integration schedule to hell before you do.

I suspect that [redacted] strikes close to the truth with one statement: "...the Agency has suffered great difficulty in developing large software systems using today's software acquisition methodology." If he refers only to software developed in-house, I will agree. But the great difficulty is not caused by our methodology; we have great difficulty because we will not accept the discipline and the accountability that goes with any methodology. I have been through some very large system acquisitions under contract, and have seen methodology successfully applied. Industry workers may not like it, but they accept the discipline and methodology, and it works. Industry managers have remarked to me that the government managers cannot or will not apply 81-2 and 81-3 standards to their own

workers with the same diligence they display in applying it to contractor personnel. I believe the statement is true. If we allow our methodology to fall into desuetude internally, we will always have great difficulty developing large software systems.

Flexibility is built into NSA Acquisition Policy. The documentation required for system development depends upon the needs and intentions of the customer, and the type and size of the project. The policy itself so states; the Manuals 81-2 and 81-3 contain many words about tailoring documentation requirements to the needs of the project. If a manager takes exception to a particular requirement of the policy, there is usually relief available. If the leeway in our policy is inadequate [redacted] in T303, is always looking for a better method to develop software, or ways improve the method we use. He has always been willing to help me with such problems. In the meantime, our method may be all wrong, but it is what we have to work with.

[redacted] R741

P.S. I really need that study that compares the cost of developing software in-house with the cost of contracting for software development. My managers are excited about the potential savings. Could you send me a copy right away?

The author replies:

A careful reading of [redacted] conclusion and my own shows us to be in basic agreement. Specifically, my paper concluded by calling for a review and reevaluation of the Agency's current software acquisition methodology. [redacted] in his conclusion, acknowledges that our method may be all wrong, but it is what we have to work with, which of course, is my point. I can only infer that he welcomes my proposal to review and revise appropriately, and I heartily welcome his articulate support on this matter.

Admittedly, we have a few point of disagreement, but not on the need for discipline and control; from my experience, small teams usually possess and abundance of both commodities.

I suspect our principal difference lies in what I would label "the knowability assumption" -- the basic premise upon which our prevailing acquisition methodology is based. Today's methodology employs a "waterfall" model of steps: identify and understand all requirements, document, design, code, test. However, my experiences at the Agency have led me to reject the notion that the desired system is knowable enough to document and design in cement at the outset; a tremendous amount of knowledge is gained through an interactive development process. With my approach, a fast start can be undertaken with the knowledge gained rapidly assimilated into the process. And note: large teams get in the way of a fast start.

Yes, today's methodology provides discipline and control, but precious little in the way of timeliness. [redacted] and I agree we would like to do better than we're doing. Let the review begin!



To the Editor:

A while ago I bought a Russian-alphabet element ("golfball") for my Selectric typewriter. Every time I hit the letter Ж, it would print imperfectly: only part of the letter would print. Several phone calls to IBM in the Washington area finally got me to the "expert." He told me that on the Russian-alphabet element the Ж is in the position that is occupied by the regular element by the colon and semicolon. That position, as well as the position occupied by the period and comma, has reduced velocity, because otherwise the English punctuation marks would pound holes through the papers. The rest of the conversation went like this:

Me: But I want to type Russian words containing the letter Ж.

Him: Then you'll have to phone us and we'll send a technician to your home. He'll take the machine apart and reset the tension for that character.

Me: But what if I want to switch back to English again?

Him: Then it will punch holes through the papers.

Me: Do you mean to say that every time I want to switch back and forth, I've got to have a technician make a service call and reset the tension?

Him: That's right.

Me: That's impossible! I want to switch back and forth from English to Russian, sometimes even within the same sentence!

Him: Say, I've got an idea! How often do you need that letter?

Me: As often as it occurs.

Him: Well, then, why don't you just use other words instead? Or just leave out the letter completely?

