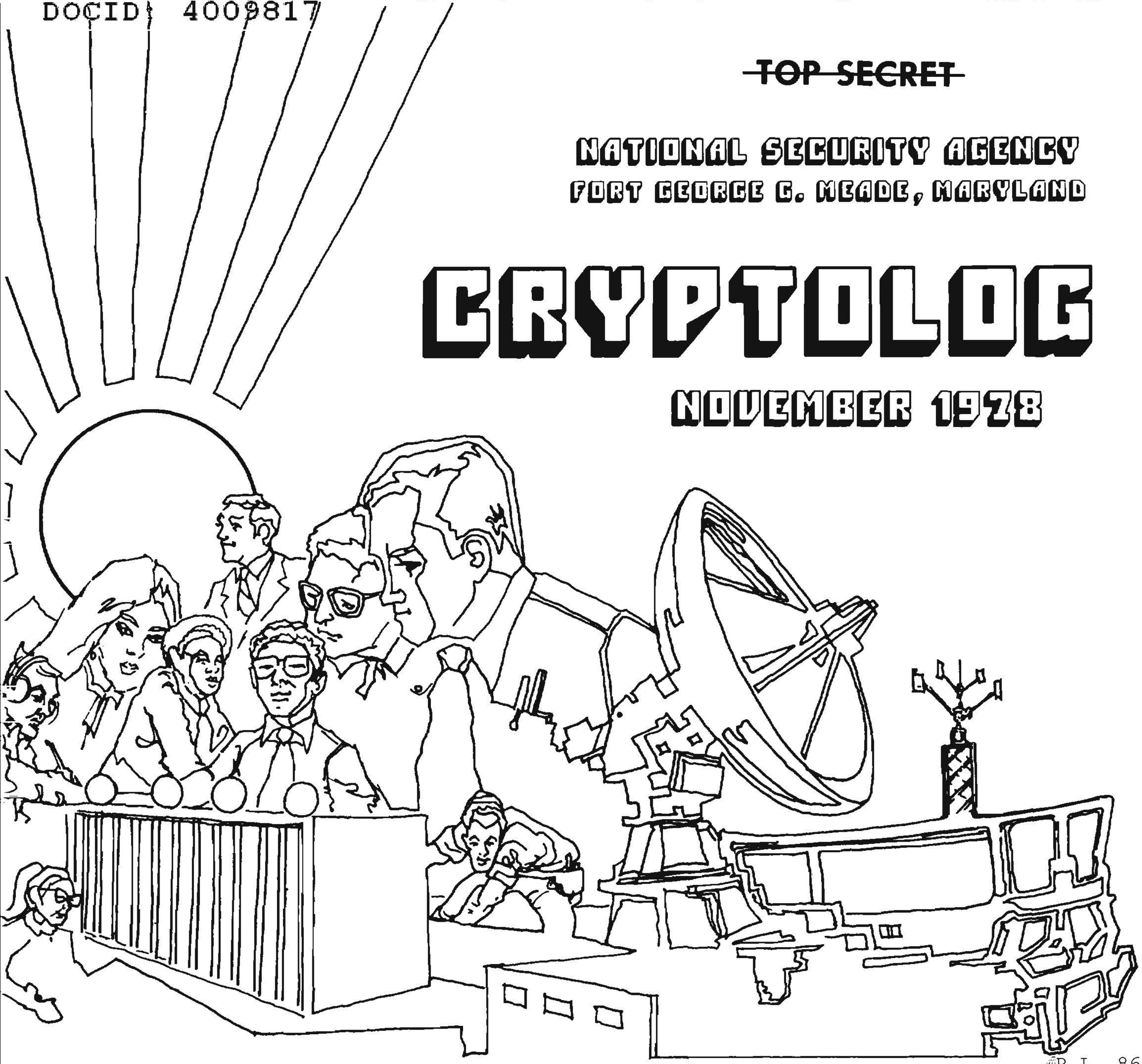
DOCID: 4009817

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOVEMBER 1978



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

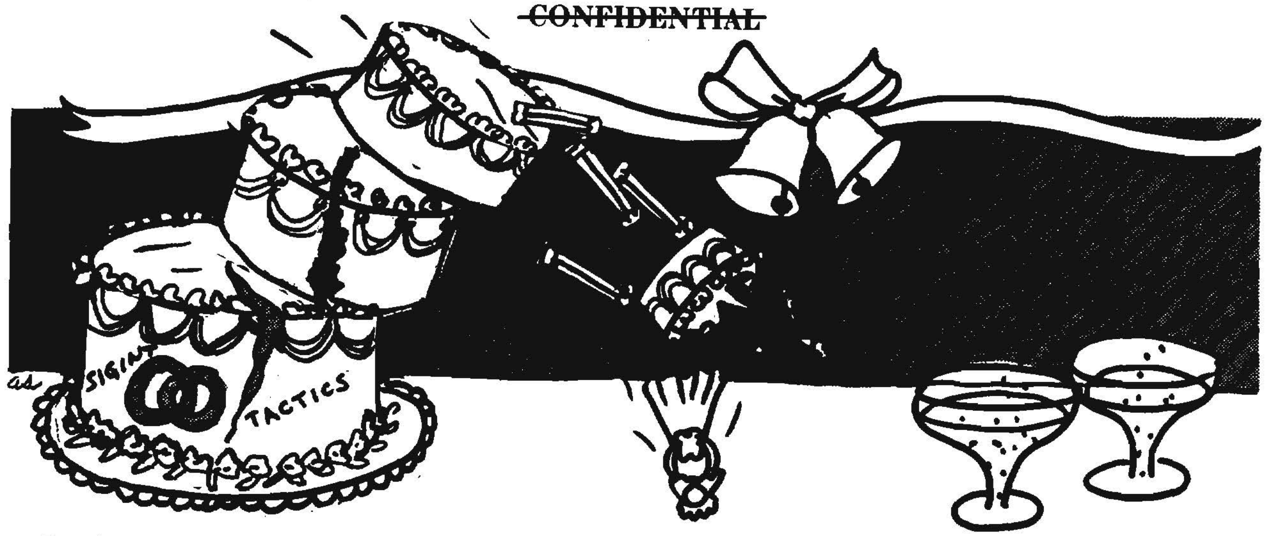
VOL. V, NO. 11 NOVEMBER 1978

PUBLISHER WILLIAM LUTWINIAK

P.L. 86-36

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~CONFIDENTIAL~~



Wedding Bells and That Old Gang of Mine

E. LEIGH SAWYER, B4

[redacted]

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

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

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

[redacted]

[redacted]

~~(C - CCO)~~

A SMALL PROBLEM

[redacted] P14

P.L. 86-36

[redacted]

[redacted]

~~(C)~~

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

YES, CRYPTOLOG READERS, N.S.A. DOES HAVE A

DATA STANDARDS CENTER

Mark T. Pattie, Jr., P13D (NDSC)

Before I tell you what the NSA Data Standards Center (NDSC) does, perhaps I should explain why we do it. One very good reason is that a previous director, VADM Noel Gayler, established the NDSC by direction on 1 January 1971. This was later formalized by the reissuance in May 1972 of NSA Regulation 80-9, the NSA Program for Standardization of Data Elements and Related Features.

That would be reason enough to have a Center, of course, but there is more. The NDSC is really the element responsible for the Agency portion of the Department of Defense Data Standards Program, which had its beginnings in DoD Directive 5000.11 when that document was published on 7 December 1964. We also work closely with the National Bureau of Standards, which, under Executive Order 11717 of 9 May 1973, is responsible for government-wide automatic data processing standards. By "work closely" I mean that NDSC personnel are often in touch with people from the DoD and other government agencies on data standards matters and they take part in interagency committees and working groups as the NSA representatives to their meetings. All of this comes under NSA Regulation 80-9, which names the NDSC as the Agency point of contact for federal, DoD, and other external programs or efforts for data standardization. One example of our committee work is our participation on the Data Standards Panel of the Intelligence Information Handling Committee of NFIB.

But even if we did not have the official reasons for establishing an NSA Data Standards Centers, there would still be the practical reasons for it. It must make good sense to have data standards instead of Babel and it even saves money. Let me illustrate:

$x + y = 7$ $\quad\quad \pi r^2 \quad\quad$ $a^2 + b^2 = c^2$

Would it make any difference in working with these elements if I were in Germany instead of the United States? Or in Italy? Or in Sweden? No, for everyone recognizes that these are mathematical symbols, which are standard around the world.

How about another example?

Speed Limit 50

Well, right away I suspect some readers will be uneasy. Here it does make a difference, for we have to know if speed is measured in miles, in kilometers, or whatever.

