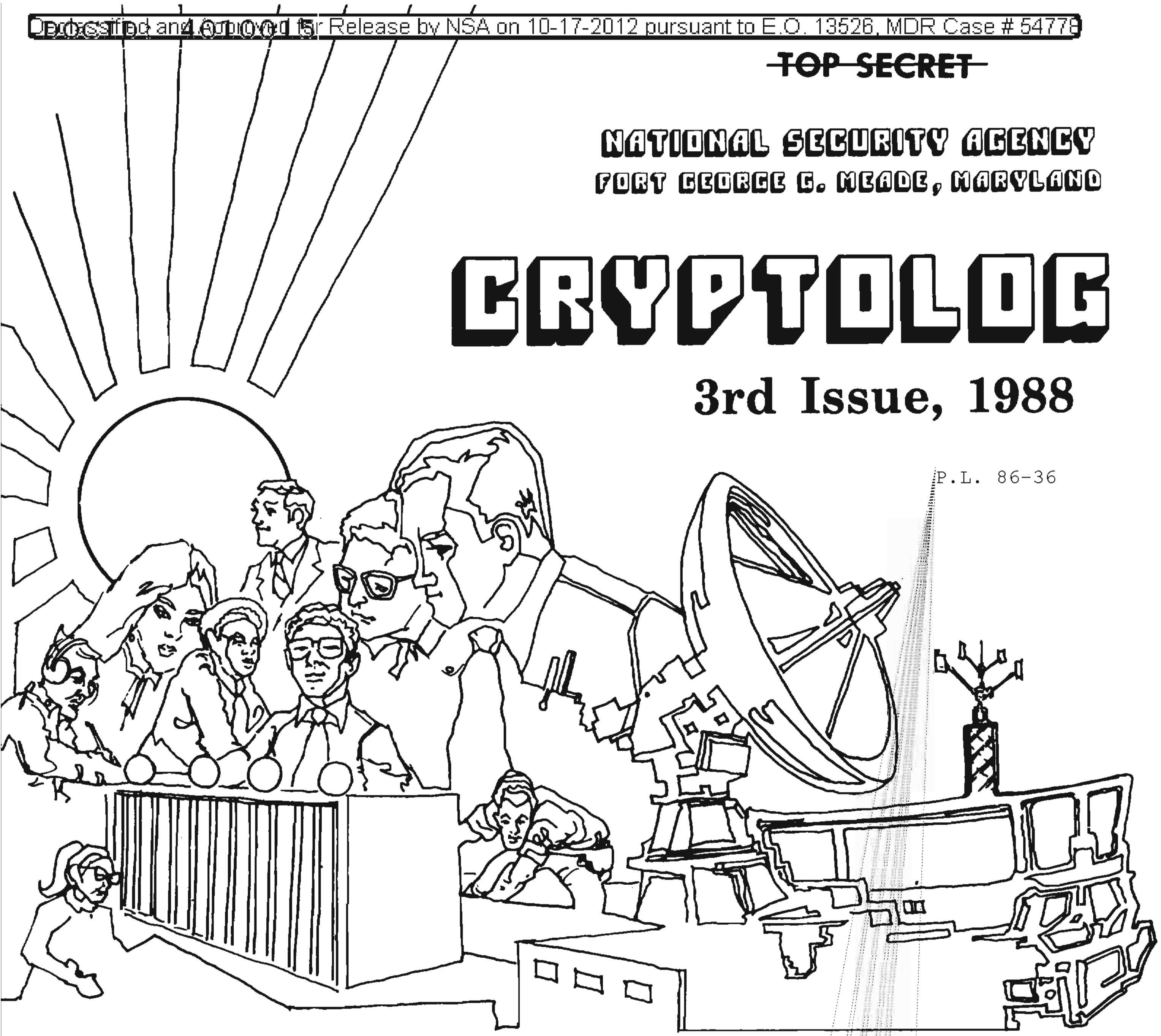
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

3rd Issue, 1988



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

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

~~TOP SECRET~~

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

~~NOT RELEASABLE TO CONTRACTORS~~

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XV, No. 3 .... 3rd Issue 1988

PUBLISHER .... [redacted]

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.

Contents of CRYPTOLOG should 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.

YELLOW PAGES FOR NSA

What NSA needs is Yellow Pages, just like the phone book, showing functional responsibilities. Or where to get information. Or even, how to found out how to get information.

What brought this to mind is a kind of inquiry that CRYPTOLOG often gets. Here's a typical exchange:

Reader: *I'm looking for articles on Project XYZ. It seems to me I read about it in* CRYPTOLOG.

Editor: *Let me check. [Pause.]* No, sorry. *Probably you saw it in* The Cryptologic Quarterly. *The two publications are often confused. Their number is 972-2355.*

[A week passes.]

Reader: *About that Project XYZ. CQ tells me that they didn't publish it, either. Do you know where else I can try?*

Editor: *Try STINFO, T513. Their number is 968-8611. They can do a keyword search in classified documents and in open sources as well.*

Reader: *Thanks. By the way, someone from another agency is coming in for a briefing on the project. I'm supposed to make the arrangements. Where can I find out what I have to do?*

It would be nice to say, "Look it up in the Yellow Pages," which, of course, is printed on yellow paper -- or better yet, in this day of automation, is kept on line. It could be limited to a few outlets, one terminal per office, something like the personnel files on the M204, for example.

Why not?

CHANGES IN AGENCY REPORTING

[redacted] P05

P.L. 86-36

~~(C-CCO)~~ In November 1982, NSA, with G Group at the lead, launched a major initiative to move away from the traditional full-text translation format [redacted] to a journalistic format.

~~(C-CCO)~~ The basis for this change was multifaceted. One was security related. We had lived through instances of seeing verbatim quotes of some of our product in the media, and needless to say, even in an English translation form, a quote in the media of a verbatim translation of target communications makes it much easier for a target counterintelligence effort to track our source and to take countermeasures. While the journalistic format does not provide full-proof protection in the case of leaks or other compromises of our product, it does give at least some additional security.

(U) Another reason for the move to the journalistic style was to provide a product better suited to the reader, especially the executive reader, who has to scan rapidly much incoming material to determine quickly the key elements of the reports. The journalistic format encourages the reporter to summarize briefly the highlights of the report at the beginning of the report. Thus, by reading the title and the introductory summary, the reader quickly learns what the report covers and can decide whether to read the entire report. In contrast, when the information is published as a full-text translation, the reader often has to wade laboriously through long-winded salutations and extraneous material to extract the important parts of the report.

~~(C-CCO)~~ Finally, another reason for the switch to journalistic style was that we have only a limited number of foreign-language translators to cope with an ever increasing volume of intercept. [redacted] Some reporters complained that the switch to the journalistic style detracted from their verbatim translation skills upon which they were tested for certification. Some senior checkers complained that the switch to the journalistic format actually took more time because they could not feel confident of the reports done by the junior linguists unless they first saw a full-

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

P.L. 86-36

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

text translation upon which the report was based.

(U) But gradually those growing pains have been overcome. Our reporters and checkers have adjusted to the journalistic style and now most feel quite at home with it, preferring it over the old style because it makes them think more about the story they want to convey and how they want to convey it.

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

CUSTOMERS' REACTIONS

~~(C-CCO)~~ As the new Agency initiative began to develop momentum, we got mixed reactions from readers. Some were quite pleased with this new format [redacted] As time went on, we encouraged customers to develop a direct relationship with our reporting elements to help answer any questions arising with our product.

[redacted]

COORDINATION WITH SECOND PARTIES

[redacted]

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

[redacted]

WHERE WE ARE HEADED

~~(C-CCO)~~ Any changes as dramatic as the Agency's move to the journalistic style for our [redacted] product would be expected to take time as we progress toward our objectives. New reporting policies and procedures have evolved as we made adjustments to come up with a more efficient production process and to provide the best product possible to our customers. Sometimes communication with our readership, with our Second Party agencies, and even within our own ranks has not been as good as it should have been. But with the patience and persistence of top Agency officials, managers at all levels, and reporters at the Agency and in the field, we have made tremendous progress since setting out on this road over five years ago.

