MEMORANDUM
RM-3765-PR
AUGUST 1964

ON DISTRIBUTED COMMUNICATIONS:
IX. SECURITY, SECRECY, AND TAMPER-FREE CONSIDERATIONS

Paul Baran

PREPARED FOR:
UNITED STATES AIR FORCE PROJECT RAND

The RAND Corporation
SANTA MONICA • CALIFORNIA

MEMORANDUM
RM-3765-PR
AUGUST 1964

ON DISTRIBUTED COMMUNICATIONS:
IX. SECURITY, SECRECY, AND TAMPER-FREE CONSIDERATIONS

Paul Baran

This research is sponsored by the United States Air Force under Project RAND—Contract No. AF 49(638)-700 monitored by the Directorate of Development Plans, Deputy Chief of Staff, Research and Development, Hq USAF. Views or conclusions contained in this Memorandum should not be interpreted as representing the official opinion or policy of the United States Air Force.

DDC AVAILABILITY NOTICE
Qualified requesters may obtain copies of this report from the Defense Documentation Center (DDC).

The RAND Corporation
1700 MAIN ST. • SANTA MONICA • CALIFORNIA • 90406

PREFACE

This Memorandum is one in a series of eleven RAND Memoranda detailing the Distributed Adaptive Message Block Network, a proposed digital data communications system based on a distributed network concept, as presented in Vol. I in the series.* Various other items in the series deal with specific features of the concept, results of experimental modelings, engineering design considerations, and background and future implications.

The series, entitled On Distributed Communications, is a part of The RAND Corporation's continuing program of research under U.S. Air Force Project RAND, and is related to research in the field of command and control and in governmental and military planning and policy making.

The present Memorandum, the ninth in the series, is a consideration of the security aspects of a system of the type proposed, in which secrecy is of paramount importance. Present security concepts appear to be based upon an implied assumption that any "cleared" person must be trusted, and that any "uncleared" person is a potential spy. Further, information is either classified or it is not. From time to time a disquieting occurrence** causes us to wonder if these "binary" attitudes are really valid, and should form the basis upon which to predicate a military communications system for the future.

This Memorandum, in which the underlying concepts and resulting safeguards to be built into the Distributed

---

*A list of all items in the series is found on p. 37.

**Such as the William H. Martin and Vernon F. Mitchell affair at NSA; see: Sanche de Gramont, The Secret War, Dell Publishing Company, New York, p. 405.

Adaptive Message Block Network are described, is written from the viewpoint that we should fully anticipate the existence of spies within our ostensibly secure communications secrecy protection structure; hence, our primary interest should be in raising the "price" of espied information to a level which becomes excessive.

SUMMARY

One key difference between a civilian and a military communications system is the provision made in the latter for the preservation of secrecy and for immunity from destructive tampering. These considerations are most effectively integrated into a network as an integral part of the switching mechanism, rather than in the form of "black boxes" tacked on as an afterthought. This Memorandum is an examination of the proposed Distributed Adaptive Message Block Network's use of this integrated design approach to the problem of providing cryptographic security.

It is acknowledged that the approach represents a departure from conventional practices, which have traditionally maintained a separation between the design of the communications network itself (which is most often a slight modification of a system originally designed for civilian use) and the design and implication of cryptographic safeguards. The rationale is stated that recent major advances in digital computer technology now make it technically feasible and economically desirable to consider a system designed primarily with military applications in mind, and which from the outset of design is cognizant of cryptographic requirements.

As a prelude to the proposal, however, the view is expressed that if one cannot safely describe a proposed system in the unclassified literature, then, by definition, it is not sufficiently secure to be used with confidence. A totally secure system design requires a full understanding of the problem by everyone involved with every part of the system--even those who would not normally hold any security clearance.

As applied to the proposed distributed network system, the specified integrated design would include various combinations of:

1) End-to-end cryptography;

2) Link-by-link cryptography;

3) Use of automatic error-detection and repeat transmission (allowing use of more powerful cryptographic transformations);

4) Transmission of successive Message Blocks by ever changing paths;

5) Use of a cryptographic scheme which requires complete and correct reception of all previous traffic in a conversation in order to decrypt subsequent Message Blocks, and which suppresses silence periods in voice and data transmission;

6) An initial system design which assumes potential infiltration by enemy agents having access to portions of the system and the cryptographic key bases:

   a) Use of key bases split into separate parts and delivered by two or more individuals;

   b) Non-acceptance of a Message Block for processing (and non-advancement of the crypto synchronization count) until preliminary filtering tests for validity of source and timing have been accomplished;

   c) Use of an essentially new key for each separate conversation (permitting intermingling of classified and unclassified traffic without fear of security compromises);

   d) Encouraging heavy use of the system for unclassified traffic, and the processing of all traffic as if it were of the highest secrecy level (perhaps even to the extent of intentionally adding fraudulent traffic between fictitious subscribers).

FOREWORD

I would like to emphasize the fact that only information found in the open literature has been used in the preparation of this Memorandum. The often "touchy" subject of security and secrecy in relation to cryptographic considerations is herein considered without use of or access to classified material and without the benefit of a cryptographic security clearance.

CONTENTS

I. INTRODUCTION

Historically, military communications networks have been based on techniques and practices originated to meet civilian needs. And, although the military security environment is more demanding, as a practical matter there have always been technological limitations forcing the erection of "make do" patchworks for its communications systems. Starting with an essentially civilian-based system, a little is added here and a little there until we convince ourselves that the remaining security shortcomings are due to either technological or to economic lags in the state-of-the-art.

The last few years have witnessed major breakthrough upon major breakthrough in the digital computer technology. In light thereof, it is now pertinent to reconsider the ways in which we would like to build communications systems, taking advantage of these new developments.

An entire Memorandum in this series is being devoted to the problem of security alone because of its underlying importance both to the system and in the large, and due to a relative underdevelopment of the subject in general. For example, Bloom, Mayfield, and Williams in a survey on the problems of military communications report that Army officers most often cite security as their primary communications problem.*

In the proposed system synthesis, the constraints of existing practices have been purposely avoided in order to better consider an entire system from scratch. First considered are the military requirements, following which the discussion moves toward a hardware synthesis making use of this new era's rapidly advancing computer technology.

---

*Bloom, Joel S., Clifton E. Mayfield, and Richard M. Williams, Modern Army Communications, Final Report, The Franklin Institute Laboratories for Research and Development, Philadelphia, January 1962, p. 32.

However, before discussing the proposed direction of solution, it is desirable to digress and touch upon a subject rarely seen in the unclassified literature, but one that must be understood in order to fully appreciate what is being proposed: the problem of the Secrecy about Secrecy.

II. THE PARADOX OF THE SECRECY ABOUT SECRECY

THE ASSUMPTION OF A CLEAR DICHOTOMY BETWEEN CLASSIFIED AND UNCLASSIFIED SUBJECT MATTER

Present-day security laws divide all military information into two non-intersecting categories: information is either classified, or it is not. If it is, we go to great extremes and much expense to keep it secret, while relatively little, if any, attempt is made to protect "unclassified" information from untoward disclosure. If, by an almost metaphysical process, a subject is deemed to be slightly to the non-applicable side of a fuzzy classification line, it is often made freely available to all.

It is interesting to note that private "proprietary" trade secrets are often better kept than are secrets affecting national security (if the time between first disclosure and open publication "leak" is used as a measure). Yet, the weight of stringent penalties (not to mention the pressures of patriotism) exists to protect government secrets. Furthermore, most companies allow their civilian secrets to be locked in thin wooden desk drawers, to be discussed with people whose backgrounds haven't been investigated, and even to be discussed over the civilian telephone networks. Perhaps the difficulty in preserving military secrets is caused, at least in part, by the high price and inflexibility of present-day cryptographic equipment, combined with the imposition of rules that in fact hamper expeditious handling of military communications.