And so it goes. In order to communicate with one another, we have to use terms that are mutually understandable. That holds true whether we are talking about listening to a foreign language broadcast or trying to read a technical journal for which we have no background. In the various sciences there is much that is mutually understandable between scientists of different nationalities even with their language differences, whereas laymen within the same country would be at a loss to understand what is said or written.

Incidentally, I do not know whether any of you are aware of it, but some of those who are to all intents and purposes the most handicapped in the art of communication -- those who cannot hear or speak -- have the least trouble with the foreign-language barrier. They use symbols -- hand signs -- which are international standards and they can make themselves understood in any country where sign language is practiced. The hand signs are, in fact, data standards which have the same meaning, for the most part, in the language of whatever country they happen to be in or from. Of course, they might have trouble spelling words that are foreign to them but they are still better off than most of us who claim to have all our faculties.

A certain amount of data standardization is taking place around us all the time. I am referring to expressions that once were unique to particular parts of the United States at one time but which are now becoming rare. Those who make studies of such things were able to pinpoint the birthplace of almost anyone just by asking that person to pronounce about ten different words or to provide the words or terms used for certain objects or actions. For example, how do you pronounce the following words when you are "back home": BUSH/PUSH, HOG, GREASY, MERRY/MARY/MARRY.

Or what do you cook your breakfast eggs in? A FRYING PAN/FRY PAN, SKILLET, or SPIDER? And what's that big piece of furniture in your LIVING ROOM/PARLOR? -- a SOFA, COUCH, DIVAN, or DAVENPORT? How do you pronounce PARK YOUR CAR if you're from the Boston area? How do you say WATER, wherever you're from?

Such regional differences are largely falling by the wayside, perhaps because of the omnipresent TV screen and the nationwide distribution of TV programs. Or it might be because people no longer live out their years in the areas where they were born: we are a mobile nation.

Whatever the cause, data standardization seems to be with us, whether we like it or not. It is a fact of life. I'll admit that I look upon this leveling of the American idiom with a certain amount of regret. We are losing some of our rich heritage in language and I think we will be the poorer for it.

But the NDSC is not as concerned with the exchange of information between individuals as it is with the exchange of information between machines or between a machine and a terminal. Here standardization should be a way of life but it is not. There are just too many examples of Agency elements blithely going their own ways regardless of the fact that they are duplicating the work of another element, or, what is worse, establishing their own standards when Agency standards already exist.

Perhaps I should define the term "data standards." Although some readers may know what the term means, I suspect that many do not. By "data standards" we mean consistent, agreed-upon names, descriptions, and codes for categories of data that will ensure unambiguous understanding in data processing and data interchange.

Note two things in that definition. I did not use the word "cryptologic" and I ended with the words "date processing and data interchange." The NDSC is concerned with data standards in *all* fields, both cryptologic and noncryptologic. And, basically, we are trying to come to agreements about definitions that will make data machine-insertable and machine-extractable.

The latter point is essentially what distinguishes data-standards work from that in SIGINT terminology, for which the NDSC is also responsible. In SIGINT terminology we seek to build a SIGINT Terminology Data Base (STDB) and glossaries for each cryptologic field. These will contain terms that are defined in such a manner that they show the currently accepted meanings. One way of making the distinction between standard terminology and data standards is to say that the definitions for the latter are more precise than those for standard glossaries. People have less trouble interpreting nuances in meaning than do machines.

Let me give you a simple example of what we mean about the difference between the two. If we were going to put in a definition for DATE, we could use a definition from a general desk dictionary for our terminology data base.

> "DATE: 1. A statement or formula affixed that specifies the time of execution or making (as *a letter bearing the date 3 January 1856*).
>
> 2. The point of time at which a transaction or event takes place or is scheduled to take place."
>
> (*Webster's Third New International Dictionary*)

Our Data Standards description is from the *NSA Manual of Standard Data Elements and Related Features* (Annex A to USSID 412):

> "00012
>
> "DATE: The years, months and days of the Gregorian calendar.
>
> DATA ITEMS: Represented by 6 digits, unspaced, left to right: 2 for year, 2 for month (01-12), 2 for day (01-31). (E.g., 15 January 1969 would be 690115)."

You will note that the Data Standards description has measurable factors while the Terminology definition does not.

The NDSC is not an ivory tower where we "do our thing" away and apart from the rest of the NSA world. No, we work very closely with other people. For instance, every major component of the Agency has a representative who works with the NDSC staff in identifying, researching, and approving data standards and SIGINT terms. The Senior Data Representatives and Senior Terminology Representatives, in turn, work with other contacts at lower echelons in their own organizations in the proposing and coordinating phases. We may meet with the SDRs or the STRs as a group or as individuals, depending on the problem of the

The name "Data Standards Center" itself is something of a misnomer, for the NDSC is deeply involved in more than just data standards for machine processing of information. In the terminology program, people working on the development of the SIGINT Terminology Data Base provide guidance on the development and use of terms for SIGINT concepts and their accompanying definitions, maintain a central collection of reference materials on SIGINT terms, and develop a common glossary format for SIGINT glossaries published as appendices to USSID 412. Our SIGINT terminology program is unique within the Intelligence Community.

In the creation of SIGINT glossaries the NDSC terminology people work closely with the appropriate terminology panels to develop the necessary documentation. The Center, working with the Traffic Analysis Terminology Panel, developed a draft TA Glossary which is now being coordinated with certain elements and our people are working with the Signals Collection Terminology Panel on a draft glossary for that field. Terminology personnel are also working with T personnel on a Telecommunications Glossary and with the TEBAC people on a Telemetry Analysis Glossary. In the near future we plan to start work on a Data Processing Glossary, while those for other cryptologic fields and an interdisciplinary glossary will be developed as time and resources permit.

P.L. 86-36

One person concentrates on Multiple Use standards -- those that are essentially noncryptologic, like personnel or budget standards. The work involves coordination and many meetings with people outside the Agency -- from the Civil Service Commission and the U.S. Air Force, for example. Inside NSA our Multiple Use expert works mostly with personnel from E, L, M, N, or T, but the problems may be of such a nature that they concern the entire Agency.

The NSA Data Standards Center has developed a centralized file of data elements/data field definitions. This file, [redacted] serves as a repository of all the published standards for SIGINT activities [redacted] plus other data elements that are being used in DDO files and elsewhere without being standards. This file will help us to identify data elements that are eligible to be proposed as SIGINT data standards.

[redacted] may eventually become a part of Project UTENSIL, the DDO Data Dictionary/Directory that was envisioned by DDO managers in 1976. A task force, created under the leadership of the NDSC, drew up a charter for a dictionary that was to contain data elements and their meanings; the directory was to give control functions, file names, etc. In the meantime, several DDO elements have proceeded to develop their own Data Dictionaries, unfortunately with little regard for standardization, so their terms are quite often incompatible with those for another DDO dictionary and some times even with their own particular group.

[redacted]

In 1972 Harold Shaklee, then Chief of the NSA Data Standards Center, and George Hicken, COINS Project Manager, met and agreed that the NSA Air Movements files in COINS would be standardized. On 7 September 1972 Mr. Shaklee convoked a meeting of a Working Group of 22 people, most of whom represented the various Agency elements concerned with the appropriate files. [redacted]

It is unfortunate that those developing the [redacted] files in the early days did not take the time to look into the work of others before building their own unique files. The trouble with that statement is that I know that exclusive files are being created right at this moment and the lesson learned when the COINS users tried to query the [redacted] files seems to have been wasted. Some of those files are being built right within the same organization.

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

And even the limited progress we have seen in getting the [redacted] files in COINS standardized for NSA is tempered by the knowledge that many other NSA files need work and we still have not attacked the problem of standardization across the Community. In a 1976 [redacted]

P.L. 86-36

In Vol. II of the same study, on page 47, types of user problems are cited:

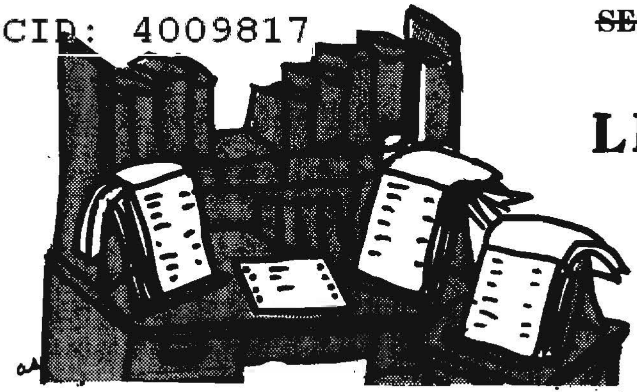
> "a. They must use different codes, acronyms and abbreviations for referencing like fields of information in different files. They experience frustration both in framing interrogations and in interpreting answers.
>
> "b. Users must cope with more than one set of data item codes for a common data element.
>
> "c. They must have access to a variety of working aids in preparing interrogations or in translating answers into meaningful information."