I must confess, dear reader, that I was unable to explain to the "expert" over the phone that this would be comparable to having F. Scott Fitzgerald type, " elda and I went to the oo today. elda loves the ebra with his ig ag stripes."

Art Salemme, Ret.



Art tells us that he has since switched to a word processor for his free-lance translations.

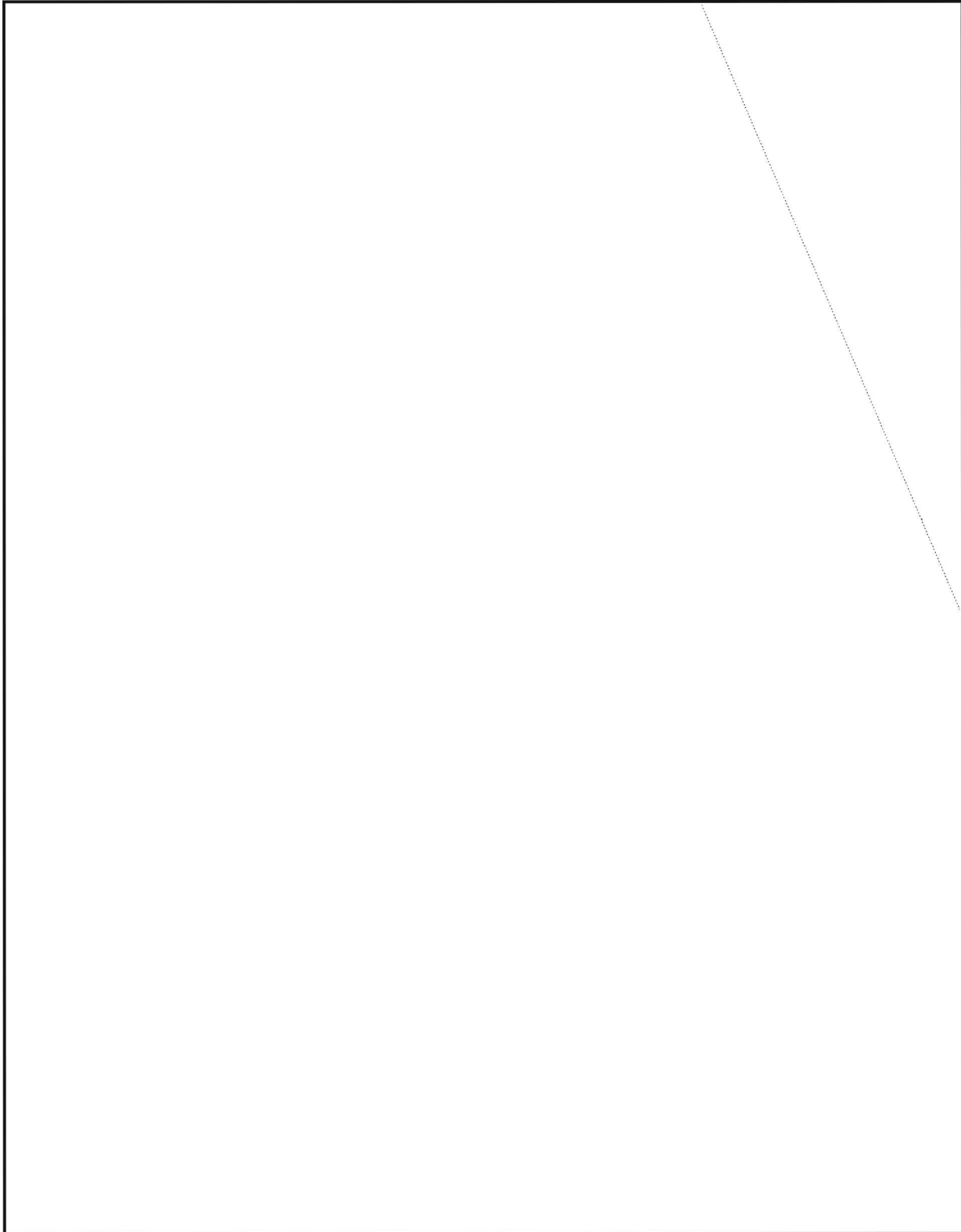
Readers may recall that Art was the Editor of CRYPTOLOG in the late 70s who set the tone for this rag with his sprightly and irreverent sketches. We've kept them in our portfolio for recycling, and show one of them in the previous column.