COST AND RESULT OF PRESENT-DAY CRYPTOGRAPHIC EQUIPMENT

Present-day communications cryptographic equipment is very expensive; as a result, it is not economically feasible to provide all the cryptographically-secure channels which

might be otherwise considered necessary. For example, it has been said that the cost of providing cryptographic security on every communication link carrying sensitive military traffic could exceed the total expenditure for the entire remainder of the system. Thus, our present, and not very satisfactory, response to this dilemma is to force large volumes of "unclassified" military traffic to be sent out over the communications networks in the clear, accessible to all.

The writer has heard military communicators comment that the higher the rank of an officer using an unclassified communication circuit, the greater the probability that highly classified information will be discussed in the clear. Further, the greater the military tension, the higher the probability. Again, the reasons appear quite valid and overriding--particularly in military crises (and in more remote countries) the commander is so grateful to have any communications resource, that he does not demand (and indeed, given the situation, such demand would probably be unreasonable) the non-crisis-period luxury of voice cryptography.

In present-day communication networks, a circuit carrying information between two stations is usually routed over the same links day in and day out. It is only slightly more difficult to eavesdrop on networks containing switching nodes, inasmuch as the number of alternate paths is highly proscribed. It appears to be a relatively easy task to predict which links will convey traffic between any given station and any end destination.

ON SECRECY OF SECRECY

Discussions of the problems of security and secrecy with regard to military electronics equipment are more often found only in highly classified documents. It

should be noted that this Memorandum has been purposely written to be unclassified, for we feel that unless we can freely describe the detailed workings of a proposed military communications system in the open literature, the system hasn't successfully come to grips with the security problem. No violation of security can occur with this procedure because the only background information used is that found in the unclassified literature, including patents, hardware development progress reports, advertisements, newspaper and journal articles, etc. Therefore we assume we have available to us less information concerning U. S. communications security procedures than does our enemy counterpart, giving us freedom to talk without fear of saying anything not otherwise obvious. Further, this material was prepared without our holding a cryptographic clearance* (which we do not want, in any case) and, therefore, without access to information thereby restricted. If we had such a clearance, we would be so constrained as to be unable to discuss this subject without fear of loss of the clearance.

Without the freedom to expose the system proposal to widespread scrutiny by clever minds of diverse interests, is to increase the risk that significant points of potential weakness have been overlooked. A frank and open discussion here is to our advantage.

The overall problem here is highly reminiscent of the atomic energy discussions in the 1945-55 era--only those who were not cleared were able to talk about "classified" atomic weapons. This caused security officers to become highly discomfitured by the ease with which unclassified clues were being combined to deduce highly accurate

*Industrial Security Manual, Department of Defense, U.S. Government Printing Office.

versions of material residing in the classified domain. This points up a commonly recurring difference of opinion (or philosophy) between the security officer and the technically trained observer. The more technical training an individual possesses, the less confidence he seems to have of the actual value of secrecy in protecting the spread of new developments in a ripe technology. True security does not always equate to blanket unthinking secrecy. While the security value of effective secrecy can be high, we must be realistic and acknowledge the constraints of living in a free society where effective secrecy in peacetime is almost impossible. Avoiding a touchy subject by falling back on edicts rather than rationality may automatically insure the continued existence of the touchy subject.

Secrecy of Cryptographic Design

If the distributed network described in this series is to be built, many people must become involved in its design, manufacture, maintenance, and operation. It would be foolhardy to think that we can actually withhold the hardware details from our enemies. The network would be essentially worthless unless it were so designed that its operations could be discussed openly without resorting to the make-believe game of security in which we all agree to avoid talking about weaknesses--even if these weaknesses are obvious to all. Secrecy of cryptographic design can be self-defeating if it is maintained by blanket edicts in lieu of judicious restraint. The more bright people we can get to review this system now--particularly computer trained individuals--the less trouble we need expect in the future.

The Assumption of Almost-Infinite Effort in Code-Breaking

Part of the reason that current crypto systems are expensive is found in the requirement that they totally survive the efforts of a determined enemy, applying all his energies to break the code. The thought occurs that the money now being spent to insure a high degree of security in cryptographic devices might be better spent buying many more lower-quality cryptographic devices.

If it were not for the almost unyielding requirement for absolute security, we would be able to consider using many low-cost cryptographic schemes providing capability for handling all traffic. While these lower-protection-rate ciphers might yield to a determined enemy, extreme cipher-breaking activity could be made to extract such a high price, that in the long run, a lesser volume of really secret data would be lost. Such less-powerful crypto devices could help reduce the burden of the human classification decision and would speed communications.

Part of the delay in today's hard-copy communications system is the time spent in deciding whether text should be classified or not. Anything that reduces this inordinately heavy burden of deciding whether something is or is not classified, makes the goal of having all military traffic encrypted a highly desirable one in itself.

The proposed network is a universal high-secrecy system, made up of a hierarchy of less-secure sub-systems. It is proposed that the network intentionally treat all inputs as if they are classified, in order to raise the intercept price to the enemy to a value so high that interception would not be worth his effort. Of course, that extra layer of conventional cryptography would be maintained for use in those extremely sensitive cases where the proposed approach might seem risky.

Thus, fullest advantage is taken of the mechanism within the proposed system that takes a channel or a message and chops it into small pieces (like a fruit salad), transmitting it on as a series of message blocks, each using a different path. Additionally, much unclassified material is purposely transmitted cryptographically, and perhaps even a light dose of obsolete traffic is mixed in. Given a big enough bowl, it becomes very difficult to separate the garbage from the salad.

III. SOME FUNDAMENTALS OF CRYPTOGRAPHY

DIGITAL TRANSMISSION

One reason cryptographic equipment is expensive is that it is necessary to convert all signals into digital form. (Digital operations permit complex cryptographic operational transformation of the data stream without irrevocable added distortion.) Today's cryptographic devices have not been designed as an integral part of any particular communications system, but, rather, are "black boxes" added onto communications networks designed for other purposes and other times.

In the all-digital system concept being developed, a potential savings occurs by combining the digital switching equipment together with digital cryptographic equipment. Such a combination, irrespective of potential savings offered, is not implemented without difficulty, for it represents the merging of two design areas historically kept apart, both managerially and technically. Probably, a prime reason that on-line cryptography has been so slow in developing is due to the tendency to fund communications systems under the service budgets, while the cryptographic devices used by these systems are supplied as government-furnished equipment by the National Security Agency (NSA). Hence, the true cost of the cryptographic equipment in a system is often not appreciated by the communications system designer, and feedback which would encourage better overall design of future systems by reducing the high cost of the cryptographic gear is lacking. Perhaps better systems would result if this suboptimization were avoided by making the hidden cost of the cryptographic equipment in each communications system more visible. Thus, in the development of the distributed network concept, it was felt desirable to include the cost of the cryptographic equipment as an integral part of the switching equipment.

LAYERS OF ENCRYPTION

On-line cryptographic communications operation is defined as one in which information is inserted into a network in real-time, converted by cryptographic transformation, transmitted, received, decrypted, and output to the recipient without appreciable delay.

On-line communications traffic can be encrypted at several different stages. These choices might be labeled end-to-end, link-by-link, and, a combination of the two, double encryption (see Fig. 1).

End-to-End Encryption

In the end-to-end encryption, a cryptographic device is connected adjacent to the user and a reciprocal transformation device at the receiver. It is an economical way of using cryptographic gear where the two end-points have sufficient volume to warrant tying up the special terminal equipment on a full-time basis. Figure 1a depicts end-to-end encryption, in which the message and the crypto encoder reside in a secure area, as does the end addressee. The same data transformation device (key) must be available to both crypto units.