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

In closing, I would just like to say that although the NSA Data Standards Center can be justifiably proud of its accomplishments in standardizing Data Elements within the Agency, we are all too aware of the fact that we have barely scratched the surface.

The second point I would like to leave with you is that we covet your cooperation. If you don't work closely with us in the effort to reduce the data maze in the Agency, all our attempts to improve data standards will become little more than a treadmill operation -- no progress, but a lot of work just to keep abreast of the problem.

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



LINGUISTICS AND THE CODE RECONSTRUCTOR

STUART H. BUCK, P16 (Retired)

Let me hasten to point out that I make no pretensions to more than a very limited knowledge of modern linguistic theory. It was my fate to be born several decades too soon. By the time I entered college, language majors were expected to delve deeply into literature and history, but that was about it. Philology, as it was called then, was regarded as a field for specialists, not as a requirement for an AB in Romance Languages. I remember once suggesting, rather timidly, that I would like to take a one-semester course in phonetics. My tutor knocked that one down quickly. Such an aberration, he pointed out, would conflict with a course on Voltaire, which would stay with me longer. He made it sound like a steak dinner. And so the advent of Bloomfield and his disciples caught me preoccupied, first with Voltaire, and then with the Great Depression, when it didn't seem to make any difference what kind of linguist you were -- everyone suffered equally. I can make one small claim to fame, however. Carl Darling Buck, the great philologist, and I are distantly related. Moreover, Carl Buck was Leonard Bloomfield's teacher. That ought to count for something. I wish that I could settle for that, but total candor compels me to reveal that my learned relative and I share a common ancestor, one Colonel Jonathan Buck, who is reputed to have burned a witch back in the 18th century. So much for name-dropping. . .

I have mentioned all of this in order to explain why I was such a late-bloomer in the field of linguistics. It wasn't until I arrived at Arlington Hall over 30 years ago that I realized something was going on that I very little about. After the war, I received some free benefits when my older brother decided to get his PhD in linguistics. He not only tested each theory on me, but passed on many of his textbooks, hoping that they would do me some good. In self-defense, I began to read through them. I started with Bloomfield -- and discovered that there was a whole new world waiting out there. Then I read Bloch and Trager, and found them informative, but not likeable. While this sort of desultory reading was going on, I became deeply involved in bookbreaking -- or, to use a term that I prefer, *code reconstruction*. Before I retired in 1973, I had worked on a great variety of codes, [redacted] I know that this sounds boastful, so I shall hasten to add that I still consider myself a novice in the field. I have seen a lot, but not all, of the elephant, so give me credit for being aware of that gloomy fact. One result of all this knocking around was that I acquired a compulsion to talk and write about my experiences, remembering that when I started out, no one told me anything. Not a word was uttered in my presence regarding tools, techniques, or standards. The implication was that either you could do it or you couldn't -- it was just as simple as that.

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

Plopped into My First Assignment

[redacted]

Throughout most of my career, I have been a loner. On the few occasions when I have worked with another bookbreaker, I have discovered a curious reluctance on his or her part to talk about methodology. Usually it was a case of "That's what it means because I say so" or "If you challenge my results, you attack me

Stu Buck retired from NSA in 1973 but returned to P16 several days a month as a reemployed annuitant to work on a special project requiring his unique qualifications. When he was finally debriefed at the conclusion of that project in October 1977, he handed over to a few coworkers copies of papers they might still find useful. Among those papers was the text of a talk Stu had given in September 1974, which is published here as sound words of advice for the next generation of people to carry out what Stu calls "one of the basic missions of the Agency."

Ed.

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

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

as a person." After you have had your head bitten off a few times, you tend to be less talkative -- unless you enjoy name-calling for its own sake. In my experience, the great exception to this cantankerous type was Betty Doane. May she rest in peace! Betty was not only completely honest, but was not afraid to lay all her cards on the table. She never hid behind a mystique, and there was no chip on her shoulder as big as a plank. Everything was out in the open for all the world to see (those with proper clearances, I hasten to add). She was feisty, tough-minded, completely logical in all of her arguments, and she never used arrogance as a shield for ignorance or insecurity. For that, I remember her with a special reverence. . .

[redacted]

[redacted]

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

[redacted]

P.L. 86-36

Q & A:

A DIALOGUE BETWEEN MS. USER AND DR. ANALYSIS

[redacted] R51

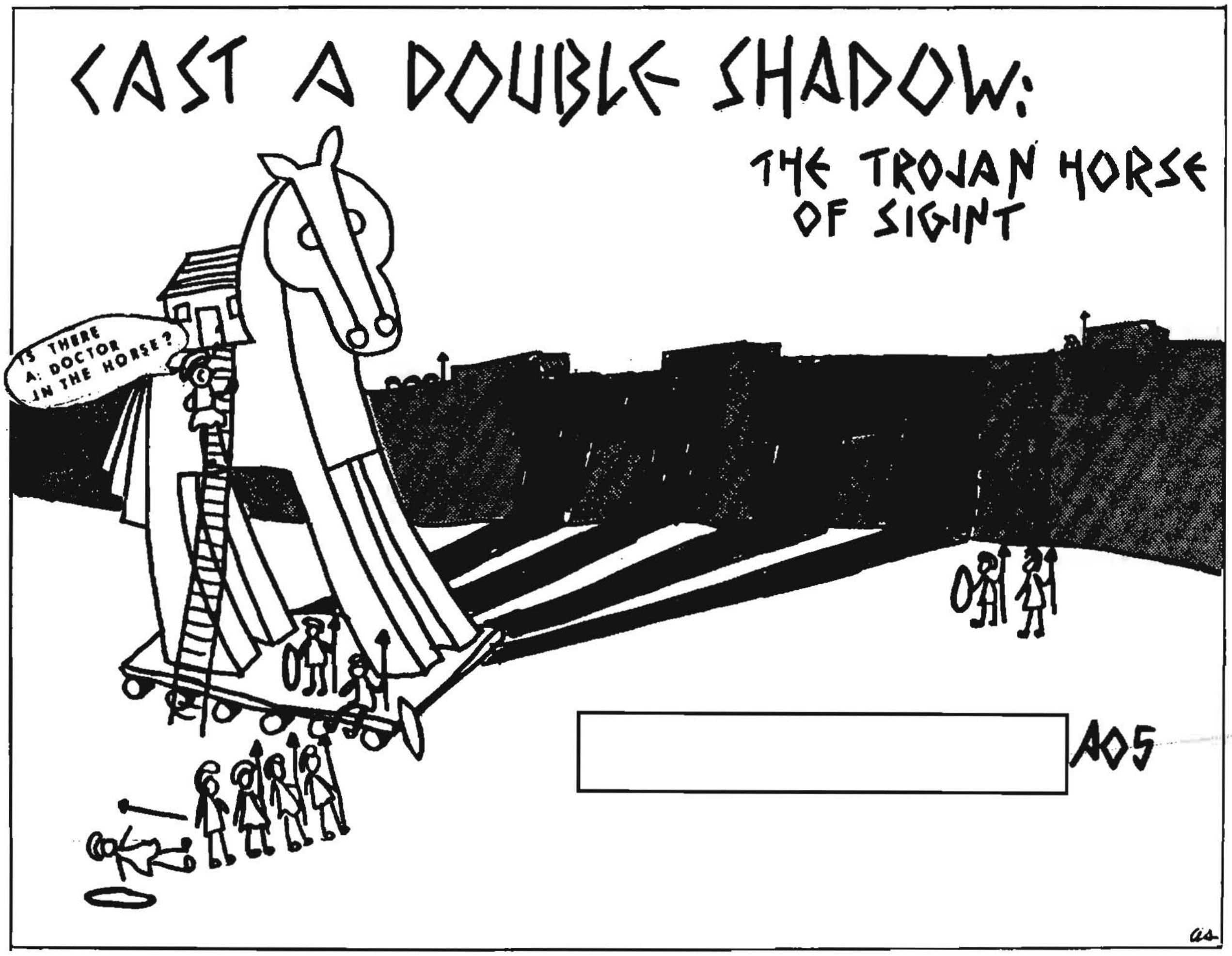
[redacted]

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

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

[redacted]

CAST A DOUBLE SHADOW: THE TROJAN HORSE OF SIGINT



[redacted] A05 P.L. 86-36

Among the leading attributes of COMINT, according to its past and present practitioners, are the dual qualities of timeliness and authenticity. SIGINT support to tactical military commanders is contingent on these two characteristics, while a wealth of combat and peacetime applications have borne out this unique dependency on the intelligence source known in the open literature as "intercepts." Only recently, in the works of Kahn, Winterbotham, and Brown, has the public been told the story of the central, critical role played both by COMINT and by radio strategems in World War II and in the Allied victory. In fact, so consummately has this story been told that it is now necessary to revise history in light of information only recently made available to scholars. Here we see journalists, and a former SSO, in the role of historical revisionists -- not a new role for journalists, but certainly a new role for SSOs, at least in the open literature.