Art was pleased to learn that CRYPTOLOG is still going strong, and sends warm greetings to readers, editors, and contributors.

~~TOP SECRET UMBRA~~

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

FROM THE PAST



~~TOP SECRET UMBRA~~

minicrypts

or



by Bill Lutwiniak, P1

Years ago the New York Herald Tribune published a short cryptogram along with its daily crossword puzzle. There was a special ground rule -- every letter involved had to be used at least twice. Over the years constructors began to torment solvers with very short cryptograms which, while they conformed to the ground rules, were not very easy to solve. These held a strange sort of charm for some of us cryptanalysts, and they may still have appeal.

The other rules were intelligibility, of course, and that the plain text consist of a sentence of three or more words. There was no caption for the cryptogram, nor were proper names so indicated.

To illustrate how brief the minicrypt may be, consider:

A Father's day commercial

I SIS IS
A DAD AD

or

What's the kazoo for?

A SEES AS
I TOOT IT

What if Eisenhower Runs

A'PP PART ART*
I'LL LIKE IKE

(The asterisk indicates a proper name)

If this puzzle proves of interest, we'll publish more of them. We also solicit contributions. Here are three for this round.

KNIGHT AHAT TAGNKI

TRANRTYNE AY EY ETRA

SWOOSH KWYS PHOOHY SHO PWK PHH PH

SPECIAL OFFER

Just to get to moving on this initial round, a prize is offered to the first person or team to solve the minicrypts. Indicate whether the solution is an individual or a team effort.

Send your entries to CRYPTOLOG PUZZLE, P1, HQS. In case of a tie, the winner(s) will be selected by lot.

Readers in the Field may send entries via PLATMAIL to: cryptlg@bar1c05. Field entries will be competing only with other field entries.

Solution to

LEFTOVERS 3rd Issue 1988

1. CORN DEAN SEND RAIN I
2. STAR BAIL PITY RAMP M
3. ADAM ISIS IRON PAIR P
4. EXIT LENS LIVE RILL R
5. APER FORD MERE AIDE I
6. REAL PIPE TARS LINT N
7. DIPS MEAN TALE PEAT T

NSA-CROSTIC (plus) No. 67

G422

This puzzle has a user-friendly feature. The squares are numbered so that all squares on the left side have an even middle (tens) digit, while those on the right side have an odd middle (tens) digit. Further, all squares in the same column end with the same digit.

Fair warning: There's a wild card in this puzzle !