Cryptographic Data Transformations

A canonical form of cryptographic transformation uses two synchronized pseudo-random binary streams generated by two "key generators," one at the transmitting site, the other at the receiving site. Figure 2 shows the operation of this process. A short key-base contains the starting and modification parameters of a key generator. The key generator creates a long non-repeating digital stream. This stream is then combined with the outgoing message by some logical transformation and the resulting stream, comprising the encrypted text, is transmitted. There are a

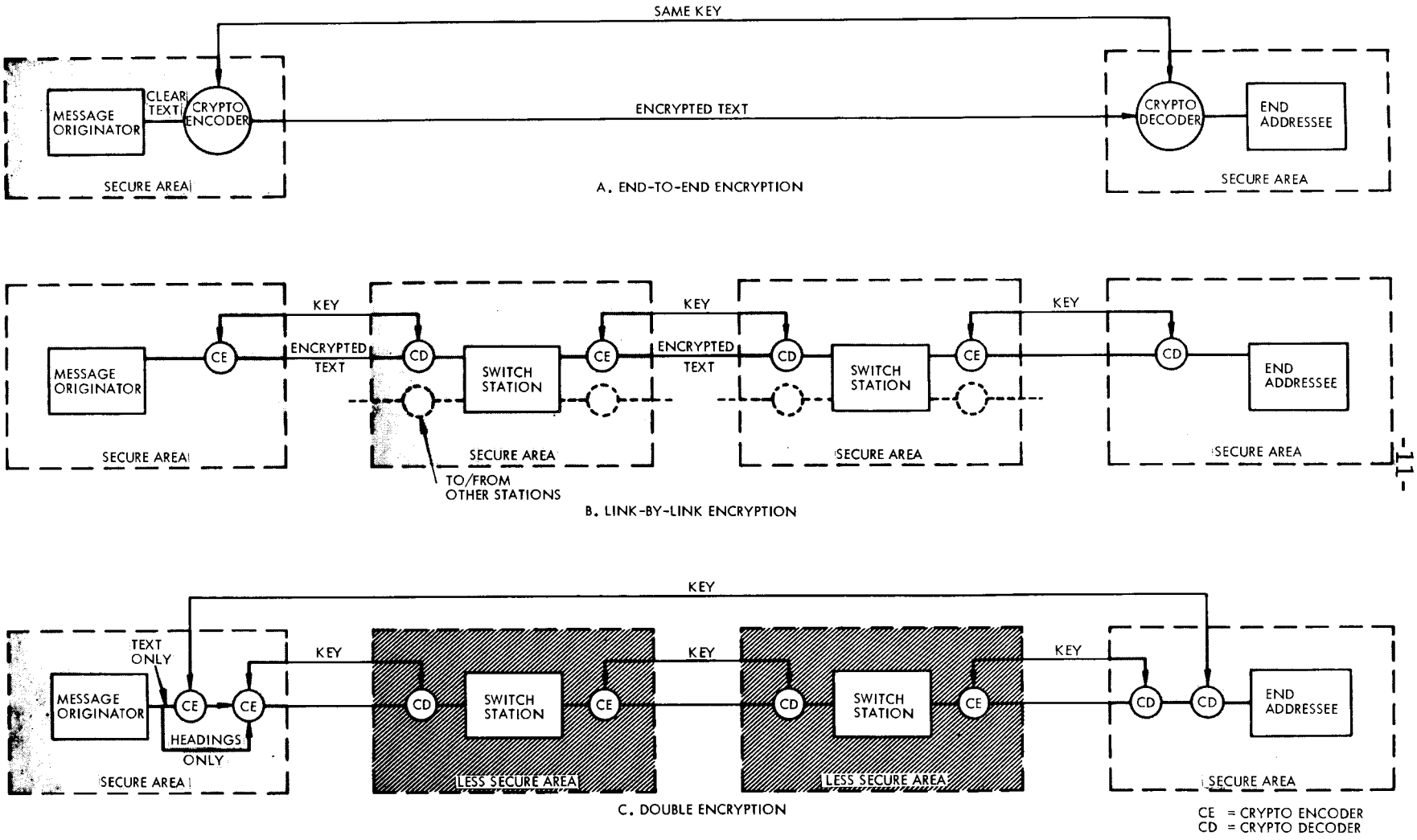
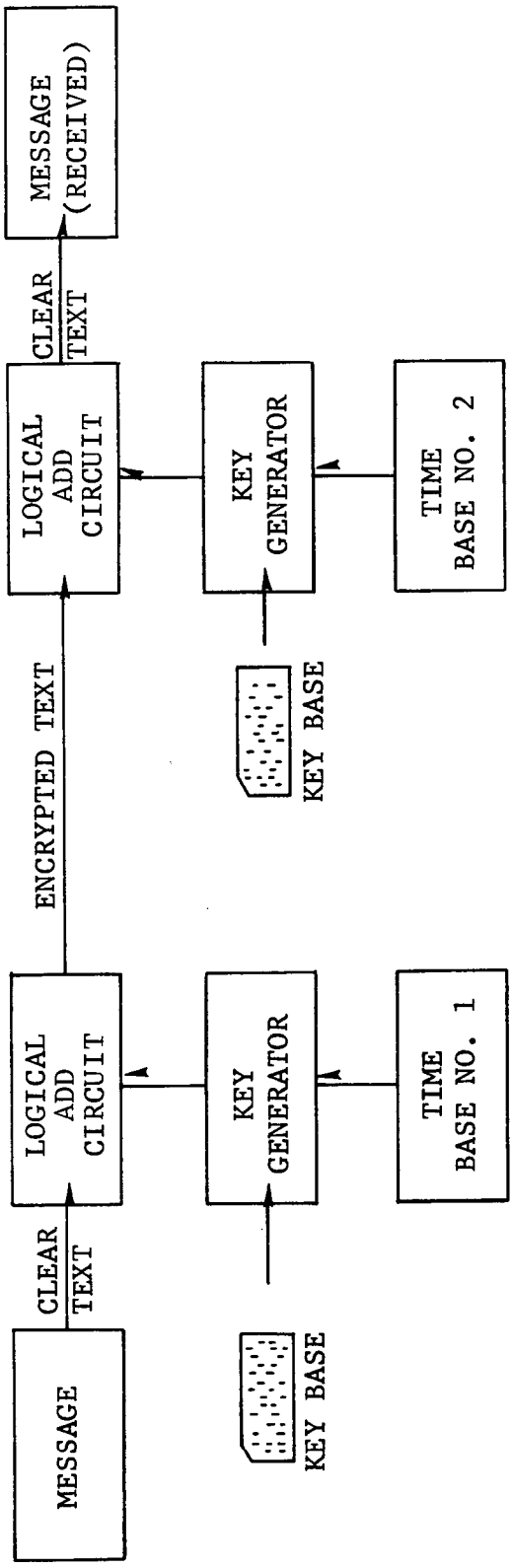


Fig. 1--Types of Encryption Systems



1 1 0 0	MESSAGE
1 0 1 0	KEY
0 1 1 0	INPUT

0 1 1 0	OUTPUT
1 0 1 0	KEY
1 1 0 0	MESSAGE

Fig. 2--The Crypto Proce

few important points to be kept in mind. First, the key generator is presumed to have statistical properties that make it appear as a totally-random digital noise generator. Secondly, in this scheme it is necessary that both key generators be fully synchronized, and that means be provided to cause the time base at the receiving end to coincide with the clock rate at the transmitter end. Third, the logical function combining text and key be such as to produce the same probability of transmitting a "1" for a "0" as for a "1". In Fig. 2, a "logical-add" circuit is used to perform the equal probability of transformation that allows reciprocal operation at the receiver. That is,

$$M \oplus K = E$$
$$E \oplus K = M$$

where M = the original message
K = the key
E = encrypted text
$\oplus$ = the logical-add transformation.

