

~~SECRET~~

CRYPTOGRAPHIC EQUIPMENT FOR EITHER
SINGLE-ORIGINATOR OR MULTI-ORIGINATOR COMMUNICATION

1. a. Progress in the cryptologic field during the past few years has led to a basic change in cryptologic philosophy, a change which has already been recognized by and is of important interest to the ASA.

b. The trust which has heretofore been placed in the ordinary types of crypto-systems, the solution of which depends upon, or is directly or indirectly correlated with, the number of tests that have to be made to exhaust a multiplicity of hypotheses based upon keying possibilities, is daily decreasing. The beginning of this decreasing confidence in the degree of cryptographic security potentially offered by a vast number of permutations and combinations available of keying possibilities can be traced back to the advent of the application of tabulating machinery to the solution of cryptanalytic problems. Later, when specially designed cryptanalytic machines employing electrical relays came to be constructed and applied successfully to these problems, a real blow was struck at our former concepts of cryptographic security. And, now, the assurance that electronic cryptanalytic machinery can be applied to speed up the solution of complex cryptographic systems is tending slowly to undermine what faith was left in the systems or crypto-mechanisms currently considered as being the best there are, those using rotors with complicated stepping controls.

c. To sum this up, it can be said that, save for one exception, cryptologic theory and practice during the past quarter of a century serves only to corroborate the theoretical validity of the century-old dictum first enunciated by Edgar Allan Poe: "Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot solve."

2. The foregoing summation is, as noted, theoretical and pessimistic in outlook. From a practical viewpoint, it can be stated that, so far as concerns the currently-employed high-echelon cryptographic systems of the U.S. Army, there is every reason to believe that, despite the recent advances in cryptanalytic techniques and machinery, these systems are still quite secure. But for how many more years this may continue to be true is a matter of serious concern. The lead which our cryptographic techniques presently have over our cryptanalytic techniques is not sufficiently great to leave no room at all for speculation or apprehension as to the situation in which we might find ourselves, say 15 or 20 years from now, when the new cryptographic machines under development will have

Declassified by NSA/CSS

Deputy Associate Director for Policy and Records

On 20121119 by RM/RECORDS COPY 1

DO NOT DESTROY OR MUTILATE

~~SECRET~~Do NOT Destroy Return to the
NSA Technical Library when no longer needed

27,886 TC Copy No. 1

~~SECRET~~

been completed. It is hardly necessary to note that the Research Laboratories Division is endeavoring to anticipate what the future may hold in store and is bending all its efforts to produce improved crypto-equipment that will be secure against a greatly advanced cryptanalytic art. Basically, these efforts are in the direction of increased sophistication and complexity in the present types of equipment, on the theory that this will always keep our cryptography in the lead of our cryptanalysis. But what if it should happen that because of unforeseen developments, in electronics and related fields, progress in cryptanalytic techniques and machinery has actually been greater than that in cryptographic techniques and machinery? National security demands that we take all measures necessary to guard against such a contingency.

3. The sole exception alluded to in Par. 1c above, in connection with Poe's dictum, appears to be involved in the case of what may be called a "holocryptic" system, that is, one which is theoretically absolutely unsolvable because a message in it can be read only by actual physical possession of the key. In a truly holocryptic system, if the key consists of a perfectly random, unpredictable sequence of all the elements (letters or characters) of the language, the sequence being as long as the enciphered text itself and being a primary sequence (that is, one not derived from the interaction of a limited number of basic components), the cryptogram appears to be unsolvable in the cryptanalytic sense. It appears to be impossible to present or to develop any practical technique for the solution of a truly holocryptic system as defined herein.¹ It is to be noted that in the three foregoing sentences the phrase "appears to be" is used. It is employed advisedly, for it would be somewhat dangerous to insist upon a categorical statement in the absence of experimentation to demonstrate the positive validity of the statements made. It is indeed possible to conceive a theoretical general solution for certain of the so-called holocryptic systems, but no further remarks will be made in this paper on that phase of the subject, except to indicate the necessity for further study.

4. a. It is to be noted that there are three conditions which a cryptographic system must fulfill before it can be termed a truly holocryptic system: (1) the key must consist of all the characters found in the plain text of the language involved; (2) the keying characters must form a perfectly, or at least an entirely unpredictable, random sequence, so that it

¹Even were telepathy established as a practical reality, the reading of a cryptogram by this means would not constitute a cryptanalytic solution.