~~(FOUO)~~ Our main effort now is to consolidate these changes into a new draft of USSID-300 in a way that will clearly document these and other changes for the workforce. And we have established a DDO Intelligence Staff Product Improvement Working Group to provide a forum for within-DDO communications of the success and problems associated with this initiative and to surface other ideas on ways to publish better product with our limited resources. We encourage the active participation of everyone concerned in these endeavors. □

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

P.L. 86-36

[redacted]

UPDATE ON PACKET RADIOS

[redacted] *G923*

P.L. 86-36

(U) As a follow-up to my article "Is Packet Radio Alive and Well on HF?" (Cryptolog, 3rd Issue, 1987), here is some recent information:

[redacted]

- (U) The following countries should be added to figure 2, countries whose amateur radio operators are active in amateur packet:

Bahrain
Bermuda
Bolivia
Bulgaria
Egypt
French Polynesia
Gabon
Greece
Honduras
Hong Kong
Iceland
India
Ireland
Israel
Kenya
Lebanon
Lesotho
Malaysia
Malta
Marinique
Monaco

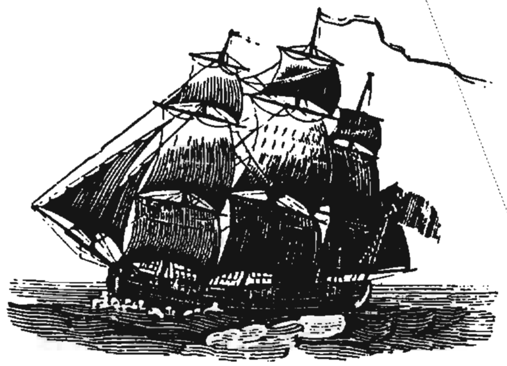
Namibia
Nepal
New Caledonia
New Guinea
Nigeria
Oman
Pakistan
People's Republic of China
Peru
Poland
Qatar
Senegal
South Korea
Soviet Union
Surinam
Thailand
United Arab Emirates
Western Samoa
Yugoslavia
Zaire

UNCLASSIFIED

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

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

Release of Embargoed Information



P.L. 86-36

[redacted] *P05*

(U) This is a discussion of pertinent facts and regulations concerning the release of embargoed items to non-NSA contractors. Keep in mind that the distinction between **embargoed** and **unembargoed** information applies only to information released to the non-NSA contractor.

~~(C-CCO)~~ The key to identifying end-product that DIRNSA considers embargoed is that, regardless of its COMINT category, it bears caveats, handling restrictions, or channels markings other than, or in addition to COMINT channels.

(U) DIRNSA's policy is to not release any embargoed material to a non-NSA contractor on a blanket basis. In other words, the sponsor must identify each and every specific document requested, together with supportive justification. A general request such as, "All information pertaining to technical intelligence on the [redacted] system" is unacceptable.

(U) Embargoed information falls into the following categories:

- ~~(C-CCO)~~ End-product, regardless of its COMINT category, bearing any restrictive caveat, such as **NOFORN, ORCON, GAMMA** Controlled Item, **PROPIN, NO CONTRACT**, etc., is considered embargoed information. (These are examples of restrictive handling and distribution exchange designators, and do not purport to represent all possible versions of such restrictions).

- (U) Any end-product protected in a special channel, such as **LOMA**, and/or **TALENT-KEYHOLE**, instead of, or in addition to COMINT channels.

[redacted]

- (U) All technical data is likewise embargoed, regardless of classification and/or channels protection. Technical data includes working aids, technical support letters, reports and manuals; information of SIGINT production processes; raw SIGINT data; tapes of specific signals; and tapes of electromagnetic spectra.

- (U) Foreign encrypted signals are not, repeat not, releasable to non-NSA contractors without the specific approval of the Director or Deputy Director, NSA.

To Request Release of EMBARGOED Information

~~(FOUO)~~ A request for the release of embargoed information to a non-NSA contractor involves the following steps:

~~(FOUO)~~ 1. The sponsoring agency's contract monitor must submit a written request (electrical message/letter/memo) to DIRNSA, ATTN: P05/SAO. Military sponsors should forward their requests to the cognizant intelligence command for review and validation, with an information copy to DIRNSA (PO5/SAO). Upon PO5/SAO's receipt of the cognizant intelligence command's validation, it will initiate processing action.

P.L. 86-36

~~(FOUO)~~ 2. The request must contain the following:

(a) The title, contract number and expiration date of the contract.

(b) The contract statement of work or information sufficient for NSA/CSS understanding of the contract's purpose.

(c) Certification of the contractor's need for access to the SIGINT infomation.

(d) Certification of the contractor's clearances.

(e) Security certification of the contractor's storage facility or the facility in which the SIGINT information will be processed.

(f) Name and phone number of the contract monitor.

(U) 3. Upon receipt of the above, PO5/SAO will review the request and determine the appropriate action office (generally dictated by what organization originated the material, and/or the OPI of the subject matter involved). In most cases the OPI (action office) is the final authority regarding the releasability of the material requested, and has the prerogative of mandating specific provisions or precautions to be adhered to in connection with the release. The OPI is also responsible for advising PO5/SAO concerning the decision to release of the requested information.

(U) 4. PO5/SAO will then forward the Agency's decision to the requester in writing, based upon the recommendation of the OPI.

~~(FOUO)~~ NSA-originated SIGINT or SIGINT-related material may not be released to a non-NSA contractor unless the above process is observed and PO5/SAO (DDO's designated Central Point of Contact regarding release of material to contractors) is aware of the request/action.

(U) For clarification as to whether material requested for a non-NSA contractor falls into the embargoed or unembargoed category, please call me on 963-5463s. □

BULLETIN BOARD

WORD PATTERN LISTS

~~(FOUO)~~ A program to generate word pattern lists is available in G244. It produces patterns in the familiar form ABCDAC, *et al.*, when run on an edited plaintext data base. For information call Fred Pollnitz or Bob Silva, 963-5380s.

IBM TO XEROX CONVERSION

(U) There is now a program to strip superfluous function codes (carriage return and line feed) from IBM floppies before conversion to the XEROX STAR format. (Preliminary tests show that it also works for IBM to Macintosh conversion.) This is a quick routine, a matter of seconds, that eliminates the customary time-consuming multi-step "find-and-replace" routines. For a copy of the program and instructions call or write [redacted] P16, HQS, 963-1103.

P.L. 86-36

SOFTWARE VERIFICATION

(U) The National Bureau of Standards has adopted a new standard for improving the accuracy and quality of software during development and maintenance. Called "Software Verification and Validation Plans" (ANSDI/IEEE 1012-1987) it was developed by IEEE. We expect to see it published as a Federal Information Processing Standard in the near future. For further information call or write [redacted] P13D, FANX-II, 968-8161.

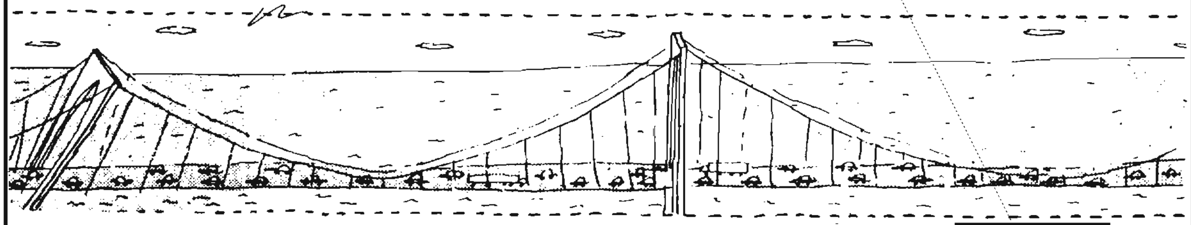
P.L. 86-36

WANTED: CONVERSION FROM APOLLO

(U) CRYPTOLOG is seeking to convert files prepared on APOLLO, particularly those done in Te$_{\text{x}}$,, to IBM DOS or Macintosh or Xerox STAR. If you know how to do it, please get in touch with the Editor, [redacted] P1, HQS, 963-1103.

P.L. 86-36

THE SHORT BUT HAPPY LIFE OF WIDEBAND



P.L. 86-36

[redacted] P0431

~~(C)~~ There was a time when we had collection resources all around the world. [redacted] The manning in those stations, however, was to become a source of concern for Agency management. Collection activity as it was performed in those bygone days was man-intensive and quite costly.

(U) In the early sixties another problem arose that exacerbated the concerns about station manning. The French, for whatever reasons they had, began a run on the gold reserves of the United States by cashing in dollars. Other nations, not wanting to be left holding the bag when the U.S. ran out of money, followed suit. Several programs were started on a national level to halt the erosion and to bolster our country's reserves, but they are not involved in this story.

(U) NSA, as its contribution, sought means to limit its contribution to the gold flow. One of the most significant factors identified was the pay that our field personnel spent off base. That money went into the foreign economy as dollars that were at that time redeemable in gold.

(U) This was the issue: How do we limit the spending of our personnel on the foreign economy? Cutting their pay, limiting off-duty time or restricting off-base activity were all equally unattractive as solutions. We have never enjoyed an overabundance of the skilled, intelligent personnel required to man a SIGINT field station and any solution that would make the duty less pleasant would make it more difficult to find people to do the job. The only reasonable approach to this problem was to develop some method of limiting the number of people to spend the money.

[redacted]

[redacted]

[redacted]

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

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

(U) ECSR has been considered by some people as an evolutionary stage in the development of remote intercept technology, and that may be accurate. But just as the tyrannosaur, the

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

diplodocus and the triceratops may be gone, the gekko, the alligator, and the iguana are their descendants and still fill ecological niches. So, too, does the ECSR system of today serve its collection functions.