The truth table for the logical-add ($\oplus$) is shown at the bottom of Fig. 2. If the message bit is "0" and the key bit is "0", the output is "0"; if the message bit is "0" and the key is "1", the output is a "1"; if the message bit is a "1" and the key bit is "0", the output is "1"; etc. It can be seen, therefore, that the logical-add operation is perfectly reciprocal when the key is again added to the encrypted text. The message bits emerge in their original form. Other more complicated "operators" can be used in lieu of the logical-and circuit. (For example, see the Appendix.)

While it is theoretically possible to write an unbreakable cipher merely by using an infinite-length nonrepeating key, it would be necessary to have a copy of this

key at both the transmitting station and at the receiving station. At the high data rates being considered, this data storage requirement proves to be impractical. Therefore, the alternative of creating a long key from a relatively short key base has been chosen. It is possible to generate a long mathematical series or string of bits from a moderate-length key base. The length of the key should be chosen such that the series does not repeat or reveal periodicity before the time the key is changed. Thus, for example, a new key base can be inserted into the key generator daily and the receiving crypto system synchronized to match the time base at the transmitting station. The length of a series that can be generated by a set of digital elements cannot be greater than $N2^N$,* where N is equal to the number of flip-flops or storage elements used in the circuit creating the series. This means that extremely long sequences can be created that do not repeat, using a relatively small number of storage cells. For example, if N = 50, then $N2^N$ is equal to more than 50,000,000,000,000,000. Or, maximal sequences up to this length can be created. Not all such sequences would, however, be usable, because their statistical properties would reveal the construction of the generator function.

Link-by-Link Encryption

Link-by-link encryption, as shown in Fig. 1b, is used when there is not sufficient traffic to warrant a full-time cryptographically-secure circuit between two subscribers.

*Assuming that the sequence generator is exactly equivalent to a nonlinear shift register.

Thus, one key is used between the subscriber and his relay station, separate keys between each pair of relay stations. In such a system, there is an underlying assumption made that each switching center, together with its cryptographic equipment, is located in a secure area and only trustworthy, cleared personnel ever have access to the text which may be in the clear while passing through the switching center. Because of the different transmission time delays and the problems associated in providing a separate set of keys between each originator and every possible end addressee, it must be assumed that each switching center or station, together with its crypto equipment, is located in a secure area. Thus, messages generated in the clear are encrypted and sent to a switching center. Next, each message is decrypted, the address is used to set up the proper outgoing line connection, and the message is sent to the next station. The assumption of absolute security is not always a safe one to make in handling extremely sensitive information. Thus, it might be said that the chief limitation of link-by-link encryption is in the reduced security offered messages passing through several tandem switching centers. Traffic flowing throughout the entire network is openly readable by those inside any switching center--a highly undesirable possibility. Worse yet, as the complexity of the switching networks increases, the number of intermediate switching stations also increases. A point is reached where it becomes almost foolhardy to rely upon this technique alone for protection.

Double Encryption

Double encryption is a combination of end-to-end encryption for the text and link-by-link encryption for the message heading plus the encrypted text.

Figure 1c exemplifies double encryption. The first encryption operation is for text only, the second layer of

encryption is for both the text and the heading. Headings must be available in the clear at the switching center in order that the switching center have the necessary information to route traffic.

IV. IMPLICATIONS FOR THE DISTRIBUTED NETWORK SYSTEM

As it will be necessary to pass through very many switching centers in the proposed distributed network, the limitations of link-by-link encryption are strongly felt. A system with several hundred nodes, depending solely upon link-by-link encryption, would probably be considered inadequate except perhaps for the transmission of semiclassified data--data that would probably be sent in the clear today. Further, end-to-end encryption alone is also unsatisfactory, as the heading on each message block would be in the clear.

Thus, the distributed network shall use both link-by-link and end-to-end encryption. Rather than adding boxes to each switching center, the cipher encoder and decoder circuits shall be designed as an integral part of the Switching Nodes and Multiplexing Stations.

LINK-BY-LINK CRYPTOGRAPHY IN THE DISTRIBUTED NETWORK

The link-by-link crypto used in the distributed network is described in detail in ODC-VII.* Identical pseudo-random flip-flop chains exist at adjacent Switching Nodes. A logical operation combines the key and the text; timing is established from a piezoelectric clock. Each sequential Message Block contains a "Crypto Serial Number" in the clear derived from the time base.

Timing is established by shifting the local timing so that incoming Message Blocks arrive synchronized to the "start of Message Block" point of the local counter. Then, the difference between the Crypto Serial Numbers is measured by a digital subtraction and the local timing rate is increased or decreased accordingly. The process is repeated until the link has been pulled into synchronization.

*ODC is an abbreviation of the series title; the number following refers to the particular volume in the series.

Synchronization is automatic for link outages up to at least 12 hours duration.

It is anticipated that the key at each Switching Node will be changed on the order of once per week, or thereabouts. Storage for two alternatively assigned key phases is anticipated to eliminate the need for personnel to be at two or more Switching Nodes at the same time.

It should be emphasized that the link-by-link cryptography serves primarily to keep message headings secret from the eavesdropper.

During the periods in which no valid traffic is being transmitted, a "dummy" or filler stream of bits is sent, not only concealing traffic loading, but also for maintaining the timing synchronization. The dummy stream is created by an electronic noise generator tube feeding several stages of a pseudo-random counter.

The keys used for the link-by-link crypto are in the form of cards, statically read out.

While the crypto stream would be rather hard to "break," it will be seen that comparatively little damage will result should such an event occur.

END-TO-END CRYPTOGRAPHY IN THE DISTRIBUTED NETWORK

The end-to-end crypto built into the Multiplexing Station (see ODC-VIII) is more complicated than that used on the links between the Switching Nodes (and the links from the Multiplexing Station to the Switching Nodes). The added complexity is due to the fact that Multiplexing Station cryptography must permit any subscriber "to talk" to any other subscriber. As the number of potential subscribers is in the millions, the requirement for key storage can become overwhelming. Therefore, an alternative approach has been chosen of storing at each Multiplexing Station key bases only to other Multiplexing Stations.

Since we anticipate a maximum of 1024 Multiplexing Stations, only this number key bases need be stored at each Multiplexing Station. We will also assume that any pair of subscribers will desire connections to be kept open for periods ranging from a few seconds to a full day. Such connections, called "pseudo-circuits," are discussed in detail in ODC-VIII.

The first few Message Blocks in any "conversation" exchange housekeeping information necessary for rapid processing of subsequent Message Blocks. This interchange will require on the order of perhaps two seconds. Every time a new call is placed by a subscriber, the originating Multiplexing Station notes which Multiplexing Station is being called and increments its corresponding stored Serial Call Number for the called Multiplexing Station. This serial number is used by both Multiplexing Stations as a crypto start point for synchronization. Since each Multiplexing Station contains a powerful computing engine, and as one second is a long time in the life of a fast computer, sufficient time and capability exist for creating a new pseudo-random number for each new call with no apparent relationship to the key base used on previous calls. Thus, information concerning one call is of no use whatsoever in breaking subsequent calls. This is important in a system with widespread entry, and even allows civilian traffic to be combined with military traffic without weakening the secrecy protection offered.

Modification of the Derived Key Base

To this point, both Multiplexing Stations are synchronized and are using the same derived key bases. (Means are also included to handle errors and reset (advance only) the counters in the rare event of system malfunction. However, in no circumstance is the same derived key base ever

used for more than a single conversation call.) After the setup interval, Message Blocks will arrive at a very high rate. It is necessary to create a key from the derived key base at a very rapid rate, leaving very little time for processing. As this is a routine continuous operation, a "stamping mill" processor, with a portion of the Multiplexing Station equipment working full time on this operation, is utilized. The Multiplexing Station uses a drum or similar recirculating register to store the key bases, the derived keys, and the Message Blocks. Figure 3 shows the cryptographic processing of a drum operating on incoming encrypted text. The processing scheme used depends primarily upon a very low Message Block error rate at the Multiplexing Stations. Unfiltered errors and lost Message Blocks are expected to be such rare events, that we shall intentionally "knock down" a quasi-circuit if a single bad Message Block slips by the error-detection filters. (It should be understood that such a rigorous response to errors is infeasible in conventional transmission systems because of their relatively high error rates.)