~~SECRET~~

must be a primary sequence, not a secondary one derived from the interaction of a limited number of basic elements; and (3) the keying sequence must be used once and only once. In our best rotor-type cipher machines the first of these conditions is fulfilled; the third is fulfilled to a degree which, for all practical purposes, is quite satisfactory; but as regards the second condition, it is obvious that although the keying characters in SIGABA, for example, form an unpredictable sequence, for all practical purposes in the present state of the cryptanalytic art, it is not a primary sequence and therefore the SIGABA or any similar machine presently falls short of competing with the truly holocryptic system in security. As time goes on, it is possible that the competition will not lessen in favor of SIGABA or its successors. This point is worth some elaboration.

b. It may be stated, in view of what is now practicable and of what may become practicable in the near future, that, at least theoretically, whatsoever be the nature or construction of a crypto-mechanism, if it embodies within it all the crypto-elements of the system, messages prepared by it can and will ultimately be solved. Only when the crypto-mechanism is controlled by some external keying means does it present truly holocryptic features--and then only if that external keying means is properly designed and employed. Even if an internally-controlled crypto-mechanism is employed in a manner such that the internally-produced keying sequence is employed only once, as in SIGHUAD for example, the system is still theoretically solvable because that keying sequence is produced by the interaction of a limited number of primary keying elements, that number being very small in comparison with the length of the secondary or resultant keys. Therefore it cannot in the present state of the art be considered as falling in the class of holocryptic systems and must be considered to be theoretically solvable. How soon it may become practically solvable is a question that will be answerable only with the passage of a few more years. *

5. From a practical viewpoint, it may be assumed that messages in a holocryptic system will never be solvable, no matter what the state of the cryptanalytic art may be. It would therefore be wise to extend the usage of such systems. Unfortunately, the last two conditions which must be fulfilled in a truly holocryptic system impose practical limitations on the extensive employment of such systems in military communication. The large volume of communication required and the large number of commands which must intercommunicate make it wholly impracticable to prepare and to distribute

the multitude of lengthy primary sequences that would be required. Moreover, the keying sequences can only be used once. If used more than once, even only two times in most cases, such a system is quite insecure.

6. It is usual to refer to a system using a pad of sheets of paper on which keying characters appear as a "one-time pad system", and systems using perforated tapes, such as the SIGTOT, as a "one-time tape system". For the system using the SIGABA or similar equipment there is no analogous designation based upon the number of times a key is used, though supposedly such a system could be referred to as a "many-time system"--a designation technically too loose and inaccurate for the purposes of this paper. The real essence of the matter is that, in the case of a one-time pad or one-time tape system, practical, almost-absolutely-sure intercommunication is assured only when there are but two copies of a pad or tape, one held by the originator of a message, the other by the addressee; and furthermore, an originator must not use as the keying sequence for any of his outgoing messages a sequence intended to decipher any of his incoming messages. So far as concerns the ability to originate messages that will be absolutely secure, therefore, a true one-time system must be limited in its distribution to one originator; for this reason such a system will hereinafter be referred to as a "one-originator system". A system such as the one employing SIGABA, for example, will be referred to as a "multi-originator system", because many holders of the equipment can originate secure messages and thus intercommunication among many holders can be provided.

7. a. The question arises: would it be possible, practical, and advantageous to have crypto-equipment which will, in the same basic machine, provide for truly holocryptic, one-originator systems as well as for high-security, multi-originator systems? In other words, what about a single machine which for the greatest part would be used for multi-originator communication but which could, when special circumstances dictated, serve also for single-originator communication?

b. The possibility that such a machine can be devised has already been demonstrated in at least two cases. The first is to be noted in the case of the obsolete Converter M-134A, wherein the angular displacements of the rotors of a 5-rotor crypto-maze were controlled by perforated tapes. Multi-originator communication was provided for by issuing the tapes in sets of 48 and using them according to the variations indicated in a key list. To employ such a machine by the use of individual tapes according to the single-originator system is obviously possible, though it was actually not done when

~~SECRET~~

Converter M-134A was in current usage. The second example is to be noted in the case of SIGSALY, wherein holocryptic, single-originator communication was provided for by the use of SIGRUVE records and high-security, multi-originator communication was provided for by the so-called Busch machine. The latter was hardly ever used, however, for various reasons, mostly because of mechanical or electrical difficulties, not for security reasons.

c. There seems to be little question of the practicability of the idea of a single machine capable of serving both functions. If the basic equipment is designed to incorporate the idea, and is in itself practicable, there should be no problem about providing for the dual function by means of suitable adapters or cooperating components. For example, in the case of SIGABA, it is perhaps possible to provide a "basket" or crypto-component in which the control and index rotors are replaced by a tape transmitter through which could be passed a 1-time tape. With the normal component (present SIGIVI), the availability of SIGABA for multi-originator communication would remain intact; yet, when occasion demanded the assurance of absolute security, this could also be furnished by the special component replacing the SIGIVI.