[redacted]

(U) A new chapter is being written in this story. Just as the technique is more than twenty years old, the equipment now being used is ten to fifteen years old and is beginning to show its age.

(U) There are people in NSA who are beginning to be concerned about the equipment and the methods now in use and who are persuading themselves that new technology should be developed to supplant the banks of recorders that are in use to record a little more than a Mhz apiece. There is discussion of digital recording techniques, techniques using VCR technology, and of techniques that retain the basic technology in use at present, but modified to record at half the speed used now, thus saving - in theory, at least - head wear, tape wear and tape volume. Reduction of the tape volume, in turn, would also reduce tape storage space requirements, shipping costs and the expenses involved in rehabilitating and inspecting the tapes.

(U) Each of these options has one thing in common with the others: They are all very expensive. The least expensive of the options, the half speed modifications, has been tested and seems to work well, judging by the limited experience we have had with it. The cost for modifying each recorder would be in the neighborhood of $50,000 per unit, and the modification also requires that new high performance tapes be introduced into the system. Tapes now in the inventory will not serve.

(U) It has been postulated, however, that the high performance tapes may be more abrasive than the tapes used at present, which would, of course, increase the wear on the recording and playback heads. Would that offset the savings realized from the slower tape speed and the reduced footage that would be recorded and played? There are no definitive answers to that, yet.

(U) One additional advantage to the half speed modification would be the fact that the new version could probably be phased in more easily than could the introduction of entirely new technology. Thus the cost of the option could be spread across a few years, resulting in smaller impacts on annual budgets and less disruption to ongoing activity. New technology would require a turnkey operation and, while it could be phased in by theater, it would probably have to be done theater-wide in each phase.

(U) There is one other disadvantage to the half speed proposal, however. It involves replacing the heads, capstans and other parts on the recorders already in the inventory. With this, you have new technology on what are still old machines. We would be putting hundred dollar saddles on ten dollar horses. The motors, power supplies, and other parts of the machines will just continue to get older. Worse yet, when the parts that never break start to break, they will be very difficult and expensive to replace—all out of proportion to their original value—if past experience with other kinds of hardware holds true.

~~(C-CCO)~~ There is no good answer to what we should do about our wideband'resources. Perhaps, before we consider the answers to those questions, we should examine other questions. For example, is wideband recording paying for itself in intelligence gains? [redacted] Is there any other way to derive what we now get from wideband recording?

(U) This has not been a research paper; it has been some random ideas that have crossed the writer's mind. The historical chronology may be fuzzy, the costs cited may be inaccurate, but the basic facts are facts and we are coming to a time when a decision should be made.

(U) Any suggestions? [redacted]

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

[redacted]

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

N. C. GERSON, R6

~~THIS ARTICLE IS CLASSIFIED SECRET HVCCO IN ITS ENTIRETY~~

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

LANGUAGE BRIEF: XHOSA

[redacted] G94

(U) Xhosa is a Bantu language spoken by more than 6 million people in the Transkei and Ciskei "homelands" of South Africa, which border Lesotho and face the Indian Ocean. The Bantu family of languages numbers over 300 and is spoken in an area encompassing most of the southern part of Africa extending south of Cameroon and Kenya. Xhosa was the first South African Bantu language to appear in print, transcribed by missionaries in 1821.

(U) Xhosa is a tonal language, with high, low, and falling tones. Because the Xhosa people interacted with the Hottentots early in their history, their language shares some of the peculiar clicks characteristic of the language spoken by the Hottentots, people of a South African race related to the Bushmen. (Sotho also shares some of these characteristics, although it has only a single click.) The clicks are represented by the letters "X", "Q", and "C" and, in combination with vowels and consonants, form 20 click combinations . Changing one click combination for another can change the entire meaning of a word.

(U) The "X" click, or lateral, sounds like an equestrian urging his horse on; the "Q" click, or palatal, sounds very much like a cork being released from a bottle. The "C" click, or dental, sounds like the nonverbal sound a person makes to express disgust.

(U) Xhosa is based on a system of concords, or prefixes. Depending on which of seventeen classes the noun of the sentence fits into, the prefix of the noun will influence the form of the verbs, adjectives, and other parts of speech which are brought into relationship with the noun. Examples are shown below. Because of these concords Xhosa is extremely alliterative, which makes it fairly easy to recognize in written and spoken form.

(U) In addition, Xhosa is an agglutinative language, as opposed to inflectional, having a predominance of detachable particles which can be added to the word to vary its meaning. It is a language filled with interjections, and has ideophones as well. Ideophones are descriptive and exclamatory utterances designed to complement the thought being expressed and are often imitative of the action described, or of a sound associated with it.

(U) Although Xhosa is one of the principal languages of South Africa, along with Zulu, Tswana and Sotho, it is not considered an official language in that white-ruled country. Only Afrikaans—a bastardized version of 16th century Dutch—and English are officially recognized.

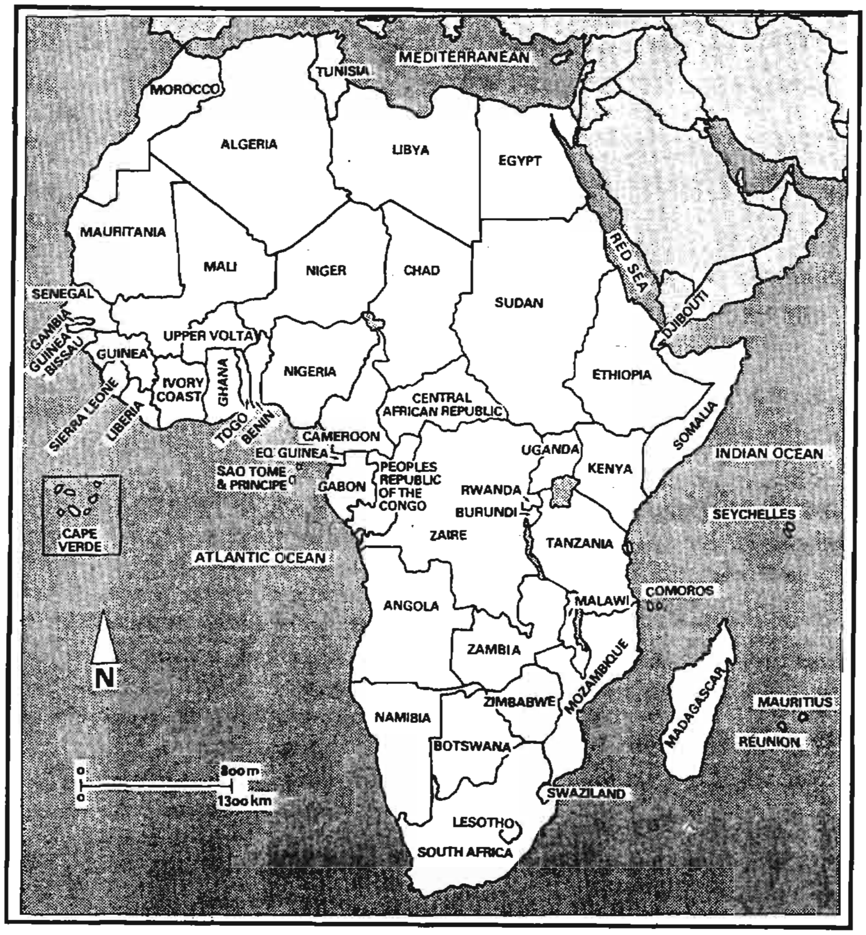
[redacted]

Unclassified

EXAMPLES OF CONCORD

All people want peace	Bonke	abantu	bafuna	uxolo.
The whole country wants peace.	Lonke	ilizwe	lifuna	uxolo.
The whole nation wants peace.	Sonke	isizwe	sifuna	uxolo.
All nations want peace.	Zonke	izizwe	zifuna	uxolo.

Unclassified



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

EXPO 88

★

19 October 1988

Friedman Auditorium

★

See it now!

★

High tech for linguists!

Custom-designed workstations for linguists!

Online dictionaries!

Electronic gazeteers!

High-resolution displays!

Neat inventions!

Useful gadgets!

★

Sponsored by The Office of the Chief Scientist and the Natural Language Working Group, a consortium of linguists, computer scientists and engineers from A, B, G, T, R, and Z.

Nineteenth Southeastern Conference on Combinatorics, Graph Theory, and Computing, 15-19 Feb 1988, Louisiana State University, Baton Rouge.

Reported by: [redacted]*R512*

P.L. 86-36

I attended this conference to present my paper "A New Combination Generation Method, " to keep abreast of developments in a vital area of mathematics, and to support Agency recruitment of professional mathematicians.

[redacted]

There were five invited presentations and about 180 fifteen minute talks in three parallel sessions. As conference proceedings are scheduled to appear in *Congressus Numerantium*, published by Utilitas, and also because no earth-shattering new results were announced, I am limiting myself to comparatively few remarks about the talks themselves.