Incoming encrypted text alternately fills one of the two assigned registers while the other register is simultaneously being read out and "logically-added" to the key base. The clear output text is then stored on one of two alternately assigned registers reserved for this purpose. Meanwhile, the clear text and the incoming text operate upon one another in a controlled manner to produce a new key base, based upon the previous key base used. This procedure may appear to be similar to the conventional "autokey"* procedure, but it should be noted that the next

*Shannon, Claude E., "Communications Theory of Secrecy Systems," Bell Systems Technical Journal, Vol. 28, No. 4, October 1949, p. 668.

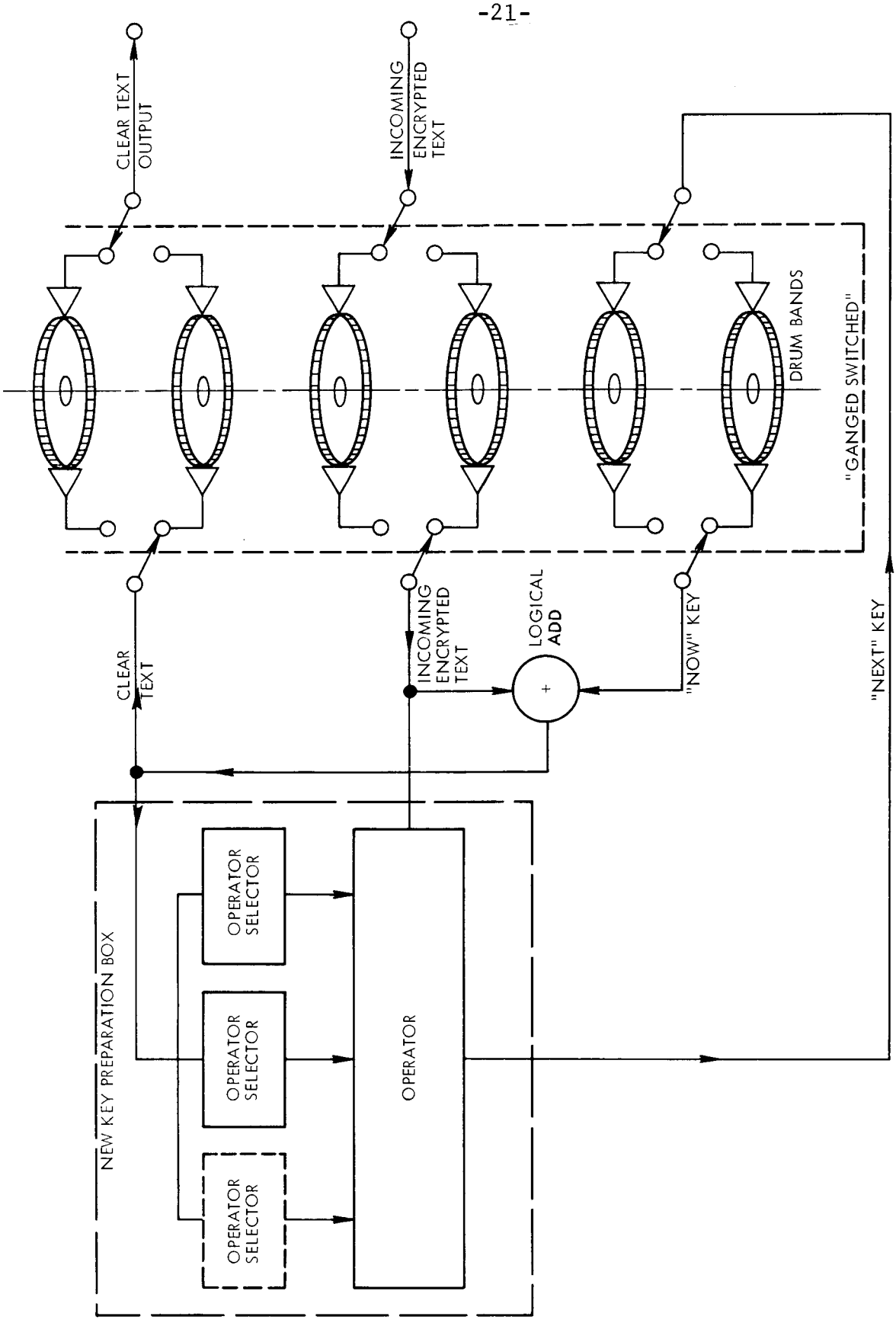


Fig. 3--Updating the Key at the Multiplexing Station

key is related to its previous one by a very complex and unknown mathematical operation. Even having the entire encrypted text and a sample of clear text will not facilitate ascertaining subsequent samples of clear text.

Thus, very high speed processing of Message Blocks with high cryptographic security for 1024 separate subscribers per Multiplexing Station does not appear particularly difficult to accomplish. All the equipment required for these operations is included in the parts breakdown in ODC-VIII.

It should be pointed out that the detailed implementation described may or may not be the precise method used. The present detailed description seeks only to point out that secure cryptographic processing at extremely high data rates appears technically possible. The actual choice, and detailed selection of the cryptographic operators, is left to the appropriate agency at the appropriate time.

Message Block Pre-Filtering Key

In order to prevent interruption of the sequence of Message Blocks arriving at the Multiplexing Station by false Message Blocks, means to detect and eliminate acceptance of "counterfeit" Message Blocks are included. Such false Message Blocks might conceivably be generated by a sophisticated enemy agent who has somehow managed to break the link-by-link crypto.

It will be recalled that the Message Block comprises 1024 bits, of which 128 are reserved for various housekeeping functions. Twenty of these housekeeping bit positions are set aside to act as a Pre-Filter Key.* Both the transmitting and receiving Multiplexing Stations generate

*Twenty bits are sufficient to detect better than 1,048,575 out of 1,048,576 random fraudulent Message Blocks.

these keys simultaneously. If, and only if, the incoming Pre-Filtering Key matches the next expected short Pre-Filtering Key, will the Message Block be accepted for further processing and the crypto key count be advanced. If any Message Block arrives that does not meet this test, it is transmitted to the human intercept position at the receiving Multiplexing Station for intervention checking.

GENEALOGY OF THE KEYS

A hierarchical development is being employed to create a very long key from a relatively short key base and caution must be exercised. If too long a sequence is generated from a single key base, it might be possible to deduce other keys derived from the same base. Therefore, let us examine the sequence lengths required by this system to insure that they are very much shorter than would reveal the nature of the generator function.

1) Number of Multiplexing Stations 1,024
2) Number of new subscriber-to-subscriber calls per key-change period between the i'th and the j'th Multiplexing Station 100,000*
3) Maximum length of time between key changes ..... 48 hr
4) Maximum length of time for connection of a "quasi-circuit" ..... 24 hr
5) Acceptable probability of breaking and entering a Switching Node, analyzing Message Block headings, and spending full time on a single link attempting to interrupt a single call in progress by creating false Message Blocks ..... $< 10^{-6}$
6) Average time between potential interruptions (= 2/3 ms per Message Block x 10^6) ..... > 10 min

*However, the design is based on 1,000,000+.