d. As to the advantages and disadvantages of the proposal, there is no doubt that it would complicate matters to a certain extent, but the advantage of having a single machine capable of performing the dual function and of affording not only highly secure multi-originator communications but also nearly-absolutely-secure single-originator communication is obvious. Even now there would be a practical usage for such a machine. Recent cases wherein question has been raised with regard to the security of specific messages demonstrate the point. "Eyes Only" messages also demand special treatment. But of greater significance is the importance of having such a machine with which to face the future. For, should it turn out that 15 or 20 years from now the actual progress in cryptanalytic techniques and machinery approximates or surpasses the expected progress, we should not be caught unprepared. Our security equipment could still meet the needs of security to a better degree than would be the case if we proceed on the assumption that our cryptography can always be advanced, by increasing sophistication and complexity of construction, to be sufficiently in the lead of our cryptanalysis to permit our confidence in the security of our equipment to remain undisturbed. In short, the proposal here made is in the nature of an insurance policy against unforeseen contingencies--we ought not to allow ourselves to be caught in an unfavorable communication security position because of wholly unexpected developments or much more rapid improvement in our signal intelligence position.

~~SECRET~~

8. It has been suggested that as an alternative to the development of adapter-type components in equipment designed to be capable of performing the dual function outlined herein, it would be possible to issue special key-lists and use a specific keying arrangement once and only once; this being nearly equivalent to the truly holocryptic single-originator system under discussion. There is no doubt that such a scheme would give added security, but it does not meet quite squarely the issue presented herein. The point has been touched upon in Par. 4b and the argument therein presented is equally applicable here.

9. If the principle or proposal advanced herein has merit, it could be adopted as a general policy to incorporate it wherever possible and practicable.

10. It is recommended that:

a. The proposal suggested herein, viz., that future development of security equipment be so directed as to incorporate features or components which will alternatively permit of single-originator and of multi-originator communications by the same basic machine, be studied to ascertain its merits.

b. If the proposal is found to possess advantages important enough to outweigh its disadvantages, it be considered for adoption as a general policy.

c. Consideration be given to the proposal in connection with the current revision of SIGIRA.

d. Some research and study be given to the question of holocryptic systems to ascertain what might be accomplished by the use of new machinery now only dimly conceived but perhaps possible of being constructed.

e. Further research and study be devoted to a careful examination of the nature of our present mechanisms for the generation of our 1-time keys and of the nature of the cipher alphabets employed in connection therewith for the encipherment of classified communications.

William F. Friedman
WILLIAM F. FRIEDMAN
Chief, Communications Research
2 May 1947

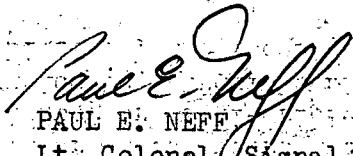
MUST REMAIN WITH ATTACHED PAPERS

NUMBER EACH MEMO OR REPLY IN LEFT BORDER, PLACE NAME, RANK AND TELEPHONE NUMBER BOTTOM OF EACH ACTION. DRAW LINE UNDER EACH ACTION

ENTER FILE CLASSIFICATION ADJUTANT _____

TO	FROM	DATE	SUBJECT
AS-20	AS-14	2 May 47	<p>Cryptographic Equipment for Either Single-Originator or Multi-Originator Communication</p> <p>1. The attached paper is submitted at this time in connection with the current revision of SIGIRA.</p> <p>2. The substance of the paper is to recommend that serious consideration be given to an extension of the potential usage of 1-time systems by providing adapters for use in connection with (a) current crypto-mechanisms now generally operating only as "multiple-communication" equipment or (b) similar mechanisms now in the research and development phase.</p> <p style="text-align: right;"><i>William F. Friedman</i> WILLIAM F. FRIEDMAN Chief, Communications Research Ext 215</p> <p>1 Incl Paper on Cryptographic Equip. for Either Single-Originator or Multi-Originator Comm.</p>
2. AS-14	AS-23	21 Jul 47	<p style="text-align: right;">Major Moak/462</p> <p>1. The inclosed paper on Cryptographic Equipment for Either Single-Originator or Multi-Originator Communication has been studied by Operations Division, Research Laboratories Division, and Security Division.</p> <p>2. With reference to the recommendations contained in paragraph 10 of the inclosure, the following comments are made:</p> <p>a. It is recognized that holocryptic systems provide the only theoretically unsolvable systems. At the present time, however, the employment of holocryptic principles is accompanied by a number of serious operational as well as production and distribution problems. Further, in the case of low echelon cryptomechanisms, a requirement for the provision of infinite security has not been established. In the case of high echelon cryptomechanisms, it is agreed that, whenever practicable, holocryptic principles should be embodied in multi-originator mechanisms.</p> <p>b. In the present work on SIGIRA, account is being taken of a basic military requirement for a one-time mechanism to fulfill the need for holocryptic systems where required. In this connection, the question arises as to whether, at the present stage of development, it might be better to achieve speed and</p> <p>Declassified by NSA/CSS</p> <p>Deputy Associate Director for Policy and Records</p>