Dependency on SIGINT's timeliness, authenticity, and -- oft-times -- uniqueness is unsettling. The quality of "believability" or creditability -- the much sought A1 source -- is fraught with potential disaster, as Brown's *Bodyguard of Lies* convincingly demonstrates, even to the most skeptical reader. Creditability is everywhere and at once a two-edged sword.

[redacted]

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

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

[redacted]

FORMATTING PL/I SOURCE CODE

[redacted] P16 P.L. 86-36

IBM's Programming Language One (PL/I) is an extremely large and complex higher-level language, even by the standards of programming languages being designed today. To the novice this language is presented either in a watered-down version, sort of a "new style" of FORTRAN, or in such detail that the novice is quite easily overwhelmed. One would expect (as in fact is the case) that the compilers which process this complex source are themselves complex and they, too, are often presented in the same two extremes to the inexperienced user. Either one uses with faith a set of mysterious "JCL" which has been passed around the office and takes for granted that this JCL is in some now-unknown sense optimal, or one obtains one of the compiler guides and attempts to wade through the wealth of information presented there. To aid the PL/I programmer, two catalogued procedures have been developed which allow the programmer to maximize the amount of useful information on the job listing and to have that information arranged and formatted in a highly readable way. These procedures have also been designed to be easily used: each requires only one JCL card.

The PL/I Compilers

Unlike most other higher-level languages, PL/I is supported by two distinct compilers. One compiler, the Checkout compiler, provides very detailed and elaborate diagnostics in addition to, in some sense, acting as a PL/I interpreter. It is not too incorrect to consider that the Checkout compiler interprets PL/I code, while checking subscript bounds for array references, string ranges for substring operators, the attempted use of uninitialized variables, etc., in addition to "trapping" many system-level errors (e.g., overflow or underflow, transmission errors, etc.) and providing diagnostic information before the standard system action is taken. The facilities of the Checkout compiler can be invaluable for program development.

The user, however, "pays" for the extensive checking and debugging aids of the Checkout compiler in increased execution time. For this reason another compiler, the Optimizing compiler, is used for the final compilation before the program is used in production. This compiler attempts to optimize (either time-optimize or space-optimize) the resulting object module by eliminating both common and redundant expressions, replacing in-line code for library function calls, and analyzing DO groups to allow for optimal object coding for some special cases. The Optimizing compiler can substantially reduce the execution time of a PL/I program compared to the old PL/I(F) compiler and, as was stated earlier, the Checkout compiler. It will not, however, check for certain types of user errors such as the use of uninitialized variables. It is precisely these types of errors that can return to haunt the programmer, or, more probably, the person now in charge of maintaining someone else's old program with an unexplained abnormal termination after months of successful production use. The use of the Checkout compiler in program development can reduce the occurrence of such errors.

KENSPL1 and KURTSPL1

A large number of compilation options exist for each compiler. These options vary from those that govern the amount and type of information on the job listing to those that determine the amount of optimization to be done or debugging aids to be included. The proper use of these options will allow the user to get the most out of any particular debug run, or will allow the programmer who has to modify some old source code to understand the program logic as easily as possible. The catalogued procedure KENSPL1[1] does a PL/I compile, link-edit and execution using the Optimizing compiler, and KURTSPL1[2] does the same thing with the Checkout compiler. Both these procedures have been designed to be used by the novice, so that the following JCL is all that is required:

```
//name JOB       (standard JOB card)
//  EXEC KENSPL1    (or KURTSPL1)

             [PL/I SOURCE]

//
```

So, in essence, the user need remember only one JCL card, the EXEC statement.

KENSPL1[3] formats the PL/I source using the standard PL/I format conventions, e.g., DO groups and the THEN and ELSE clauses of IF ... THEN ... ELSE statements are indented, statement labels are highlighted, etc. Comments can be formatted in three different styles, all under the control of the individual programmer. The formatting of the entire source is done in a 100-column-wide section of the listing, allowing for complex PL/I statements to be listed in one line. The block and DO-group nesting level prefaces each statement. Commonly used PL/I abbreviations (E.G., DCL, PROC, PTR, DEF,

[1] KENSPL1 is named in honor of [redacted] a former Agency employee. P.L. 86-36

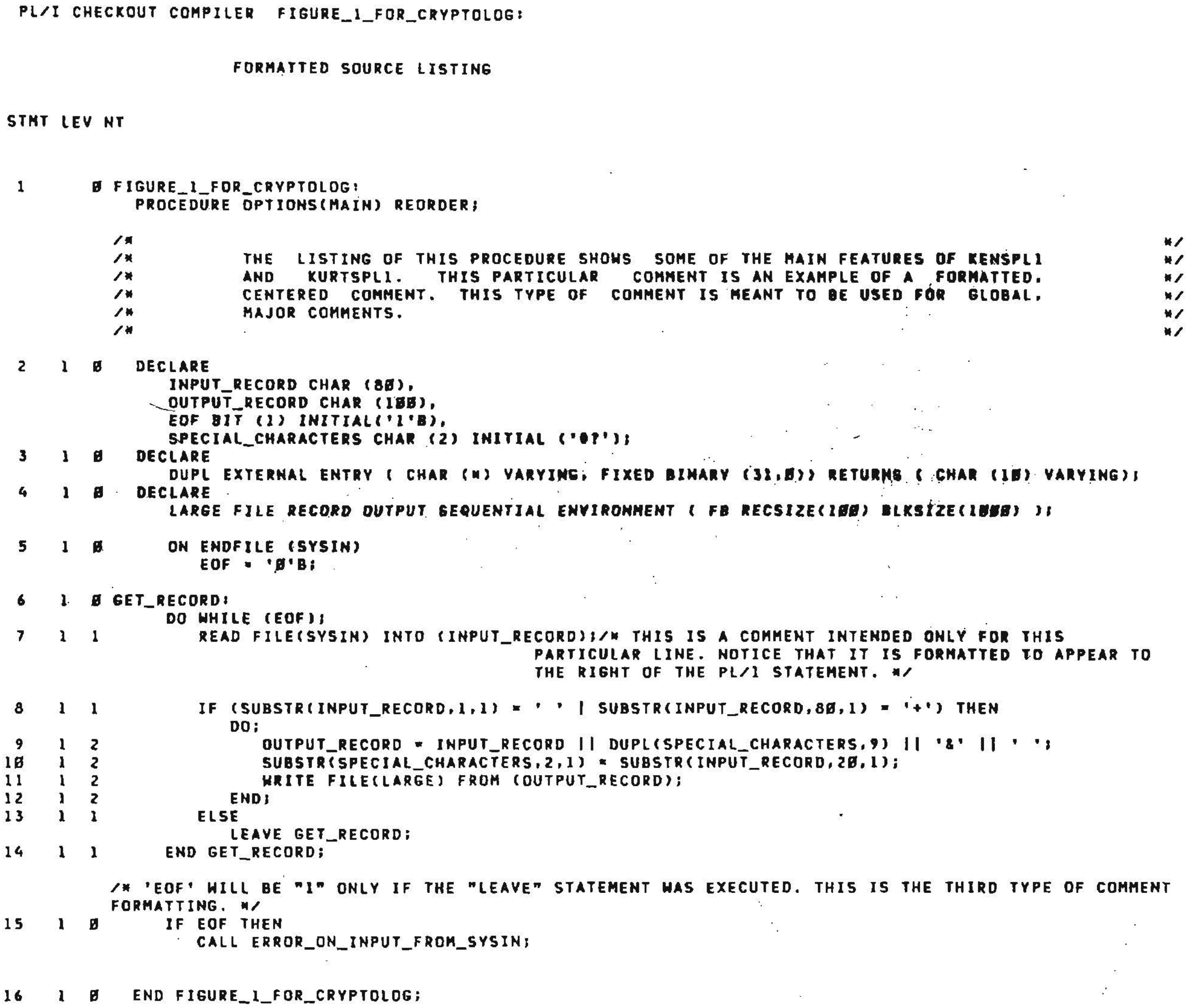
[2] Guess!