7) Maximum number of Message Blocks exchanged between any two subscribers on any single call 1,960,000*

If the active part of the crypto key base used per call is 866 bits, then the longest generated sequence can be as great as 2^{866}, or about 10^{300}.**

GENERATION AND DISTRIBUTION OF KEYS

A constant supply of key bases is required to keep the distributed network system operating. One possible plan is shown in Fig. 4, in which two major key preparation stations are depicted, one in the East and one in the West. Each such station contains a large general-purpose computer with about six tape units. Separately written, highly complex, random number generating programs are used by each key preparation site. Choice parameters which modify the random number generator are inserted by three individuals at each site working independently. Conventional one-inch magnetic computer tapes, recorded at high speed, are played back into a ¼" tape duplicator for preparation of the 300-ft spools of ¼" tape used in the Multiplexing Stations. The one-inch computer tape outputs are also used to drive an off-line card punch to prepare the shorter set of key bases used by the Switching Nodes. The output of each of the two sites' tapes and card duplicating facilities are stored in about twenty geographically distributed sites.

The Switching Node and Multiplexing Station keys are comprised of two parts, one coming from the distribution

---

*The highest normally expected data rate per subscriber is:

(19,600 bits/sec)(3600 sec/hr)(24 hr)

= 1.693×10^9 bits per key change

= 1.824×10^6 Message Blocks.

**For comparison, recall that there are only about 10^{80} electrons in the universe.

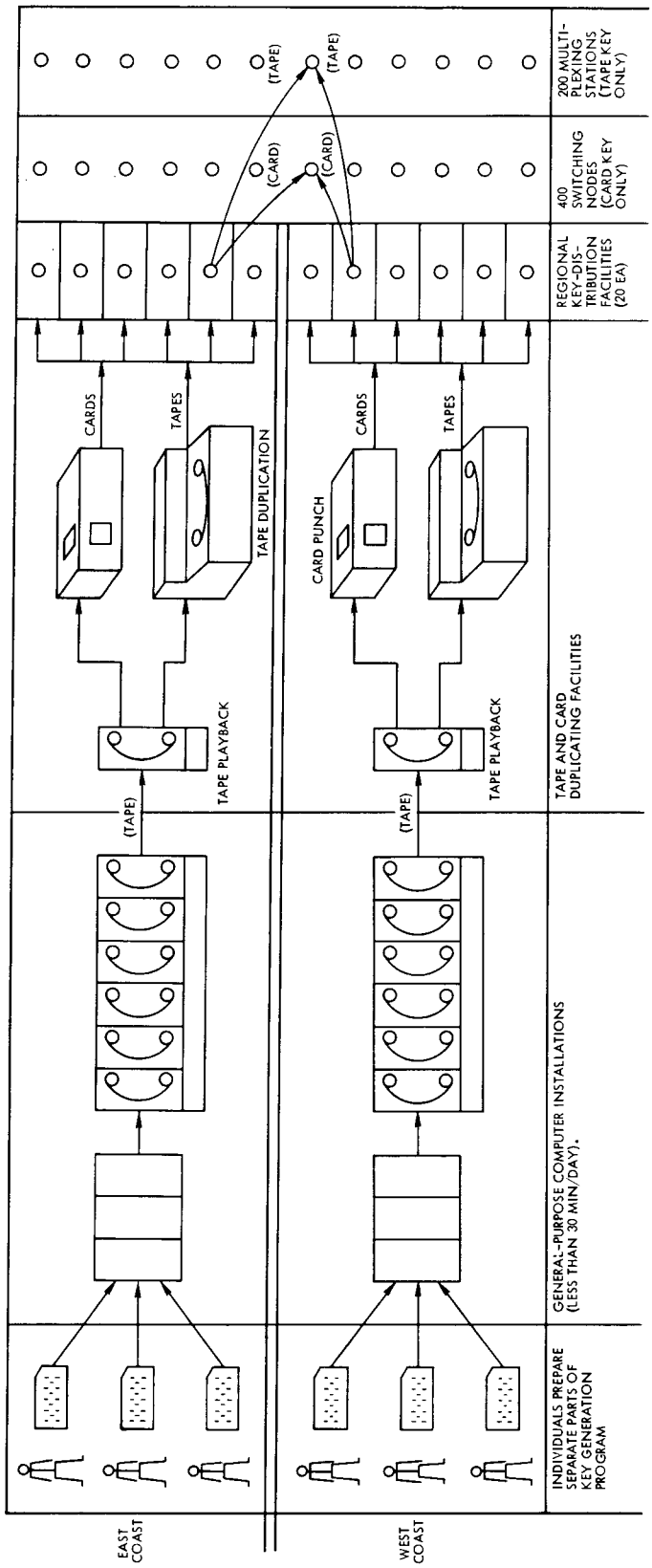


Fig. 4--One Method of Preparing and Distributing Key Bases

site prepared by the East unit, and the other part coming from the West unit via different distribution sites. Each member of a two-man team has mechanical key access to only his own part of the key base. Thus, the system is relatively secure from a single enemy agent having access to an entire key base for any unit.

In the next section it will be shown that even if an enemy were, somehow, able to gain access to the full key, he would still probably not be able to reconstruct traffic.

PROTECTION OFFERED BY SEMI-RANDOM PATH CHOICE

In the distributed network, each Message Block usually travels by a path distinctly different than that taken by the previous Block. Path selection is determined on a Switching-Node-by-Switching-Node basis. Each Switching Node chooses the "best" path for each Message Block. If the "best" locally connected link is busy or inoperative, the next best link is used; the heavier the network loading, the more circuitous and varied are the paths taken.

It will be recalled that it is impossible to decrypt a stream of Message Blocks unless all preceding Message Blocks have been correctly received. An eavesdropper, even one equipped with both the link-by-link and the end-to-end keys, cannot decipher any "quasi-channel" or stream of Message Blocks unless he has correctly received all previous Message Blocks. Thus, unless the interceptor records all outgoing links from the Switching Node for a single Multiplexing Station and has all keys, he will not be able to decrypt the sequence of Message Blocks.

It will also be recalled that the links used in the system can have a rather poor unfiltered error rate--one error per 1000 Message Blocks.* The filtered error rate is extremely low--some five orders of magnitude or so

*See ODC-VI for link error rate determination.

better. This, however, is obtained only by the use of an automatic error detection facility and allowance being made for requests for repeat transmissions. An eavesdropper, even one equipped with all keys, cannot very well ask for repeat transmissions. Thus, he is at a decided disadvantage in deciphering the stream of Message Blocks, because his streams will contain errors.

Further, devices able to record 1.5 million bits per second with an adequately low error rate are on the fringe of 1963 state-of-the-art. Lastly, it will be remembered that all silence periods in voice transmissions greater than about 1/20 sec will be suppressed, making the determination of the sequence of Message Blocks extremely difficult and time consuming (see ODC-VIII).

V. A "DEVIL'S ADVOCATE" EXAMINATION

The secrecy provisions for the distributed network system are not being described in full and complete detail in this Memorandum. For example, some preliminary thinking about methods of extending the zone of full secrecy to individual subscribers remote from the Multiplexing Station has been omitted. One reason for such omissions is the fact that the basics of the problem are still being examined.

A key rationale for writing this Memorandum has been to fulfill the need for a working paper which would impart to the reader a feeling for the detailed secrecy measures necessary in the proposed system and to aid in a subsequent "devil's advocate" examination of the system as a whole. The proposed network must successfully operate in a hostile environment, and therefore the system design should be made always keeping in mind potential system weaknesses. We are concerned lest a clever and determined enemy find in it an Achilles heel. As an acid test, we elicit and encourage a response from the reader who will "don the hat of an enemy agent" and try to discover weak spots in the proposed implementation. Such an enemy is assumed to have a limited number of highly competent cohorts plus all the equipment he can transport. Further, it is assumed that the fundamental human inadequacies of our, or any security clearance system will permit infiltration by some at least minimal number of enemy agents who will gain a complete and detailed understanding of the workings of the system.