On 20121119 by REM

TO	FROM	DATE	SUBJECT
AS-14	AS-23	21 Jul 47	<p style="text-align: center;">SECRET REF ID: A4127221 Cryptographic Equipment for Either Single- Originator or Multi-Originator Communication</p> <p>light weight in such a device, issuing it to all holders for emergency use, rather than to burden machines designed primarily for multi-originator use. Settlement of this question must obviously await a more advanced stage in the development of cryptographic devices now under consideration.</p> <p>c. Improvements in the methods of generating perfectly random, unpredictable key for use in connection with holocryptic systems are now under study by Security Division.</p> <p>3. In view of the above, research in the development of all cryptographic devices should include consideration of holocryptic principles in the provision of dual single-originator - multi-originator equipment. In this connection it is desired that the Chief, Communications Research Section continue to pursue this matter and insure, through coordination with the various operating divisions, that continuing consideration is given the recommendations contained in the inclosed paper.</p> <p style="text-align: right;">  PAUL E. NEFF Lt. Colonel, Signal Corps Acting Deputy Chief Army Security Agency Ext 498 </p> <p style="text-align: center;">SECRET</p>
1 Incl n/c			

~~SECRET~~

2. AS-14 AS-23 21 Jul 47

Major Moak/462

1. The inclosed paper on Cryptographic Equipment for Either Single-Originator or Multi-Originator Communication has been studied by Operations Division, Research Laboratories Division, and Security Division.

2. With reference to the recommendations contained in paragraph 10 of the inclosure, the following comments are made:

a. It is recognized that holocryptic systems provide the only theoretically unsolvable systems. At the present time, however, the employment of holocryptic principles is accompanied by a number of serious operational as well as production and distribution problems. Further, in the case of low echelon cryptomechanisms, a requirement for the provision of infinite security has not been established. In the case of high echelon cryptomechanisms, it is agreed that, whenever practicable, holocryptic principles should be embodied in multi-originator mechanisms.

b. In the present work on SIGIRA, account is being taken of a basic military requirement for a one-time mechanism to fulfill the need for holocryptic systems where required. In this connection, the question arises as to whether, at the present stage of development, it might be better to achieve speed and

VERNA SECURIBILA VERENCA

MENDOSYSLEMS

~~SECRET~~

~~SECRET~~

REF ID: A4127221

Cryptographic Equipment for Either Single-
Originator or Multi-Originator Communication

AS-14 AS-23 21 Jul 47

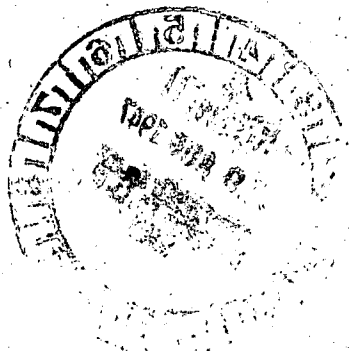
light weight in such a device, issuing it to all holders for emergency use, rather than to burden machines designed primarily for multi-originator use. Settlement of this question must obviously await a more advanced stage in the development of cryptographic devices now under consideration.

c. Improvements in the methods of generating perfectly random, unpredictable key for use in connection with holocryptic systems are now under study by Security Division.

3. In view of the above, research in the development of all cryptographic devices should include consideration of holocryptic principles in the provision of dual single-originator - multi-originator equipment. In this connection it is desired that the Chief, Communications Research Section continue to pursue this matter and insure, through coordination with the various operating divisions, that continuing consideration is given the recommendations contained in the inclosed paper.

1 Incl
n/c

PAUL E. NEFF
Lt. Colonel, Signal Corps
Acting Deputy Chief
Army Security Agency
Ext 498



WASHINGTON 21 JUL 47
ARMY SECURITY AGENCY
HEADQUARTERS

~~SECRET~~

Leo,

Read the penciled
notes underneath starting
with the bottom one.
That should give you
the background.