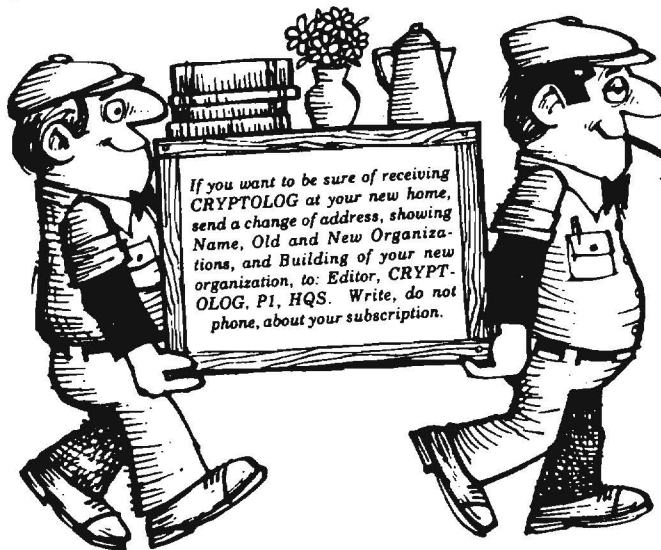
A. Where Crockett County is	230	273	228	191	153	115	75	53	18											
B. Fixes	255	235	84	102	40	3	27	71	111	133	194									
C. A kind of cheer	257	239	272	190	212	173	152	67	127	208										
D. Like tropical rain	226	200	113	137	195	170	192	99	117	70										
E. Poisonous herb	2	23	65	44	87	125	106	169	189											
F. Fletcher	112	51	46	85	144	130	213	271	233	251										
G. Mock Roman naval battles	215	299	187	197	145	165	57	224	245	178										
H. Respite from work	164	211	269	60	42	1	35	11	28	72	52									
I. Kind of production	264	270	82	121	41	20	7	30	49	69	62									
J. World War II program	4	123	141	220	132	2522	232	180	161											
K. Rank	205	79	10	151	244	122	253	166	157	68										
L. A canine	258	236	217	199	159	156	135	175												
M. Anastasia, for one	210	207	181	240	221	260	160	140												
N. Said <i>grazie</i> or <i>спасибо</i>	114	93	29	14	38	59	119													
O. Relating to a letter	128	150	168	146	100	64	61	43	25	5										
P. Religious fervor	216	196	177	16	134	58	37	32												
Q. Astonishment	238	186	73	54	94	91	109	149	129	172										
R. <i>Hibiscus syriacus</i>	202	163	104	45	126	107	248	231	214	95	36	17								
S. Inflammatory	31	8	56	77	118	154	182	204	246	263										
T. Every bride has one	247	218	90	86	47	12	136	176	24											
U. John Hancock used one	206	223	241	243	124	83	103	142												
V. Necessities	232	261	203	183	167															
W. Praise phrase	33	13	50	98	89	110	148	185	227	265	274									
X. Specimens of <i>xiphias gladius</i>	225	250	268	266	9	21	101	80	76	97	138									