Inasmuch as few people have ready access to the crypto keys and since the keys are changed on a short-time basis, it can be assumed that the subversive agent will generally not have access to more than a portion of the key--unless

he resorts to force in obtaining the key, thereby tipping his hat.

As more and more about the limitations of the proposed implementation is learned, we plan to add more and more safeguards to complicate the task of the enemy agent, until a point is reached where we can safely say, "It is now unreasonably difficult for an enemy, or a friend, to interfere with the operation of this network."

The rationale for a limitation on the number of cooperating agents in the pay of an enemy lies in the high probability that any locally recruited agent will be, in fact, a double agent. Hence, the number of agents who know of any proposed operation must be limited for fear of revealing the attack plan.

APPENDIX

USE OF A FUNCTION OF N-BOOLEAN VARIABLES AS A SECOND-ORDER MODIFIER FOR "NEXT-KEY" GENERATION

In the foregoing text, little was said about the types and the range of operations possible in modifying the key in the end-to-end auto-key subsystem. This Appendix lends some insight into the added complexity of analysis that can be created for the eavesdropper by simply varying the logical addition operator.

In Fig. 5 three drum bands, each containing 866 bits, are shown. The first band contains the key used to decrypt the last Message Block; the second drum band stores text in the clear that has been derived by use of the old key; and the third drum band stores a new key computed by a "black box," labeled "Z".

A, B, and C, could, for example, represent three magnetic heads on the Multiplexing Station drum, 16 bits apart. Similarly, D, E, and F, would represent a second set of three heads. The box, Z, contains Boolean logic which performs "some" operational function upon the old key for the sake of increasing complexity. Consider the six separate heads to form six separate inputs. We ask, "How many different ways can six inputs be logically organized to form separate and distinct output functions?"

Any Boolean function can be expressed as the logical addition of a series of "min-terms."* Each min-term is a logical product of each of the fundamental inputs or its logical complement. Any logical function can be expressed as a series of points on a Veitch Diagram (see Fig. 6).

---

*See: Ware, W. H., Digital Computer Technology and Design, Vol. I, Wiley, New York, 1963, pp. 4.13-4.16.

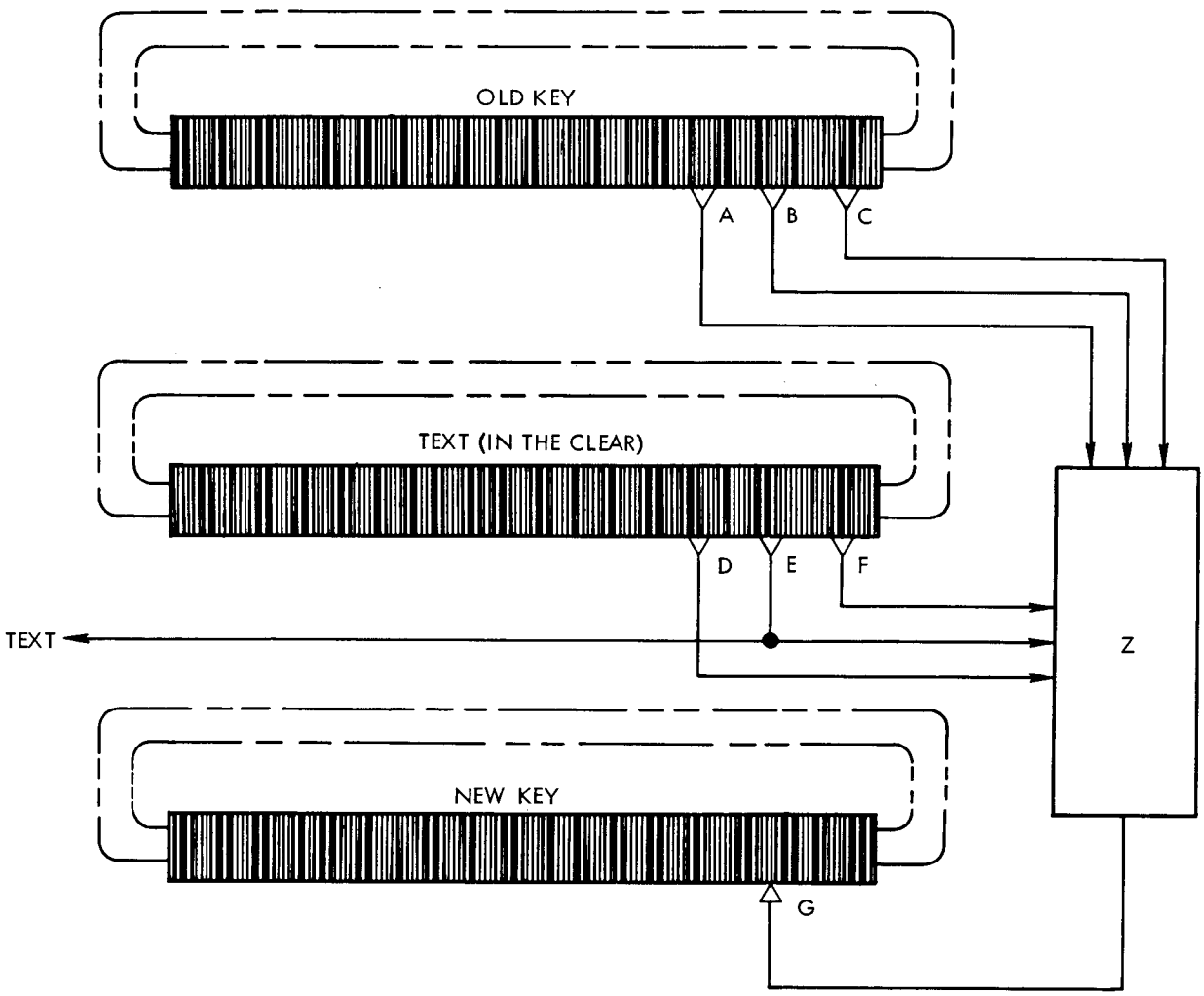


Fig. 5--The Generation of a New Key Using a Function of N-Boolean Variables as a Transformation Operator