Your opinion
would be appreciated

MR

Mr Roach

Wp Stauffer will
discuss with you

R

SECRET

CONFIDENTIAL

REF ID: A4127221

RESTRICTED

TO

DATE 27 Nov 44

FROM

Commanding Officer

Assistant Commandant

Dir of Comm Research ✓

Control O

Administrative O

Adjutant

Intelligence O

Provost Marshal

2nd Sig Serv Bn

Chief, Pers & Trng Div

Chief, Pers Br

Chief, Trng Br

Chief, Oper Serv Div

Chief, Communications Br

Chief, Laboratory Br

Chief, Machine Br

Property & Supply O

Purchasing & Contracting O

Fiscal & Certifying O

OIC, Mail Section

Chief, Security Div

Chief, Protective Sec Br

Chief, Cryptographic Br

Chief, Development Br

Chief, Intelligence Div

Chief, Language Br

Chief, Mil Cryptanalytic Br

Chief, Gen Cryptanalytic Br

Chief, T/A and Control Br

Chief, I & L Br

As discussed

As requested

Comments and return

Information and file

Information and forwarding

Information and return

Recommendation

See note on reverse ✓

Signature if approved

Your action

Mark

Maybe it's not too

late yet

Suggest you

talk it over with Leo

F

[Handwritten signature]

Mark:

I note you proposed
to file patent.

Was that ever
done?

J

No, In my innocence I
thought if the idea had any
merit the people who read the
report would do something about it.
Hearing nothing, I did nothing.

Coincidence REF ID: A4127221

1. Your remark in these minutes of a gadget I had invented years ago (p. 4)

2. Capt. Smith's telling me about some old reports of mine he had just come across. (See pages 3 + 4 of Blue Item)

WR.

Date 28 August 1944

From Lt Parks 1509-B.

Col Corderman

Col. Collins

Col. Hays

EXTRACT FROM FIFTH MEETING OF ARMY-NAVY CRYPTANALYTIC RESEARCH
AND DEVELOPMENT COMMITTEE 15 NOVEMBER 1944

* * * * *

Current Developments in Intercept Equipment

Lt. Col. Rosen mentioned a device which is being constructed for marking the Baudot start pulse position on undulator tapes. This device, if successful, will greatly facilitate the reading of tape records of 5 unit code transmissions. At GCCS this marking is done by hand.

Mr. Morris stated that the time delay recorder is undergoing test at Vint Hill. In a current security monitoring mission in which multitone teletype transmission was transmitted on one side band and speech on the other, the delay device made possible an arrangement by which all telephone communication was recorded without the long intervals which actually occur between transmissions and without loss of any part of the communication. It was suggested that this method is of significance in connection with telephone monitoring of any sort. Mr. Friedman point out that this was a means of accomplishing what Capt. Rhoads had suggested in 1935: that a message be copied by automatic means only where such an identifying word as ETAT appears in the transmission, thus saving monitoring time. Capt. Wenger reported that the P/L equipment will be set up temporarily at Skags I. until something further develops on scrambled speech transmission. Mr. Morris said none of the latter, i.e. Japanese origin, had been observed for a year.

Declassified by NSA/CSS

Deputy Associate Director for Policy and Records

On 20121119 by RFM

~~TOP SECRET~~EXTRACT FROM FIFTH MEETING OF ARMY-NAVY CRYPTANALYTIC RESEARCH
AND DEVELOPMENT COMMITTEE 15 NOVEMBER 1944

* * * * *

Current Developments in Intercept Equipment

Lt. Col. Rosen mentioned a device which is being constructed for marking the Baudot start pulse position on undulator tapes. This device, if successful, will greatly facilitate the reading of tape records of 5 unit code transmissions. At GCS this marking is done by hand.

Mr. Morris stated that the time delay recorder is undergoing test at Vint Hill. In a current security monitoring mission in which multitone teletype transmission was transmitted on one side band and speech on the other, the delay device made possible an arrangement by which all telephone communication was recorded without the long intervals which actually occur between transmissions and without loss of any part of the communication. It was suggested that this method is of significance in connection with telephone monitoring of any sort. Mr. Friedman point out that this was a means of accomplishing what Capt. Rhoads had suggested in 1935: that a message be copied by automatic means only where such an identifying word as ETAT appears in the transmission, thus saving monitoring time. Capt. Wenger reported that the P/L equipment will be set up temporarily at Skags I. until something further develops on scrambled speech transmission. Mr. Morris said none of the latter, i.e. Japanese origin, had been observed for a year.

~~TOP SECRET~~