CONCLUSIONS AND RECOMMENDATIONS

The Southeastern Conference addresses a type of mathematics of very special importance at NSA, namely combinatorics. Hence NSA attendance is indispensable. More than one representative should be sent when possible.

This may be an appropriate place to give a view on the value to NSA of attendance at meetings of the present type. I believe that the dominant factor is the educational and motivational value to the individual attendees. They are exposed to a lot of new information by enthusiastic researchers from the US and the world; they make contacts and are made to feel a part of a larger mathematical community. This will be reflected in better job performance. Attendance at meetings is an appropriate and economical mode of training for those of us who are already steeped in formal degree-oriented schooling. The individual attendees will be better trained, better motivated, and have improved morale. Benefits like this have the biggest potential payoff.

THE TALKS

Each of the five days was highlighted by an invited instructional lecture of one or two hours. All of the invited addresses with the exception of Frankl placed considerable emphasis on whether the problems addressed are NP complete or had efficient algorithms. I interpret this to be an indicator of current fashion.They were:

- "Cycles in Graphs and Directed Graphs" by Carsten Thomassen of the Technical University of Denmark;

- "Fast Algorithms for Convex Polygon Problems" by Maria Klawe of IBM Almaden Research Center;

- "Current Developments in Cryptanalysis" by Ernest Brickell of Bellcore and Sandia Labs;

- "Old and New Problems in Finite Sets" by Peter Frankl of Bell Labs and the University of Paris; and,

- "Recent Developments in Ramsey Theory" by Vojtech Rödl of Bell Labs and Czech Tech.

The last two speakers are mentioned as possible successors to Erdös. (Erdös himself was to have talked, but skipped off to Australia at the last moment, so Frankl spoke instead.) All of these talks were of high quality.

Klawe studied a scheme whereby certain inequalities related to convexity propagate through a matrix. "Totally monotone" is her term for matrices in which this happens. This structure was exploited to construct certain efficient algorithms. Her scheme appeared similar to one which I had employed in computing what I call "subsequence numbers." I pointed this out to her and gave her a reprint of my paper (*Discrete Mathematics* 16, 1976, 123-140).

Brickell's talk surveyed a lot of open-literature cryptanalysis very fast. I am told the presentation was not much different from previous talks he has given. Nevertheless, since there is probably interest in what he had to say, I have obtained copies of his multitudinous slides which he was kind enough to send me. He kept repeating that much of this material would be included in a paper to appear in the *Proceedings of the IEEE*, written with Odlyzko.

Frankl's talk was fairly short and included problems concerned with the existence and construction of critical (e.g., maximal or minimal) families of subsets of a finite set with various stated requirements on how the subsets in the family had to be related one to another. Sperner's theorem, for example, concerns the case where the requirement is pairwise incomparability. In most of the cases Frankl discussed, however, the requirement concerned "intersecting," or "cross-intersecting" between sets in the family, where to intersect means to overlap. As an illustration, he gave a result which says: if a collection of subsets of an n-element set has the property that any two subsets in the collection intersect, then that collection cannot have more than 2^n subsets in it. (It is easy to verify that the stated bound is attained.)

Harary mentioned **Fan Chung** in his 15-minute talk on sum and difference graphs as having character theoretical techniques for obtaining bounds on the diameters of graphs. Since the latter was in attendance, I sought her out for details. (She is married to Ron Graham of Bell Labs.) It quickly became apparent that her work is pertinent to routing problems in distributed memory/processing arrays, as being considered for HORIZON at SRC. [redacted] She sent me quite a collection of preprints, including a crucial lemma by Nicholas M. Katz which appears to be significant in its own right. Katz obtains a bound on certain sums of characters; I have a copy of his preprint.

Chung's principal result translates Katz's lemma into a bound on the diameter of a k-regular graph in terms of the eigenvalues of its adjacency matrix. I have the abstract of her relevant papers. The papers Chung sent me are as follows:

(a) an estimate for Character Sums (by Katz, 5pp, used in (b)

(b) Diameters and Eigenvalues (19 pp)

(c) The Average Distance and Independence Number (12 pp)

(d) A Dynamic Location Problem for Graphs (with Graham & Micheal E. Saks, 36pp)

(e) Diameters of Graphs: Old Problems and New Results (26 pp)

(f) Quasi-random Graphs (with Graham & R. M. Wilson, 35 pp)

These papers are undated. I will try to supply copies to anyone who expresses interest.

Chung's paper (c) verifies a conjecture of GRAFFITTI. GRAFFITTI is a computer program, and the conjecture is that in any connected graph the independence number is at least as large as the average distance between vertices. GRAFFITTI was written by another attendee at the conference Siemion Fajtlowicz, Math Department, University of Houston. GRAFFITTI has apparently enabled Fajtlowicz to look at a large number of graphs and to formulate conjectures on the basis of the results. He has sent me a recent update on his conjectures (this has been going on for several years), which I will supply on request.

Fajtlowicz may be a valuable source for efficient graph algorithms even in cases where no really efficient algorithm is possible, ie in cases where the problem is NP complete. This is because GRAFFITTI has had to contend with such computations, for example in the case of the determination of a largest clique in a given graph. Fajtlowicz told me he would be happy to supply me with this particular algorithm. (I didn't actually ask for it, however.)

My own talk, on Mardi Gras morning, went very well. It was a variant of my talk at last

P.L. 86-36

P.L. 86-36

year's NSA Mathematical Sciences Meetings, so doesn't need elaboration here. I did meet a fellow interested in this sort of thing who seems to have done new and interesting work in this area. He is Frank Ruskey of the University of Victoria in British Columbia. He supplied me with a number of recent reprints which I am enthusiastic about, but which I haven't yet had a chance to assess in detail.

RECRUITING

In accordance with policy, I identified myself as an NSA employee, although my name tag read Department of Defense. I got permission from the conference organizing committee to leave recruitment material on the table reserved for new publications. I left copies of regular NSA technical recruitment brochure and of Brent Morris's brochure. I also placed a couple copies of the Proceedings of the NSA Mathematical Sciences Meetings. One copy of each I marked to remain on the table throughout the conference. The Proceedings attracted a lot of interest. Most of the time someone had it open and was reading it.

I suggested [redacted] Math Panel Executive, as an NSA contact for math employment inquiries. I stapled one of his business cards inside the table copy of the Tech Brochure and the Meetings Proceedings. I think these measures were both conservative and effective.

AFTER HOURS

Having completed my own presentation on Tuesday morning, I was in an ideal frame of mind for the afternoon and evening trip to New Orleans for the famous Mardi Gras celebration. (That day the conference adjourned at noon.) Having been prepared by warnings about staying out of dark alleys and not keeping a wallet in a back pocket, Bert Hartnell (Saint Mary's University, Halifax) and I spent most of our time going up and down Bourbon Street. Bert and I managed to wend our way intact back to our bus at 11 PM. I was worried that I had led Bert to ruin, but his talk the next morning was great.

I was treated very well by local people. There may actually be something to the notion of "southern hospitality." This does not refer only to people connected with the conference, who sort of had to be polite, but especially to the people in the town of Baton Rouge, in the shops and parks and streets. One towns-family even invited me to ride with them to New Orleans for Mardi Gras, but I decided to go with the conference crowd. I would enjoy going back. □

The Linguistic Society of America, San Francisco. December 27-29 1987

Reported by: [redacted] *P16*

The annual meetings of this society are the principal means of reporting developments in linguistic theory and applications. Keeping abreast of developments is important to NSA because of the increasing application of linguistics to Agency work. I hope that other NSA people with training in linguistics will be able to attend future meetings.

As proceedings are not published, I am summarizing the talks I attended, arranged by topic.

SYNTAX

Ronald Kaplan and Annie Zaenen, Xerox Parc, "Crossing Dependencies in Germanic Languages and Functional Precedence"

This paper gave an LFG account of infinitival and participial constructions in West Germanic languages. The LFG account allowed them to posit that arguments of an infinitival complement follow those of higher ,verbs without having to introduce them in the same phrase-structure rules.

⟷

Nigel Fabb, University of Strathclyde, "Non-Restrictive Relative Clauses and D-Structure Adjunction"

Scope tests show that a nonrestrictive relative clause is not c-commanded by its antecedent while a restrictive relative clause is. However, tests involving binding show that the antecedent does not c-command parts of the non-restrictive clause. Fabb examines two different options for explaining these data.

DISCOURSE

Joan Levinson, City University of New York, "The Linguistic Status of the Orthographic (Text) Sentence"

P.L. 86-36

This paper discussed factors which affect the distribution of marks of sentence punctuation. Levinson first showed that neither the boundaries of sentences nor the sentence internal punctuation is syntactically specifiable and then offered a theory of information grouping to account for punctuation. This theory suggest that punctuation is a guide for how to read a text and may reflect some kind of intonational grouping.