[3] Since both KENSPL1 and KURTSPL1 produce the same output, only KENSPL1 will be discussed from this point on.

etc.) are expanded for greater readability. The equal sign, when used as an assignment operator, is separated from the target and source variable by a blank. In addition one can use imbedded listing control statements (e.g., %SKIP, %NOPRINT, etc.). (Here, "imbedded" means occurring in the same source record as a regular PL/I statement.) Without KENSPL1 this feature is not supported by the Optimizing compiler.

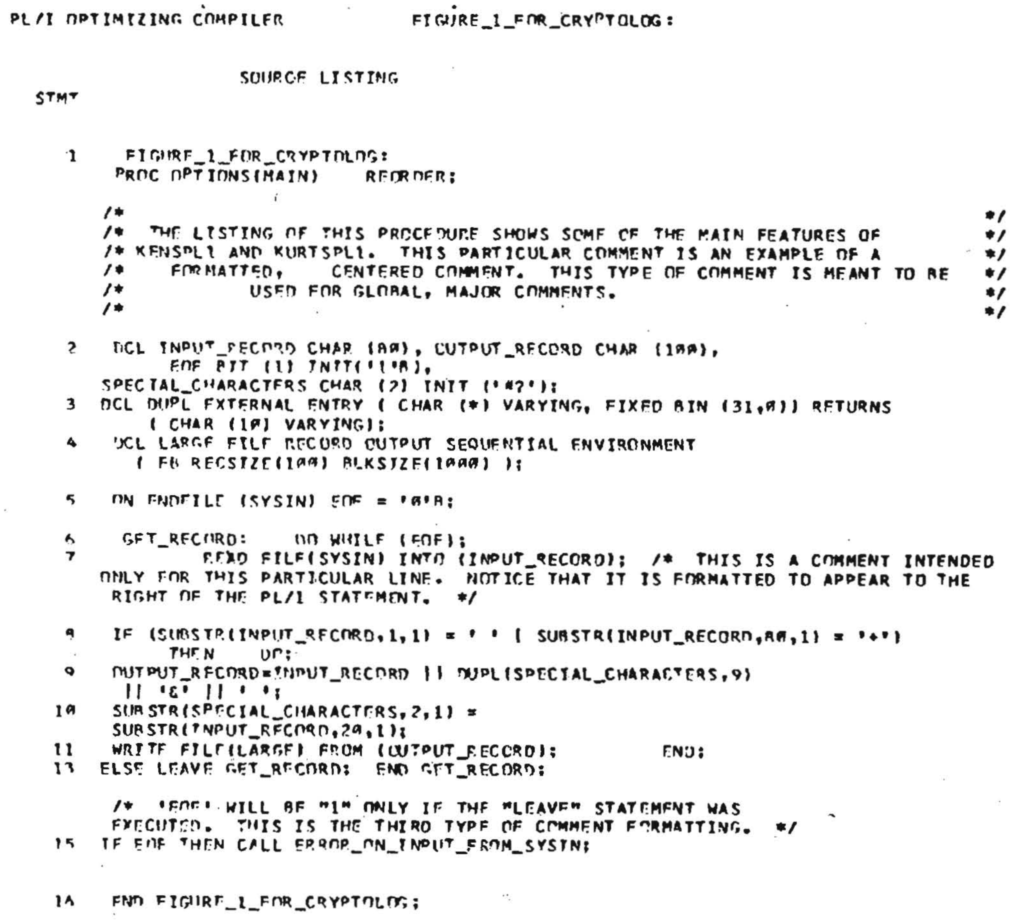
This automatic formatting allows the logic of the program to be seen more easily both by the program designer and, more importantly, the programmer in charge of program maintenance. It also frees the designer from the work of "hand-formatting" a source file and the person in charge of maintenance from the errors of any incorrect "hand-formatting." When this automatic formatting is used in conjunction with the DO levels, the correct location of missing or misplaced END statements can be quickly determined as well as some common program-design errors.

An alphabetical list of all variables used in the program follows the source listing. For each variable, this list contains all the attributes of the variable, whether declared or assumed by default, and a list of each statement (by statement number) where this variable is referenced. In addition a table of all the arrays and structures used in the program is listed along with information concerning the number of dimensions, size and alignment in storage. To aid in debugging and hand-optimization, KURTSPL1 also produces a table listing the number of times each statement in the source was executed. An example showing the output of KENSPL1 vs. the standard IBM procedure, PLIXCLG, is shown in Figs. 1a and 1b.



```
 PL/I CHECKOUT COMPILER  FIGURE_1_FOR_CRYPTOLOG:

                    FORMATTED SOURCE LISTING

STMT LEV NT


 1        Ø FIGURE_1_FOR_CRYPTOLOG:
              PROCEDURE OPTIONS(MAIN) REORDER;

            /*                                                                        */
            /*          THE  LISTING OF THIS PROCEDURE SHOWS  SOME OF THE MAIN FEATURES OF KENSPL1     */
            /*          AND   KURTSPL1.   THIS PARTICULAR   COMMENT IS AN EXAMPLE OF A  FORMATTED.     */
            /*          CENTERED  COMMENT.  THIS TYPE OF  COMMENT IS MEANT TO BE USED FOR  GLOBAL,     */
            /*          MAJOR COMMENTS.                                                   */
            /*                                                                        */

 2    1   Ø   DECLARE
                 INPUT_RECORD CHAR (8Ø),
                 OUTPUT_RECORD CHAR (1ØØ),
                 EOF BIT (1) INITIAL('1'B),
                 SPECIAL_CHARACTERS CHAR (2) INITIAL ('0?');
 3    1   Ø   DECLARE
                 DUPL EXTERNAL ENTRY ( CHAR (*) VARYING, FIXED BINARY (31,Ø)) RETURNS ( CHAR (1Ø) VARYING);
 4    1   Ø   DECLARE
                 LARGE FILE RECORD OUTPUT SEQUENTIAL ENVIRONMENT ( FB RECSIZE(1ØØ) BLKSIZE(1ØØØ) );

 5    1   Ø      ON ENDFILE (SYSIN)
                    EOF = 'Ø'B;

 6    1   Ø GET_RECORD:
                 DO WHILE (EOF);
 7    1   1         READ FILE(SYSIN) INTO (INPUT_RECORD);/* THIS IS A COMMENT INTENDED ONLY FOR THIS
                                                    PARTICULAR LINE. NOTICE THAT IT IS FORMATTED TO APPEAR TO
                                                    THE RIGHT OF THE PL/1 STATEMENT. */

 8    1   1         IF (SUBSTR(INPUT_RECORD,1,1) = ' ' | SUBSTR(INPUT_RECORD,8Ø,1) = '+') THEN
                       DO;
 9    1   2               OUTPUT_RECORD = INPUT_RECORD || DUPL(SPECIAL_CHARACTERS,9) || '&' || ' ';
1Ø    1   2               SUBSTR(SPECIAL_CHARACTERS,2,1) = SUBSTR(INPUT_RECORD,2Ø,1);
11    1   2               WRITE FILE(LARGE) FROM (OUTPUT_RECORD);
12    1   2            END;
13    1   1         ELSE
                       LEAVE GET_RECORD;
14    1   1      END GET_RECORD;

            /* 'EOF' WILL BE "1" ONLY IF THE "LEAVE" STATEMENT WAS EXECUTED. THIS IS THE THIRD TYPE OF COMMENT
            FORMATTING. */
15    1   Ø      IF EOF THEN
                    CALL ERROR_ON_INPUT_FROM_SYSIN;


16    1   Ø   END FIGURE_1_FOR_CRYPTOLOG;
```