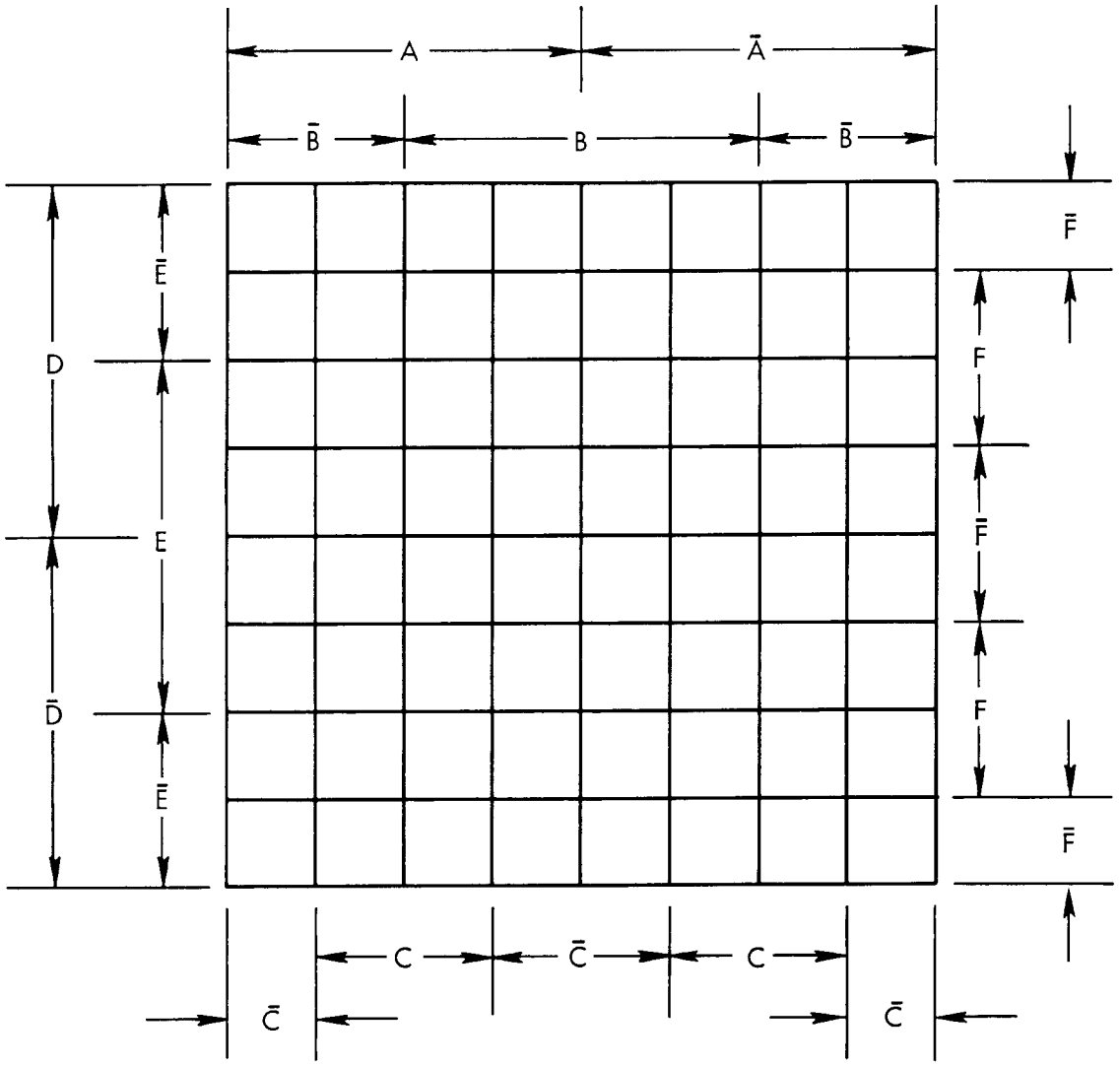


Fig. 6--64 Possible Minterms for Six Boolean Variables

Thus, we can have

$$2^{2^N} = 2^{64} \simeq 10^{64/3.2} \simeq 10^{20}, \text{ or}$$

$$\sim 100,000,000,000,000,000,000$$

allowable combinations for only six variables. This number almost "explodes" when the number of variables is raised. For example, let N equal the number of variables and compute the number of separate logical functions possible:

N	2^N	2^{2^N}	Number of Functions, Decimal Value
6	64	2^{64}	$\sim 10^{20}$
7	128	2^{128}	$\sim 10^{40}$
8	256	2^{256}	$\sim 10^{60}$
9	512	2^{512}	$\sim 10^{80}$
10	1056	2^{1056}	$\sim 10^{100}$

As any single one of the six input min-terms can be implemented with only six diodes, and as all combinations of min-terms can be implemented with 64 or fewer min-terms, it follows that <u>every</u> complicated function possible can be implemented with two-level logic, requiring 384 diodes (six diodes per min-term, times 64 diodes for all min-terms), for any of the $\sim 10^{20}$ functions possible for six variables.

Of course, rather complex logic circuitry is required for many of these combinations, but many of the functions

can be created with only a small portion of the full complement of 384 diodes.

Thus, it is seen that rather simple straightforward techniques can be used at this point to add another layer of complexity, further compounding the problems of the would-be eavesdropper.

ON DISTRIBUTED COMMUNICATIONS:

List of Publications in the Series

I. Introduction to Distributed Communications Networks, Paul Baran, RM-3420-PR.

Introduces the system concept and outlines the requirements for and design considerations of the distributed digital data communications network. Considers especially the use of redundancy as a means of withstanding heavy enemy attacks. A general understanding of the proposal may be obtained by reading this volume and Vol. XI.

II. Digital Simulation of Hot-Potato Routing in a Broadband Distributed Communications Network, Sharla P. Boehm and Paul Baran, RM-3103-PR.

Describes a computer simulation of the message routing scheme proposed. The basic routing doctrine permitted a network to suffer a large number of breaks, then reconstitute itself by rapidly relearning to make best use of the surviving links.

III. Determination of Path-Lengths in a Distributed Network, J. W. Smith, RM-3578-PR.

Continues model simulation reported in Vol. II. The program was rewritten in a more powerful computer language allowing examination of larger networks. Modification of the routing doctrine by intermittently reducing the input data rate of local traffic reduced to a low level the number of message blocks taking excessively long paths. The level was so low that a deterministic equation was required in lieu of Monte Carlo to examine the now rare event of a long message block path. The results of both the simulation and the equation agreed in the area of overlapping validity.

IV. Priority, Precedence, and Overload, Paul Baran, RM-3638-PR.

The creation of dynamic or flexible priority and precedence structures within a communication system handling a mixture of traffic with different data rate, urgency, and importance levels is discussed. The goal chosen is optimum utilization of the communications resource within a seriously degraded and overloaded network.

V. History, Alternative Approaches, and Comparisons, Paul Baran, RM-3097-PR.

A background paper acknowledging the efforts of people in many fields working toward the development of large communications systems where system reliability and survivability are mandatory. A consideration of terminology is designed to acquaint the reader with the diverse, sometimes conflicting, definitions used. The evolution of the distributed network is traced, and a number of earlier hardware proposals are outlined.

VI. Mini-Cost Microwave, Paul Baran, RM-3762-PR.

The technical feasibility of constructing an extremely low-cost, all-digital, X- or K_u-band microwave relay system, operating at a multimegabit per second data rate, is examined. The use of newly developed varactor multipliers permits the design of a miniature, all-solid-state microwave repeater powered by a thermoelectric converter burning L-P fuel.

VII. Tentative Engineering Specifications and Preliminary Design for a High-Data-Rate Distributed Network Switching Node, Paul Baran, RM-3763-PR.

High-speed, or "hot-potato," store-and-forward message block relaying forms the heart of the proposed information transmission system. The Switching Nodes are the units in which the complex processing takes place. The node is described in sufficient engineering detail to estimate the components required. Timing calculations, together with a projected implementation

scheme, provide a strong foundation for the belief that the construction and use of the node is practical.

VIII. The Multiplexing Station, Paul Baran, RM-3764-PR.

A description of the Multiplexing Stations which connect subscribers to the Switching Nodes. The presentation is in engineering detail, demonstrating how the network will simultaneously process traffic from up to 1024 separate users sending a mixture of start-stop teletypewriter, digital voice, and other synchronous signals at various rates.

IX. Security, Secrecy, and Tamper-Free Considerations, Paul Baran, RM-3765-PR.

Considers the security aspects of a system of the type proposed, in which secrecy is of paramount importance. Describes the safeguards to be built into the network, and evaluates the premise that the existence of "spies" within the supposedly secure system must be anticipated. Security provisions are based on the belief that protection is best obtained by raising the "price" of espied information to a level which becomes excessive. The treatment of the subject is itself unclassified.

X. Cost Estimate, Paul Baran, RM-3766-PR.

A detailed cost estimate for the entire proposed system, based on an arbitrary network configuration of 400 Switching Nodes, servicing 100,000 simultaneous users via 200 Multiplexing Stations. Assuming a usable life of ten years, all costs, including operating costs, are estimated at about $60,000,000 per year.

XI. Summary Overview, Paul Baran, RM-3767-PR.

Summarizes the system proposal, highlighting the more important features. Considers the particular advantages of the distributed network, and comments on disadvantages. An outline is given of the manner in which future research aimed at an actual implementation of the network might be conducted. Together with the introductory volume, it provides a general description of the entire system concept.