Jack Dubois, UC Santa Barbara, "Discourse Promotion and the Two-Track Hypothesis"

The one track hypothesis claims that anaphora operates on a single track. Thus, one can measure the distance between pronoun and antecedents in terms of the number of clauses. Dubois claimed that there are two tracks or two patterns of anaphora. In pattern 1 (for subjects), subsequent mentions are nonlexical. In pattern 2 (for objects), subsequent mentions remain lexical.

SEMANTICS

Jorge Hankamer, UC Santa Cruz, "Nested Antecedents"

Hankamer cited the following sentence:

> Bob presented his theory about the ECP, which is/*are pretty interesting.

where 'which' can be 'his theory about the ECP' or just 'the ECP' but not the plural entity corresponding to the set of the ECP and Bob's theory. He used this examples and others to show how the discourse model approach must be sensitive to syntactic relations.

Lewis Creary, J. Mark Gawron, John Nerbonne, Hewlett-Packard, "Toward a Theory of Locative Reference"

This paper proposed a treatment of locatives as components of arguments to predicates:

> (WORK agent: Tom location: (ON(Mass-Ave)), ((IN(Boston)))))

Toshiyuki Ogihara, University of Texas at Austin, "A Present Tense Embedded Under a Past Tense"

In the sentence:

> John said that Mary is pregnant.

a present tense in a verb complement clause is embedded under a past tense, thus violating the sequence-of-tense rule and causing the time of the embedded clause to contain both the time of the matrix and the speech time. Ogihara showed the deficiences of a syntactic solution (Enc forthcoming) and offered a semantic solution.

PRAGMATICS

Peter Tiersma, California Supreme Court, "The Language of Perjury"

This paper examined a Supreme Court opinion defining a false statement in the law of perjury: *Bronston vs United States.* Tiersma argued that Grice's maxims operate even in adversarial proceedings and that the court's definition of false statement needs revision.

PHONOLOGY

Natuso Tsujimura, Indiana University, "Japanese Suffixal Accentuation and Lexical Phonology"

The author identified a class of stem-making suffixes in Japanese which form intransitive/transitive pairs. Some of the suffixes show the pattern of recessive suffixes. The latter provide an exception of Halle and Mohanan (1985) and Halle and Vergnaud's (1987) claim that dominant suffixes, which are cyclic, must precede recessive suffixes.

Charles Li, UC Santa Barbara, "Contact Induced Tonogensis"

This paper showed how a Mongolian language (Baonan) acquired tones after close contact with a tonal language. Acoustic analysis of pitch and amplitude of Baonan disyllabic words revealed a system of two tones: high and low. Li hypothesized that the tonogensis was triggered by the infusion of loan words from a tonal language. This infusion caused pitch rather than amplitude to become a dominant distinctive feature.

SECOND LANGUAGE ACQUISITION

Eileen Kingsley and Ann E. Daubney-Davis, USC, "Native Speaker Nonnative Speaker Interactions: Variations in Negative Data"

This paper analyzed six twenty minute interviews of native-nonnative speaker situations in order to identify instances of negative feedback. These instances were classified as clarification, confirmation, reformulation, and distress. The researchers investigated the relationship between progress and frequency of responses to negative data. Results suggest a possible relationship between progress and the amount of negotiated interaction initiated by the learner.

William Rutherford, USC, "The Contribution of Second Language Acquistion to Learnability Theory"

Studies in second language acquistion (SLA) have mainly been studies of developing grammars. In contrast, theories of learnability (or how language can be learned via impoverished data and without negative evidence) have only recently been addressed in the SLA literature. Rutherford suggested two areas of research in learnability theory: the Subset Principle (Berwick 1985) and the the Uniqueness Principle (Pinker 1986). Examination of these two areas can help explain how learning occurs and thus offer refinement of the theory.

Monika Farner, Macalaster, "Tutorial Questions in Caretaker Speech"

This paper examined the language tutoring function of questions of two caretakers (German speaking and English speaking) of a bilingual child. The what-questions of both caretakers were analyzed. Results showed that questions of both caretakers increased in complexity over the period of study.

INVITED LECTURE

Charles Ferguson, Stanford University, "The Future of Applied Linguistics: An Overview"

Ferguson stressed the need for identification of problems in the real world requiring linguistic solution and the identification of resources to solve these problems. He pointed out the emergence of subfields in applied linguistics and how their development meshes with research in other areas. For example, he cited the effect of phonological theory upon the field of speech therapy.

PANEL DISCUSSION

"Writing Effective Reviews, Abstracts, and Referees' Reports"

This was a panel discussion sponsored by the committee on the status of women in linguistics. Panel members discussed how to write a review for a journal article, how to review a grant proposal, and how to write an abstract for the LSA conference.

CENTENNIAL LECTURE

(in honor of the centennial of Bloomfield's birth.
Leonard Bloomfield
is the father of American linguistics.)

"Bloomfield: The Man and the Man of Science"

R.H. Robins delivered the main lecture on Bloomfield. Following Robin's talk, a sympoosium of invited speakers (Isidore Dyen, Murray Emeneau, Charles Hockett, Henry W. Hoenigswald, Kenneth L. Pike, Frank T. Siebert, William G. Moulton, and Rulon Wells) spoke about Bloomfield's contributions to the field of linguistics.

AAAL SYMPOSIUM

"Canadian Immersion Programs: Recent Research", by Merrill Swan, Christina Bratt Paulston, Lily Wong-Fillmore, Fred Genessee

Swain: Five different studies were conducted: large scale proficiency, transfer study, age study, observation study, experimental study. The following conclusions were reached: a) Communicative competence includes discourse, sociological, and grammatical factors. b) The teacher needs to point out contrasts between languages and needs to link form with function. c) Beginning study at a later age is all right because the child needs a firm foundation in one language. d) Content teaching alone is not effective. There is a need for language instruction tied to content teaching.

Paulston: Paulston made a number of comments based on the results above: a) We -

need to focus upon language teaching not just language learning- Comprehensible input is not enough. b) The results of the study seem to imply that late immersion is as effective as early immersion. One must consider that perhaps early immersion students would have outperformed late ones if they had been taught differently. c) Methods to discriminate different teaching methods did not reveal any distinct differences in learning because teachers are basically eclectic. What is important is the quality of teaching.

Fillmore: Fillmore commented on classroom treatment studies: a) Evidence from the immersion studies showed that after many years of study children did not achieve native-like competence. It is clear that mere exposure is not enough to insure acquisition. Learners need input but they also need to use the language. The teachers can have a strong influence upon the degree of mastery. b) Students got little feedback about how their skills were deficient. They had little regular contact with French speakers outside the classroom.

Genessee: Genessee commented on the effect of variation in learner and environmental characteristics upon language mastery: a) Language achievement is affected by age of arrival and length of residence, but length of residence is a better predictor. b) Earlier study is not necesssarily better. Cognitive maturity and L1 proficiency both affect language achievement.

The International Communications Convention (ICC-88), June 1988, Philadelphia.

Reported by: [redacted] *P13*

Optical fiber communications was a mini-theme of ICC-88. About one quarter of the three-volume proceedings contained information about optical fiber and related telecommunications technology, and half of this was from foreign authors. Seven complete sessions were committed to the topic of fiber communications. This illustrates how important optical fiber is to the future world's communications. Within ten years more than 80 percent of the important point-to-point communications will pass over optical fiber links.

PART I: THE CONFERENCE

Leading Third World countries, viz: Brazil and China, are actively developing domestic fiber optic production capabilities, and intend to catch up with the fiber optic networks and ISDN digitization of the industrial nations by 2000. European and Japanese laboratories and manufacturers and PTT's are getting ahead of the US in the technology and use of fiber optics.

The technical development of fiber optic communications is still device-limited. The network designers cannot exploit the bandwidth of the fibers because the devices are too expensive, too inflexible and too noisy. Most of the problems of terrestrial trunk communications have been temporarily solved, and the US has installed over a million kilometers of fiber in a competitive scramble for long distance business, but the physical fiber is probably unsuitable for future needs. The potential demand for "fiber to the subscriber" is a much larger market, perhaps a hundred times larger than the trunk networks, but the electronics are expensive, and the designers have not pinned down a service they can offer at 150 Mbps or higher, which the non-business subscribers will pay for. They hope that HDTV will create a demand for the "last mile" of a total fiber network.