Fig. 1a. Source listing using KENSPL1



```
PL/I OPTIMIZING COMPILER          FIGURE_1_FOR_CRYPTOLOG:

                     SOURCE LISTING
  STMT

     1     FIGURE_1_FOR_CRYPTOLOG:
          PROC OPTIONS(MAIN)     REORDER;

         /*                                                                       */
         /*   THE LISTING OF THIS PROCEDURE SHOWS SOME OF THE MAIN FEATURES OF   */
         /* KENSPL1 AND KURTSPL1.  THIS PARTICULAR COMMENT IS AN EXAMPLE OF A     */
         /*    FORMATTED,     CENTERED COMMENT.  THIS TYPE OF COMMENT IS MEANT TO BE  */
         /*            USED FOR GLOBAL, MAJOR COMMENTS.                           */
         /*                                                                       */

     2    DCL INPUT_RECORD CHAR (8Ø), OUTPUT_RECORD CHAR (1ØØ),
               EOF BIT (1) INIT('1'B),
         SPECIAL_CHARACTERS CHAR (2) INIT ('#?');
     3   DCL DUPL EXTERNAL ENTRY ( CHAR (*) VARYING, FIXED BIN (31,Ø)) RETURNS
              ( CHAR (1Ø) VARYING);
     4    DCL LARGE FILE RECORD OUTPUT SEQUENTIAL ENVIRONMENT
            ( FB RECSIZE(1ØØ) BLKSIZE(1ØØØ) );

     5    ON ENDFILE (SYSIN) EOF = 'Ø'B;

     6     GET_RECORD:     DO WHILE (EOF);
     7              READ FILE(SYSIN) INTO (INPUT_RECORD);  /*  THIS IS A COMMENT INTENDED
         ONLY FOR THIS PARTICULAR LINE.  NOTICE THAT IT IS FORMATTED TO APPEAR TO THE
          RIGHT OF THE PL/1 STATEMENT.   */

     8    IF (SUBSTR(INPUT_RECORD,1,1) = ' ' | SUBSTR(INPUT_RECORD,8Ø,1) = '+')
               THEN     DO;
     9    OUTPUT_RECORD=INPUT_RECORD || DUPL(SPECIAL_CHARACTERS,9)
           || '&' || ' ';
    1Ø    SUBSTR(SPECIAL_CHARACTERS,2,1) =
          SUBSTR(INPUT_RECORD,2Ø,1);
    11    WRITE FILE(LARGE) FROM (OUTPUT_RECORD);          END;
    13   ELSE LEAVE GET_RECORD;  END GET_RECORD;

          /*  'EOF' WILL BE "1" ONLY IF THE "LEAVE" STATEMENT WAS
          EXECUTED.  THIS IS THE THIRD TYPE OF COMMENT FORMATTING.  */
    15   IF EOF THEN CALL ERROR_ON_INPUT_FROM_SYSIN;


    16    END FIGURE_1_FOR_CRYPTOLOG;
```

Fig. 1b. Source listing using PLIXCLG

In the link-edit step KENSPL1 also frees the user from concern about details that are almost always unimportant to the user. Subroutine calls to any of Nolan's Extended String Functions[4] or the Integrated Graphics Software (IGS) are automatically resolved without the special inclusion of any additional system library data definition ("DD") cards. In addition the link-edit cross-reference table is deleted from the listing. It is felt that this table provides little, if any, information to even experienced application programmers and in general "clutters up" the listing.

As with the extra facilities of the Checkout compiler, the features of KENSPL1 do not come free to the user. Table 1 gives an indication of the additional amount of CPU time required for KENSPL1 vs. PLIXCLG. While these figures can be used as a rough guide, the actual time for any given execution depends on the number of formatted comments, the number of instances of keywords to be expanded, the number of listing control statements, etc. This amount of extra machine processing is more than compensated for by shorter development time and easier program maintenance.

Table 1

Source description	*Extra CPU time using KENSPL1 rather than PLIXCLG**
FIGURE_1_FOR_CRYPTOLOG	1.45 sec
Medium-sized source (about 300 statements; extensive use of comment formatting)	5.46 sec
Large source (more than 700 statements; extensive use of all features)	8.27 sec

* Based on a sample of five runs for each procedure.

[4] [redacted] *Extended String Functions for PL1*, R51/PROG-NOTE/04/77, 13 July 1977.

NSA-crostic No. 19

By David H. Williams, P16

The quotation on the next page was taken from the published work of an NSAer. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS	*WORDS*
A. Central character in "Tobacco Road" (2 wds)	208 223 12 237 41 137 71 25 168 203 193 83
B. Real name of Sweden's greatest gift to American movies (2 wds)	156 23 57 231 10 27 78 188 115 50 175 101 43 96 219
C. Was (3 wds)	209 7 102 112 46 22 194 146
D. Giving of new life	37 127 119 3 139 154 77 54 110 91 187 28 73 67
E. Followed by word W, what Word B claims she *really* said (5 wds)	234 44 227 87 211 21 72 39 30 196 180 158
F. Poisonous plant which yields a heart medicine	75 33 161 117 221 107 130 86 70 63
G. Most fortunate	4 92 109 74 144 166 178 191
H. Deprive of possession	165 58 36 9 65 147 32 184 16 133 131
I. The Lone Ranger's great-grandnephew, Britt Reid (3 wds)	80 159 232 235 103 122 113 26 179 149 141 17 214 200
J. Having the gift of finding valuable things not sought for	116 238 121 229 155 182 138 213 197 8 94 106 163
K. Called, named (archaic)	169 98 220 162 84
L. Card game; cheat	69 6 224 222 215 135
M. Abpu Ben -----	48 128 201 120 51
N. Illness characterized by inflammation or pain of the joints and muscles	228 85 152 124 60 216 88 45 172 15
O. One (Japanese)	177 150 192 160
P. Kipling's first poem (4 wds)	11 236 31 40 111 226 143 93 217 13 59 126 199 181 104 53 82 153
Q. Corporate name which might result from the merger of Fairchild and Honeywell ((2 wds)	49 108 218 239 142 151 62 125 186 38 34 195 64 20 81 225 99 136
R. "Pressed into service means pressed out -------." Frost, "The Self-Seeker," 1914 (2 wds)	173 18 207 176 157 164 100

S. Correct — 56 206 35 89 1

T. Capet, Herbert, or Downs — 47 170 185 134

U. Adjective for Uriah Heep — 66 42 97 5 68

V. Xylophonist's nonhostile stance, profile to the audience: "with -----------------" (3 wds) — 95 19 183 233 140 171 123 230 105 129 55 148 167 114 212 29 198

W. See Word E — 118 145 76 132 90

X. Flagrantly wicked or impious — 190 205 174 202 79 52 2 14 210

Y. Send — 24 204 189 61

1 S	2 X	▨	3 D	4 G	5 U	6 L	7 C	8 J	9 H	10 B	11 P	12 A	▨	13 P	14 X
15 N	16 H	17 I	▨	18 R	19 V	20 Q	21 E	22 C	23 B	24 Y	▨	25 A	26 I	27 B	28 D
29 V	30 E	31 P	32 H	33 F	34 Q	35 S	▨	36 H	37 D	38 Q	39 E	40 P	41 A	42 U	43 B
▨	44 E	45 N	46 C	47 T	▨	48 M	▨	49 Q	50 B	51 M	52 X	53 P	54 D	55 V	56 S
▨	57 B	58 H	59 P	60 N	61 Y	62 Q	63 F	▨	64 Q	65 H	66 U	▨	67 D	68 U	69 L
70 F	▨	71 A	72 E	73 D	74 E	▨	75 F	76 W	▨	77 D	78 B	79 X	80 I	81 Q	82 P
83 A	▨	84 K	85 N	86 F	87 E	▨	88 N	89 S	90 W	▨	91 D	92 G	93 P	94 J	95 V
96 B	97 U	98 K	99 Q	100 R	▨	101 B	102 C	103 I	104 P	105 V	106 J	107 F	▨	108 Q	109 G
110 D	111 P	112 C	113 I	114 V	115 B	116 J	▨	117 F	118 W	119 D	120 M	▨	121 J	122 I	123 V
124 N	125 Q	126 P	127 D	128 M	▨	129 V	130 F	131 H	132 W	▨	133 H	134 T	135 L	▨	136 Q
137 A	138 J	139 D	140 V	141 I	▨	142 Q	143 P	144 G	145 W	146 C	▨	147 H	148 V	149 I	150 O
151 Q	152 N	153 P	154 D	155 J	156 B	▨	157 R	158 E	▨	159 I	160 O	161 F	162 K	▨	163 J
164 R	165 H	166 G	167 V	▨	168 A	169 K	170 T	171 V	172 N	▨	173 R	174 X	175 B	▨	176 R
177 O	178 G	▨	179 I	180 E	181 P	182 J	183 V	184 H	185 T	186 Q	187 D	188 B	▨	189 Y	190 X
▨	191 G	192 O	193 A	▨	194 C	195 Q	196 E	197 J	198 V	199 P	▨	200 I	201 M	202 X	203 A
▨	204 Y	205 X	▨	206 S	207 R	▨	208 A	209 C	210 X	211 E	▨	212 V	213 J	214 I	215 L
216 N	217 P	218 Q	219 B	220 K	▨	221 F	222 L	223 A	▨	224 L	225 Q	226 P	227 E	228 N	229 J
230 V	231 B	232 I	▨	233 V	234 E	235 I	236 P	237 A	238 J	239 Q	▨	▨	▨	▨	D.H.W.