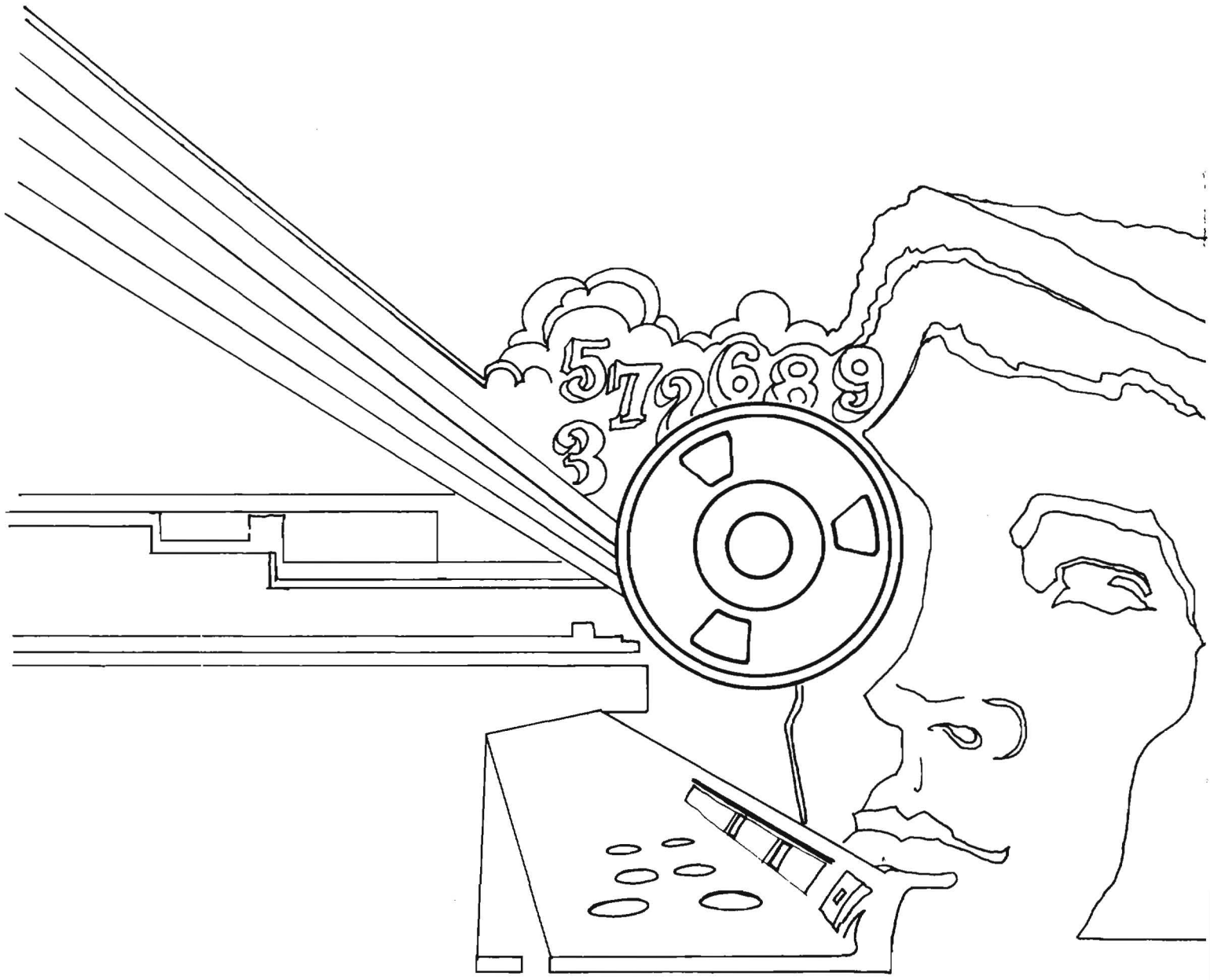
HOW TO SOLVE A DOUBLE-CROSTIC

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.

	1H	2E	3B	4J	5O		7I	8S	9X	10K	11H	12T	13W	14N		16P	17R	18A	
20I	21X		23E	24T	25O		27B	28H	29V	30I	31S	32P	33W		35H	36R	37P	38V	
40G	41I	42H	43O	44E	45R	46F	47T		49I	50W	51F	52H	53A	54Q		56S	57G	58P	59N
60H	61O	62I		64O	65E		67C	68K	69I	70D	71A	72H	73Q		75A	76X	77S		79K
80X		82I	83U	84B	85F	86T	87E		89W	90T	91Q		93N	94Q	95R		97X	98W	99D
100O	101X	102B	103U	104R		106E	107R		109O	110W	111B	112F	113D	114V	115A		117D	118S	119W
	121I	122K	123J	124U	125E	126R	127C	128O	129Q	130F		132J	133B	134P	135L	136T	137D	138X	
140M	141J	142U		144F	145G	146O		148W	149G	150O	151K	152C	153A	154S		156L	157K		159L
160M	161J		163R	164H	165G	166K	167V	168O	169E	170D		172Q	173C		175L	176T	177P	178G	
180J	181M	182S	183V		185W	186Q	187G		189E	190C	191A	192D		194B	195D	196P	197G		199L
200D		202R	203V	204S	205K	206U	207M	208C		210M	211H	212C	213F	214R	215G	216P	217L	218T	
220J	221M	222V	223U	224G	225X	226D	227V	228A		230A	231R	232J	233F		235B	236L		238Q	239C
240M	241U		243U	244K	245G	246S	247T	248R		250X	251F	252J	253K		255B		257C	258L	259G
260M	261V		263S	264I	265W	266X		268X	269H	270I	271F	272C	273A	274W					

MOVING?





~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~NOT RELEASABLE TO CONTRACTORS~~