There has been a lot of activity in the U.S. laying trunk networks of fiber, as more than a dozen competitors sought part of the long distance market after divestiture. This has produced overcapacity, and mergers and bankruptcies are expected. In addition, there are severe regulatory and political barriers to development of an "all fiber" network in the U.S., as more lawyers have come into the telecommunications field. The Asians and Europeans have proceeded more slowly, installing much more local fiber than the U.S. and prolonging the experimental and trial stages while the technology changes. This difference was manifested in the sessions, where U.S. authors dominated the fiber trunk sessions, while foreign authors had more to say about processing, switching and local loops. The French have already installed fiber to millions of homes, compared to a few hundred residential fiber loops in the U.S. The foreign

P.L. 86-36

Current Mediterranean Submarine Cables

Most of the submarine cables in the Mediterranean are analog systems, but some fiber cables have been installed. The 1984 NTIA report on submarine cables by Schenck gives maps of the analog cables of that era, and also gives technical details. There are about 50 analog links, which are numbered on the Schenck maps. The slide shown by Marone during the oral presentation of paper 2.7 indicated existing and future optical fiber links on many of the same routes as the Schenck maps. The analog cables circa 1984 are listed below. Presumably many of them will be replaced by fiber, or by repeaterless flouride fiber cables within the next ten years.

Number	Name	Capacity	Date	Constr. contract
21	Sicily-Malta	36 ch.	1955	sub cables
23	Kelibia-Bou Ficha/Tunis	120	1956	cit
26	Italy-Tunisia	60	1956	bpo
34	Marseille-Bord el Kiffan	60	1957	cit
36	Italy-Sardinia I	60	1957	stc
52	Trapani-Cagliari	120	1962	stc
53	Sicily-Crete	60	1962	scl
56	Canet Plage-Mers el Kebir	60	1962	cit
81	Cannes-Ile Rousse	96	1966	cit
90	Canet plage-Tetouan	96	1967	cit
96	Marseille-Tel Aviv (MARTEL)	96>128	1968	excofina
99	Cantanzaro-Lekhaina	480	1969	scl
100	Italy-Sardinia 2	480	1969	stc
101	Agrigento-Tripoli	120	1969	stc
104	Barcelona-Pisa	480	1969	stc
107	Marseille-Bizerte	96	1969	cit
109	St. Raphael-St. Tropez	480	1970	submarcom
110	Marseille-Beirut	160	1970	cit
113	Mediterranean-Atlantic (MAT 1) Estepona-Palo	I480>640	1970	stc
122	Peninsula-Balearic Is. (PENBAL 1)	900>1380	1971	c&w
125	Pisa-Algiers	480	1972	stc
129	Marseilles-Bord el Kiffan	480	1972	cit
134	Cantanzaro-Alexandria	480	1972	stc
137	Alexandria-Beirut	120	1972	cit
146	Barcelona-rome	1380	1974	stc
147	Civitavecchia-Cagliari	1380	1974	stc
151	France-Greece-Lebanon-Cyprus	480	1974	submarcom
152	St. Raphael-La Foux	2340	1975	submarcom
154	Heraklion-Lagonissi	1380	1975	stc
156	TELPAL (Tel Aviv-Palo)	1380	1975	stc
157	ANNIBAL (Perpig.-Bizerte)	640	1975	submarcom
160	Algeria-Spain	480	1975	submarcom
162	MARPAL (Marseilles-Plao)	2580	1976	submarcom
174	Italy-Turkey	480	1976	stc
177	Rome-Palermo	1800+2tv	1977	stc
180	Marseille-Bastia	2340	1977	submarcom
184	PENBAL 2	3900	1977	stc
195	AMITIE'(France-Morroco)	2340	1978	submarcom
205	Tripoli-Benghazi	900+2tv	1979	NEC
206	Genoa-Sassari	3600	1979	stc
207	La Seyne-Tripoli	640	1979	submarcom
210	BARGEN (Barcelona-Genoa)	4140	1979	stc
215	France-Algeria 4	2580	1980	submarcom
234	Greece-Syria PALMYRA	480	1981	submarcom
236	Greece-Cyprus 2 APOLLO	1380	1981	stc
237	France-Greece 2 ARTEMIS	2580	1981	submarcom
241	Sardinia-Sicily 2	3900	1982	stc
247	Juan le Pins-Cagnes sur Mer (France-France) (fiber optic)	340 mbps	1982	submarcom
249	France-Tunisia 3	2580	1983	submarcom
254	Greece-Egypt ALEXANDROS	624	1983	att

PTT's can develop fiber nets as part of an integrated telecommunications plan. This takes longer, but costs less, and probably avoids the rapid obsolescence and waste of the American efforts.

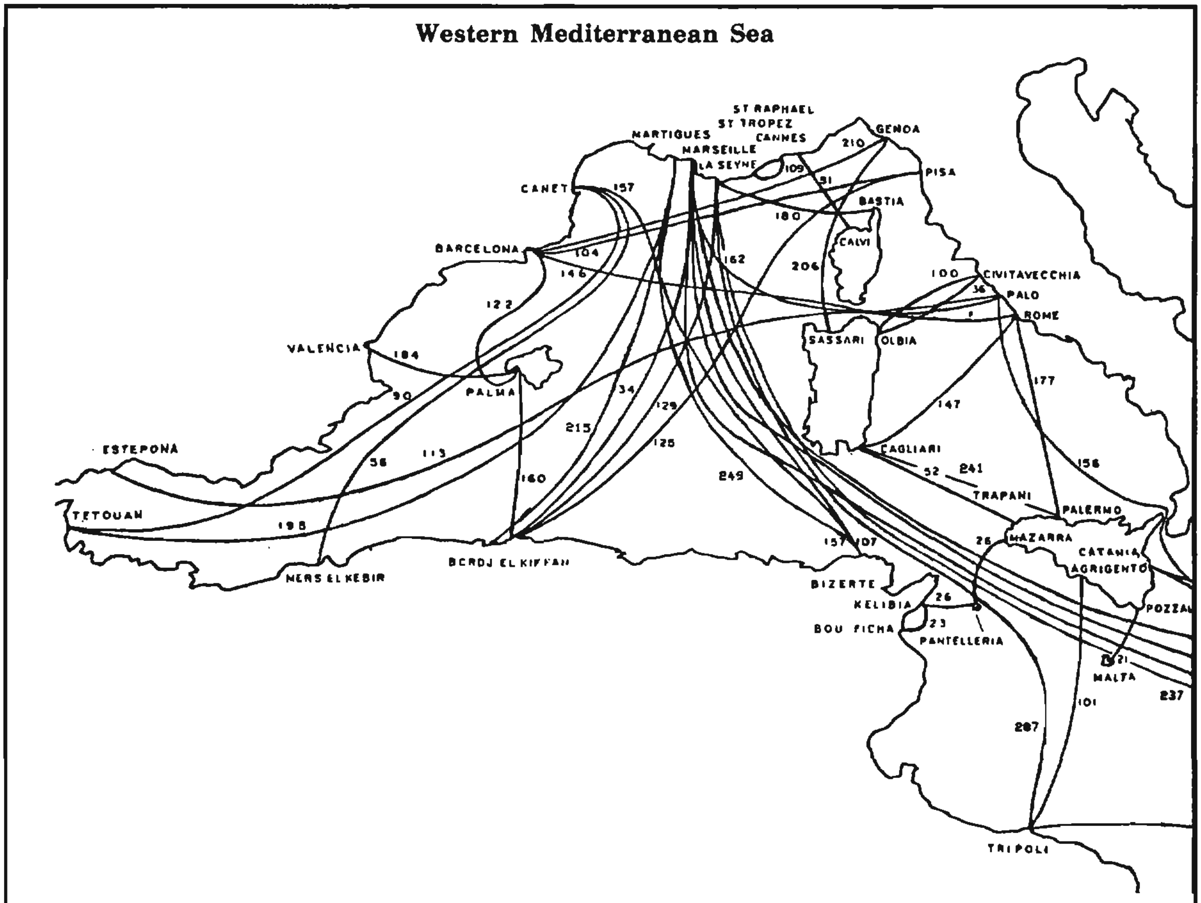
One point of interest was the development of flouride based fiber for repeaterless submarine cable links in the Mediterranean by the Italian CSELT. They expect that transmission at long wavelength will allow 300 Km repeaterless links at 2.4 Gbps by 1992, and even longer spans by 2000. Another point was the prevalence of damage to the fiber trunks from backhoes and other effects, which is spurring the design of "survivable" networks. There is a plan for a global synchronous optical network (SONET) which will use TDM multiplexing to carry 150 Mbps services at line rates of 2.4 Gbps. (16 x 150 = 2400). However, there are critical timing problems in a synchronous net which are exacerbated by the US divestiture that has different interconnecting networks driven by uncoordinated clocks.

Although there is intensive research and progress, the manufacturing of certain types of fiber and components is still difficult, and the development and operation of optical fiber networks is still a "jungle" of problems. Costs, applications, markets, and integrating the wideband capacity of the fibers into the existing narrowband copper and radio nets are creating uncertainties and delays in the actual deployments of fiber and the development of machines to interface fiber with non-fiber nets. In the meantime, the technology is spreading all over the world.

AN OVERVIEW OF THE SESSIONS

Fourteen of the 54 sessions dealt entirely or partly with optical fiber.

Western Mediterranean Sea



Session 1. on optical switching presented different schemes for switching of trunks, MANs, LANs and subscriber loops. The designers are trying to develop an all-optical net. All of the papers were foreign.