(Solution next month)

NOT ONLY "NOT ON MY WATCH," MR. GURIN, BUT NEVER ON MY WATCH, IF I CAN HELP IT!

[redacted]

P.L. 86-36

NSA Archivist

There are few people in the Agency who read Mr. Gurin's article, "Never Again!" (CRYPTOLOG, June 1978) who are more in sympathy than I with his rage at learning that his "only-one-of-its-kind" file on an important processing experiment had been thrown out and then getting an explanation that "proved to be, essentially, 'It didn't happen on *my* watch!'" In fact, my unhappiness is probably even greater than his, because, unlike Mr. Gurin, whose responsibilities for their care officially ended when the papers in question were of no further foreseeable operational value, *my* responsibilities now *start* at that point. The discarded valuable records were destined to be *my* records, and I grieve for them as only an Archivist who has also had 25 years of operational cryptologic experience can.

I must, however, set the record straight, Mr. Gurin. You may have thought that you were sending your papers to NSA's *A*rchives (and you spelled it with a capital A in paragraph 4, implying "The NSA/CSS Archives"), but you didn't. You sent them to "a records storage center." NSA didn't have any *A*rchives in September 1967. In fact, it didn't have any Archives in September 1977 either. Only *now* does it have an Archives -- the Archival Holding Area (AHA) -- with internal NSA approval on 1 March 1978 and official National Archives and Records Service (NARS) approval following soon thereafter.

To all you readers who may be inclined to heed Mr. Gurin's warning about checking the safety of your stored materials -- we (the AHA) agree. Do so! And after you have done this and have reevaluated your holdings, if you still feel that they are "documents," a "collection," or "papers"[1] of enduring value, please send them to the NSA/CSS Archival Holding Area.

What guarantees can we give you that your precious file won't have the same unhappy fate of Mr. Gurin's? As with all things in life, there can never be any absolute guarantees. But we can and do offer the guarantee that the NSA/CSS Archives will be a *thoughtfully* and *carefully* run operation, with as many controls as possible to preclude such unfortunate and irreversible occurrences. Unlike records storage areas, we will not be dealing with masses of items that are unknown and uncared for save by an arbitrary finding number. We are not just box custodians. The primary interests and reponsibilities of the AHA are for what is *inside* the boxes. As we acquire and access documents or collections that merit permanent retention (the National Archives and Records Service says that only 3 percent of all Federal records generated really fall into that category), we will be recording *who* sent them. Subsequently, we will follow the archival principles of "respect des fonds" and provenance and will record, as well as scrupulously comply with, any and all restrictions the donors may place on them. The skilled personnel of the AHA will examine all items received with a view to selecting those of permanent importance, and will, upon request, return whatever appears to be inappropriate. Once accessioned, items will be studied, described, entered into a finding-aid system tied to a source-content descriptive system, labeled, and stored in archival storage boxes on shelves in the AHA. Temporarily the AHA will be in SAB 2 (the old IRC Building). Ultimately, in the 1983-1984 time frame, it will be a part of a newly constructed SAB 5, in a separate, environmentally controlled facility designed for complete and permanent protective storage.

I hope that Mr. Gurin will forgive me for rewriting the very last sentence of his article, but I think that if he had been fully aware of the newly established AHA and its mission, aims, and potential for undoing the chaotic old system (that is, *non*system) for protecting valuable documents, he might even have made the change himself:

> "And, dear reader, if you have anything stored in archives[2], you would be wise to check right now and, if it really is of archival significance, send it to the NSA/CSS Archival Holding Area (c/o [redacted] [redacted] FANX II, A1A26, 8297s)."

P.L. 86-36

[1] Each of these terms has a special meaning to archivists, but the AHA encourages people to just send whatever they have and let us determine the proper category.

[2] Note the "archives" with a small "a," which equates to "a records storage facility."

Letters to the Editor

P.L. 86-36

To the Editor, CRYPTOLOG:

I wish to expand upon a point touched upon rather briefly in [redacted] informative article on technical translations ("Has It Ever Been Translated Before?", [redacted] [redacted] CRYPTOLOG, July-August 1978), i.e. the W31 translation effort. W31 publishes contract translations of technical articles and books (or portions thereof), the latter comprising the majority of W31 material translated. The program is aimed to satisfy the interests of W Group and the other NSA organizations. Selection criteria are based on W31 knowledge of cryptologic and other SIGINT interests to NSA elements (inputs solicited), as well as requests from organizations outside of W31. In contrast, translations by JPRS, FSTC, and FTD are performed only to satisfy specific analyst requirements.

[redacted]

Regarding the STINFO system, two copies of all W31 translations are sent for retention to the Technical Library in addition to the key words, abstracts, and publication information. An index of all NSA translations of this type (1962-1978) is available from W31 (3463s).

[redacted] W31

~~(C CCO)~~

To the Editor, CRYPTOLOG:

It's only fitting that my first letter to the editor of anything should be of the bitch-and-moan variety, but then they're the only kind that anybody reads. Whatever, after being told repeatedly for about 10 years that the old annual performance appraisal doesn't mean a damned thing, I'm finally inclined to agree to the point where I really think that the whole thing should just be scrapped. It'd save time, money, and energy, and nobody'd be likely to miss it. It doesn't work and it can't be made to.

This conclusion didn't come to me overnight. At first glance it looks like the shortcomings of the present appraisal system could be overcome. This system, as applied by A2 (and, for all I know, elsewhere), is designed to let an employee and his or her employers know what sort of work the employee has done over the past year. It doesn't do this, for the following reasons:

- It operates on a quota system. This means that you can't recognize more than a certain percentage of the people in a given grade in a given organization as doing outstanding work, no matter how many are actually doing such work. The results are misleading and counterproductive.
- It's ~~a~~ seven-level categorization sloppily modified so that only five levels may be used. Levels 2 and 6 are considered not to exist, but no compensation is made for their absence. (Actually, they're not even absent -- they're right there on the form but you pretend they're not there.) Supposedly, excessive use of Level 6 was being made by supervisors. The remaining five levels really only describe three types of performance: very bad, mediocre, and very good. Consequently, the work of most employees is categorized as mediocre, and that is a real morale-booster in a place that supposedly employs a lot of pretty sharp people.
- It's directly attached to the promotion system. This really circles back to the first reason. If your branch quota for a certain grade level is one Level 7 appraisal, and you've got someone in this grade level up for promotion, then this person has to be your 7. Otherwise someone's going to want to know just what the hell he's doing up for promotion with a crummy Level 5. There's no reason why one person's performance appraisal should be affected by someone else's eligibility for promotion.

So does this mean that the system still can't be revised and made to work? Right! it can't! Even if you remove the quotas and the attachments to promotion, and establish a whole new set of performance levels and criteria, the

P.L. 86-36

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

system is still dependent on the frequently subjective opinions of frequently unqualified supervisors. Supervisors are, in turn, encumbered by inconsistent and often conflicting managerial policies. The system was also designed to encompass too broad an area to accurately assess individual performance. The assessment of an employee's work can be done best within, at most, his own branch. Nevertheless, approval of a Level 7 appraisal must be done at such a high managerial level that often the person giving final approval has never met the person being approved.

To wrap this up, my final argument for dumping the system is that it's unnecessary. Step increases are given to acknowledge satisfactory work. QSIs, SSWPs, and, supposedly, promotions are given to acknowledge outstanding or superior work. Performance appraisals don't acknowledge much of anything and, as a supervisor, I'd much rather forgo the embarrassment of explaining to someone that, while I personally think he or she is doing excellent work, this worthless form says that the person "occasionally exceeds performance norms." Fortunately, nobody takes performance appraisals seriously enough to interpret this as an insult.

[redacted]

(U)

Editor's note: It is generally the rule that CRYPTOLOG publishes anonymous contributions only if the writer's identity is known to the publisher or editor. It is felt, however, that an exception ought to be made for the following completely anonymous letter.

To the Editor, CRYPTOLOG:

I have just received word that another key employee has joined the ranks of the Agency resignees. I couldn't help thinking what might have been the underlying cause of his (not to mention countless others) decision to leave. I hunted for a past issue of CRYPTOLOG (November 1977, to be precise) to find an appropriate article I had run across a few months back. Perhaps the words of wisdom in that article should be revitalized.

Nine months have elapsed since [redacted] interesting and factual article entitled "A Proposed Cure for the Time-in-Grade Syndrome" appeared in CRYPTOLOG. It has obviously not been forgotten by many, such as myself, who firmly believe something ought to be done about the infectious time-in-grade disease rampant throughout the Agency. It appears to have been ignored by the Agency ruling class, however.