Session 2. on long-haul fiber systems was dominated by Americans. The competitive race to build long distance fiber trunks by SPRINT, WILTEL and others has required elaborate testing and installation procedures because the new carriers did not have organic resources to do the installation and splicing. Undersea fiber cables will have "wetmux" switching, and repeaterless flouride glass links.

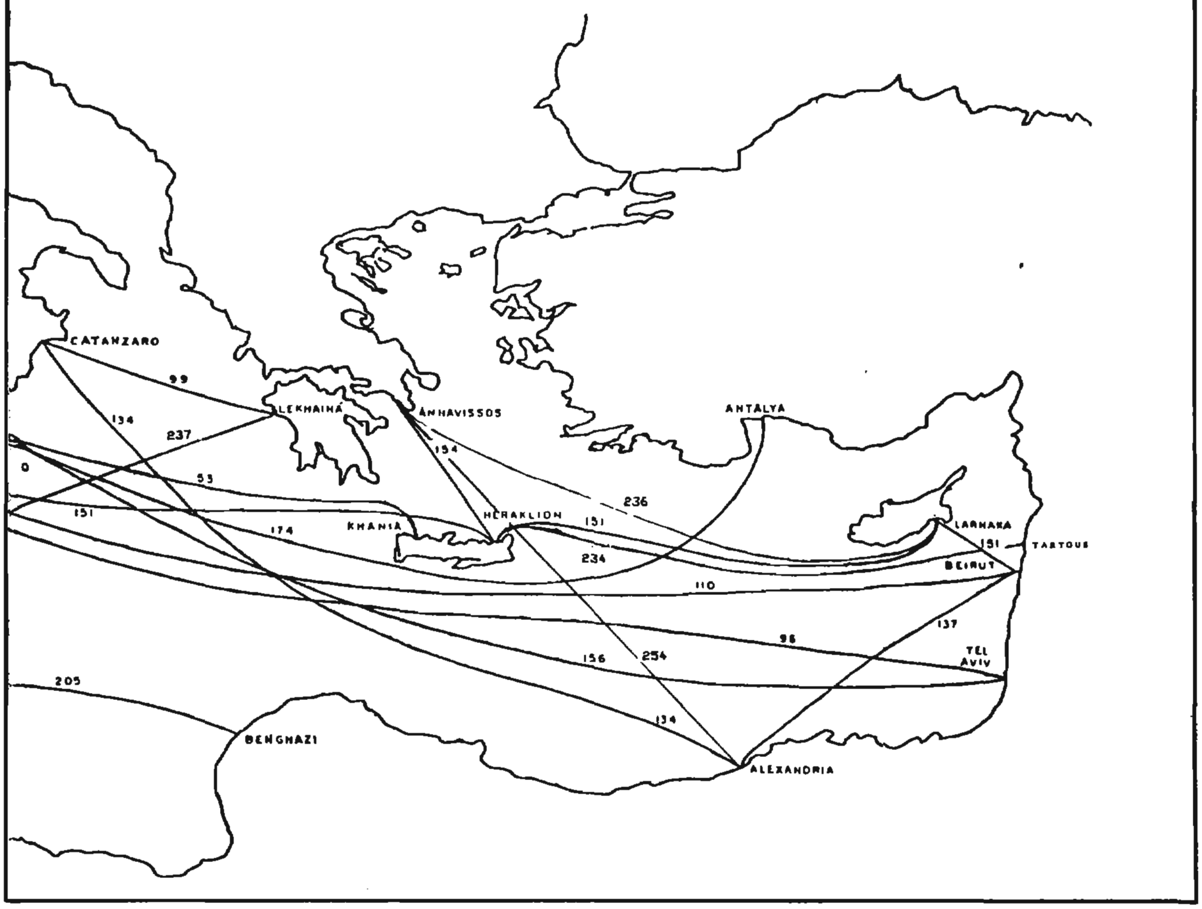
Session 10 on high speed transmission was mostly foreign papers. Foreign laboratories have demonstrated 10 Ghz linear amplifiers and receivers, and 700 Km repeaterless spans. Fast transmission is device-bound, and although more than a million kilometers of fiber have been installed, it is probably the wrong kind because it will not prevent polarization shifts that degrade coherent transmission.

Session 11 on digital cross-connects systems described the machines for interfacing between fiber trunks and local networks, particularly fiber hubbing nets. The existing asynchronous digital networks using radio and cable at electronic speeds must connect into high speed synchronous optical nets (SONET).

Session 19 on simulation of lightwave systems covered mathematical models of fiber, lasers, waveforms and subnetworks.

Session 28 on fiber access to the home described current work in the critical "last mile" of fiber installation. Costs are a major factor. The Japanese and French are trying to get an economical transition from current services to future wideband services. They have fewer regulatory barriers to the PTT's delivering CATV, but still have to deal with

Eastern Mediterranean Sea



established interests. Some of the architectures create an "ether" in which all the traffic reaches all the subscribers, while other designs select traffic flow at central switches. Combinations of fiber and coaxial cable are use to reduce the number of fiber splices and taps. Analog transmission of TV is much cheaper than digital coding and decoding, taps and bridges. Synchronization of many independent local and long distance digital fiber nets will be very tricky.

Session 29 on broadband systems showed GTE's preference for circuit over packet switching. Siemens considers 150-600 Mbps services to subscribers over fiber loops. Fujitsu prefers Asynchronous Transfer Machines (ATM) for interface between narrowband ISDN at 64 Kbps and broadband ISDN at 150 Mbps. Memory matrix TDM switches allow 8 streams of 150 Mbps to be combined into a 1.2 Gbps signal, in a switch with a throughput of 8 x 1.2 = 9.6 Gbps, currently demonstrated. The Japanese like Transport Processors (TP) for the expected bursty nature of multi-gigabit broadband services.

Session 37 on coherent lightwave transmission was dominated by U.S. papers. The Japanese noted problems in manufacture of polarization-maintaining fiber, which they think necessary for coherent systems. Coherent lightwave communications (CLC) can be used to carry microwave compatible transmissions, based on existing microwave systems. Optical amplifiers will give 20-30 dB gains. AT&T thinks a 4.5 terabit/sec star net can be built with currently available components. The decisions to install monomode fiber that does not preserve polarization and adopt TDM multiplexing will dominate switching and CLC.

Answers to

CRYPTO-"LOG" PUZZLE
2nd Issue 1988

```
 1.  Easy as falling off a log
 2.  Psychological
 3.  Logjam
 4.  Lincoln logs
 5.  Loge
 6.  Logrolling
 7.  Logy
 8.  Ship's log or logbook
 9.  Catalog
10.  Sawing logs
11.  Slept like a log
12.  Tagalog
13.  At logger-heads
14.  Backlog
15.  Sat like a bump on a log
16.  Yule log
17.  Analog computer
18.  Log cabin
```

Session 46 on lightwave local networks showed a number of schemes to operate nets at terabit rates. One academicians's scheme used pulse position addressing combined with spread spectrum transmission over fiber. Multi-fiber rings allowed many different architectures to be expressed over the same robust physical net. The Japanese proposed fiber LAN based on combining FDDI access with CSMA/CD transmission.

Session 47 on broadband ISDN and packet switching was concerned in part with how to extend broadband ISDN services to residential customers. TV and HDTV are seen as the main traffic to non-business BISDN customers. Broadband ISDN will require a global SONET synchronous optical net and ATM (asynchronous transfer machines) for interface to the existing asynchronous digital networks.

∞ ∞ ∞

In general the cost of the electronics is too high for subscriber optical loops. Europeans and Asians are able to pursue systematic development of integrated optical networks without the regulatory problems and fragmentation that affects the U.S. telecom environment. The U.S. has deployed a lot of yesterday's technology for todays short-term market share, while the foreigners are proceeding more slowly but on a broader front to get the markets, the costs, the technology and the customer demands coordinated in a profitable way. In some areas, e.g.. subscriber services, they are well ahead of the U.S. This may give them a long-term advantage, even inside the U.S. market.

PART II: SIGINT IMPLICATIONS OF TRENDS IN FIBER OPTICS COMMUNICATIONS

(U) Most of the world's long distance point-to-point communications will pass over optical fiber trunks within fifteen years. The capacity of the fiber trunks, and the low cost of transmission, tends to concentrate enormous amounts of traffic from thousands of low speed tributary systems onto a single fiber.

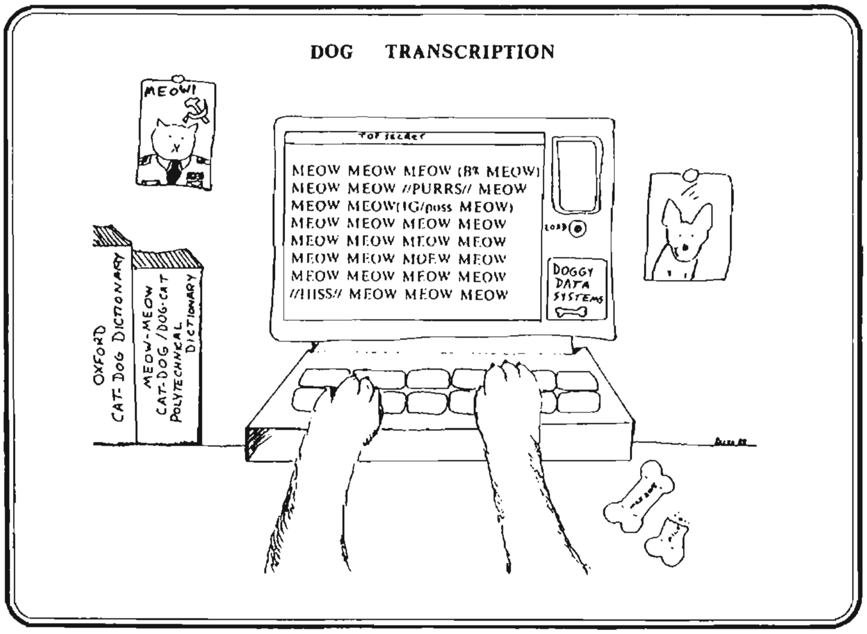
(U) The impact of fiber is so significant that even COMSAT is installing fiber. Fiber is already displacing traffic from satellite and microwave links. For broadband digital services, it has no equal. Bit rates above 3 Gbps are already in service, and rates above 50 Gbps will soon be in use on single fibers. At the same time, local nets will be carrying terabits of traffic, and on many local nets all the bits will be available to all the subscribers. Analog transmission of microwave signals will also occur on fiber, probably as part of an analog-digital format. Improvements in glasses and optical components will allow both high bit rates and long repeaterless spans. Infrared wavelengths at 3.4 microns will be used to take advantage of low attenuation in new glasses.

[redacted]

[redacted]

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

On The Lighter Side



by Charles Ralya *courtesy of:* Vox Topics

Call for Speakers

WHEN YOU WERE IN SCHOOL, DID YOU EVER WONDER:

WHY DO WE HAVE TO SOLVE THESE DARN LOGARITHMS?

WHY DO WE HAVE TO KEEP PROVING THAT TRIANGLES ARE CONGRUENT?

WHY DO WE HAVE TO LEARN MATH? I'M NEVER GOING TO USE IT!

STUDENTS ARE STILL ASKING THESE QUESTIONS.

THE LOSS OF STUDENT INTEREST IN MATH IN PAST YEARS IS THREATENING THE FUTURE OF U.S. MATH AND TECHNOLOGY.

THE **NSA MATH SPEAKERS BUREAU**

HAS BEEN ESTABLISHED BY THE MATH PANEL WITH THE GOAL OF **INCREASING YOUNG STUDENTS' INTEREST IN MATHEMATICS.**

You can help answer the WHY questions by visiting Elementary, Junior High or High School math classes in the State of Maryland as a Guest Speaker. Stimulate students' minds with discussions of:

- the beauty of mathematics in nature
- elementary cryptology
- how to solve logic puzzles
- careers in math / math in careers
- any topic that you would like to present — we have a library of topics to give you ideas!

YOU DON'T HAVE TO BE A MATHEMATICIAN TO BE A MATH SPEAKER!

For more information, contac[redacted]Coordinator, NSA Math Speakers Bureau, G423, 963-6423s, 688-5361b.

"If the math community suffers, the National Security Agency suffers."

—[redacted]Chairman, NSA Math Panel

P.L. 86-36

P.L. 86-36

CRIB PUZZLE

"LEFTOVERS" by [redacted]

This puzzle is *UNCLASSIFIED*

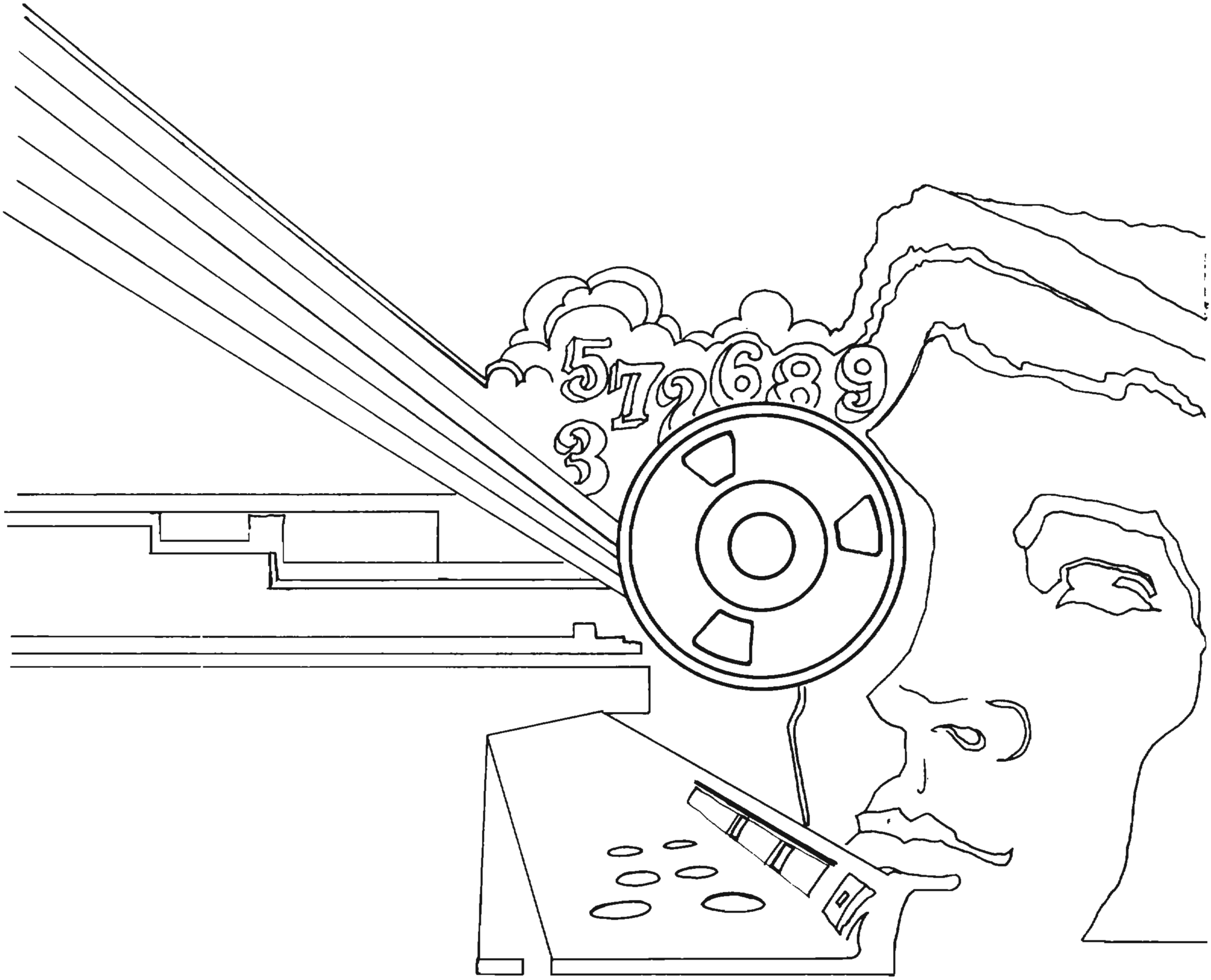
Each of the clues below contains definitions for four 4-letter words. Removing one letter from each of the first three 4-letter words and combining the resulting 3-letter pieces, in the order given, will form a new 9-letter word. The letters you removed, also taken in order, will spell a 3-letter word. You can now add a letter to some position of this 3-letter word to form the answer to the fourth definition. The letter you added is the leftover. The seven leftovers, in order, spell the solution word. Call me with the correct solution at 1351(s) and I'll print your name in the next issue.

Ex.	Bony growth **SPUR**	Ice arena **RINK**	Give temporarily **LEND**	Singe **BURN**	**B**

Remove the "U" from "SPUR," the "R" from "RINK" and the "N" from "LEND." Combine the 3-letter pieces to form the word "SPR INK LED." The removed letters spell the word "URN," and adding the letter "B" forms the word "BURN," the answer to the fourth definition. The leftover is the "B."

1.	Something on a foot or an ear	College figure	Dispatch	Pour	
2.	Beta Orionis, e.g.	Bucket handle	Sympathy	Incline	
3.	Enos' grandfather	Egyptian goddess	Wood's partner	Join	
4.	Way out	Contact	On stage	Streamlet	
5.	Imitator	Crossing	Small lake	Assistant	
6.	Concrete	Smoker	Feathers' prerequisites?	Fuzz	
7.	Road hazards	Average	Recounting	A fuel	

Courtesy of CRIB


572689
3