One point I feel [redacted] should have elaborated on, though, concerns the archaic ritual of giving yearly performance appraisals. I was led to believe these "psychological strokes" were designed to inform employees of their progress in their present job. In actuality, they seem to be used as a major factor by the "time-in-grade-loving" supervisors/panels in determining which old timer should receive his or her "pay raise" first. Notice that I did not call it a "promotion."

The performance appraisal, under normal circumstances, should be a very good indicator of an individual's performance. I say "should" rather than "is" because I, for one, do not believe it is an accurate way of determining just how well an employee executes his or her job. The way the performance appraisal is set up at present, it is impossible to judge an individual's true progress. For instance, where on the current form does it allow a supervisor to praise an individual for his or her initiative? I've had supervisors in the past completely ignore certain talents and skills I had acquired that I felt were significant towards successfully and efficiently executing my duties. I've also had other supervisors rate me according to a set of duties that some nameless individual in M Group dictated as fulfilling my particular job description, but which, in fact, I never did. And imagine my shock when a previous supervisor once announced, "I'm giving you a low rating on your appraisal this year since you've just been promoted, and we want to give others at your previous grade level a stab at a promotion." How do you think that would have looked on the personnel records if an individual, recently promoted (supposedly equivalent to a Level 7 rating), only received a Level 3 for that year? Since the past 3 years' performance ratings are often included when a supervisor prepares a Promotion Recommendation, do you honestly feel this is a fair system?

P.L. 86-36

We employees (to quote [redacted] have the responsibility for qualifying for promotion, and these qualifications (excluding time in grade) should be judged by an impartial panel, composed of upper management individuals from various elements, who will make their recommendations on the basis of an individual's initiative, drive, willingness, and experience (whether the experience was gained from working inside or outside the Agency), as well as current job performance.

Until a new system for recognizing and rewarding bright employees is established, I'm afraid we shall hear of more key people joining the ranks of the resigned.

"Wish to remain anonymous
due to impending resignation,"
F8353

(U)

P.L. 86-36

C.A.A. NEWS

- Do you like to play games and call it work?
- Are you using cryptanalytic principles and techniques while analyzing your traffic?
- Would you like to be the one to solve that new callsign, frequency, or procedure system?
- Do you already solve complex systems before lunch and sneer at those who need brunch to keep up?
- Would you like to know more about many of the crypto-TA principles used routinely on all TA PQEs?

If you answered yes to two or more of these questions, there is a Special Interest Group (SIG) within the CAA for you. In an effort to appeal to crypto-TA enthusiasts on all levels, the Crypto-TA SIG is now reorganizing to do the following things:

- Search out current practioners of crypto-TA and ask them to make formal presentations to the SIG;
- Try to reach case analysts to give them the necessary tools to recognize pertinent situations where crypto-TA principles could be applied;
- Upgrade the skill of TA professionalization aspirants through study groups, tutoring sessions, problem-solving guidance, etc.;
- Publish crypto-TA brain teasers in CRYPTOLOG every month.

For additional information concerning the Crypto-TA SIG, contact one of the following:

[redacted]	4466s
	5372s
	8356s
Paul McCormick	5845s

Communications Analysis Association:

President	David Gaddy	3247
President-elect	[redacted]	5879
Secretary		8025
Treasurer		3791
Board members		4935
		5991
		3573
		3369

~~(C)~~

Solution to NSA-crostic No. 18

(CRYPTOLOG, October 1978)

[redacted] "[A] CRYPTOLOG Interview," CRYPTOLOG, December 1976:

"Now it's possible to include in an NSA report a statement like 'this could be an indication that country X is planning an attack on country Y,' whereas previously a report containing that statement would be difficult to get out of the building. There would have been too many doubting Thomases." (U)

"I said, 'Hender hoke!'"

MILITARY LINGUISTS

Military linguists who pass NSA's Language Proficiency Test (LPT) will receive a Certificate of Achievement from the Agency's Language Career Panel. Effective 1 October 1978, anyone who scores more than 130 points on the LPT will be awarded the certificate. Those who score 140 points or higher with get the certificate "With Honors." The passing rate from 1 July 1977 to 1 July 1978 was 40 percent. The awarding of the certificate is intended to recognize the extra effort that military linguists have expended to improve their professional skills. (U)

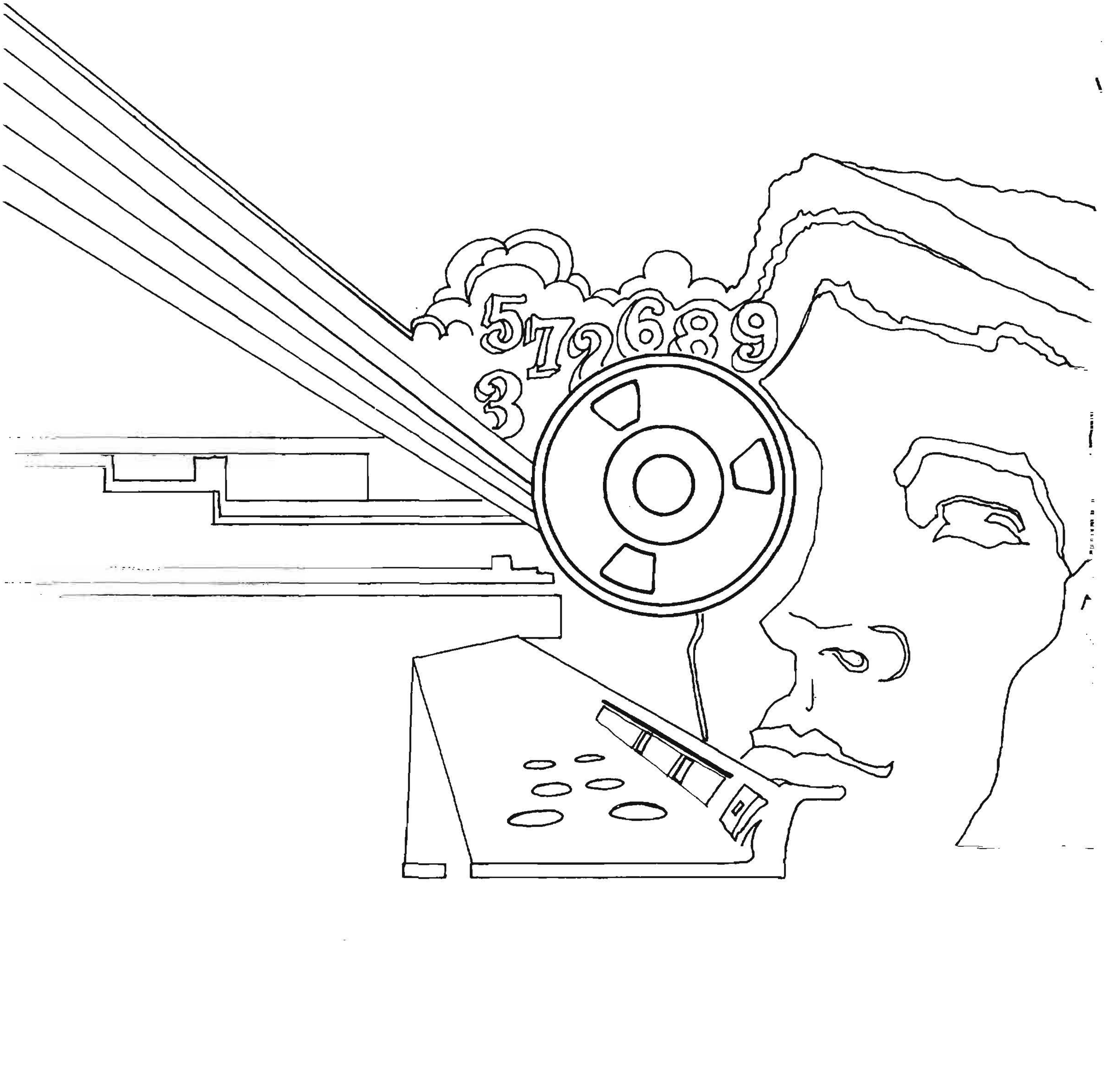
CORREZIONE!

P.L. 86-36

Now THAT'S Italian!

The spelling T-A-U-R-O-N-E, that is. As the editor of a publication that prides itself on being 100-percent free of typographical errors and misspellings (if you can prove otherwise, you may qualify to be an honorary proofreader for a month's issue of your choice), I am embarrassed to report that, as a result of a transcription error, the name of our new TA editor was Irishized in the past two issues. So please note that it's not "Don Tyrone" who's going to give aid and encouragement to traffic analysts who want to have their say in CRYPTOLOG, but Don *Taurone*, on 3573s. (U)

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~