ARMY SERVICE FORCES
SIGNAL SECURITY AGENCY
WASHINGTON 25, D. C.

SPSIS-3 2 May 1945

SUBJECT: Investigation of System Indicator Encipherment

TO: Major Horton, Security Division

1. The attached study shows that a good deal of thought has been devoted to the problems involved in the disguise of system indicators, and presents a very good case of the difficulties that would be encountered.

2. I regret that I have to say that I do not agree with the conclusions reached therein. I think that sooner or later we have got to do something along these lines of protecting our communications to the maximum degree consistent with operational practicabilities. Even a delaying effect would be useful.

3. In view of the fact that there is a good probability that an extensive survey of the security of our communications will be undertaken by a special committee under the JCB, it is recommended that this study be held in abeyance until the survey referred to is actually undertaken or a decision not to have such a survey is made. We should know the answer to this within two or three weeks.

W.F.F.

1 Incl
S/S, same as above
subject

WILLIAM F. FRIEDMAN
Director of
Communications Research

Adjutant General's Office
Form No. 6118
April 7, 1942

WAR DEPARTMENT
ARMY SERVICE FORCES

MEMO ROUTING SLIP

To the following in order indicated:

GPO 16—84260-1

		(Initials) / (Date)
1	Mr. Friedman (Name or title) (Organization) (Building and room)	
2		
3		

I would appreciate your comments and/or recommendations

RSH
16 April 45

From

(Name) (Organization) (Building and room)

(Date)
(Telephone)

~~SECRET~~ REF ID:A101100

HEADQUARTERS, ARMY SERVICE FORCES

MEMO ROUTING SLIP

TO THE FOLLOWING IN ORDER INDICATED:

	NAME OR TITLE / ORGANIZATION / BUILDING AND ROOM	INITIALS / DATE
1	Chief, Security Division	
2		
3		

1. The attached investigation of the problem of system indicator encipherment is forwarded for your information.

2. Concurrence is requested in the proposal to table this investigation for the following reasons:

a. Our investigation has indicated that it will be impractical to employ enciphered call signs or a policy of frequent changes of radio frequencies on the War Department Command and Administrative Network.

b. Very little, if any improvement, in security may be anticipated from enciphering indicators in tactical formations only.

c. The attached report indicates no reason to encipher system indicators from a viewpoint of cryptographic security.

3. The general problem of system indicator encipherment will be kept on the docket for study as a matter of interest but given no priority.

FROM: NAME / ORGANIZATION / BUILDING AND ROOM	DATE
Richard L. Downing, Major, Sig. Corps Communications Security Br.	14 Apr. 1945
	TELEPHONE 261

~~SECRET~~

W. D., A. G. O. Form 0115
1 October 1944

This Form supersedes W. D., A. G. O. Form 0115, 23 March 1944, which may be used until existing stocks are exhausted.

16—81046-2 GPO

INVESTIGATION OF SYSTEM INDICATOR ENCIPHERMENT

I Scope:

To investigate the following problems with respect to encipherment of system indicators:

1. What are the requirements of a system for enciphering system indicators?

2. How is system indicator encipherment to be accomplished?

3. What changes in cryptographic systems are necessitated by system indicator encipherment?

4. To what systems will system indicator encipherment be applied?

5. Will system indicator encipherment apply to cryptographic systems of all echelons?

6. What is interrelation of U. S. Army system indicator encipherment with Joint and Combined systems?

7. What is interrelation of U. S. Army system indicator encipherment with systems of other U. S. governmental agencies?

II Discussion:

Problem 1

1. Whatever cryptographic system is used for enciphering system indicators must fulfill certain requirements that usually are not of prime interest in the general cryptographic system. These requirements must be considered in designing a system for enciphering system indicators.

a. The system must be capable of world-wide use.

b. The system must be a Cryptographic System unrelated to any now in use.

c. The solution of keys for one day will not compromise the keys of any other day.

d. The system must resist solution in cases where many encipherments of the same plain text is available for analysis.

e. The system must produce a different encipherment of the system indicator in each message.

2. It is obvious that a single world-wide system must be employed, otherwise indicators for indicator systems would have to be set up, which is absurd, and could be extended ad infinitum.

a. A world-wide system involves several problems in production and distribution but these are generally similar to those now arising in the production and distribution of other cryptographic systems. The amount of production, of course, depends on the type of system adopted. Distribution will follow the channels now operating. However, consideration must be given to cases of compromise of the system and the action to be taken when this happens. World-wide distribution does encounter delays.

b. In the compromise of the usual cryptographic systems there must be allowed a day or two of delay merely to permit notification of all holders. For the system with a few holders there isn't much danger of overlooking one or two and failing to notify them of the compromise and resulting changes. On a world-wide basis, though, a notice must be sent to all holders and it is quite possible that some will be overlooked or will receive the notice after a delay of several days. Under these conditions there will be confusion at those headquarters on incoming messages and at stations receiving messages from these headquarters there will also

be confusion in identification of systems. Consequently, explicit instructions must be devised to cover all situations involving delays.

c. Distribution and use of the system must be coordinated on a world-wide basis. Consider the general cryptographic system: Should a headquarters fail to receive a key list on time there is no great harm done since the previous key list may be re-used for a short time or else a stand-by system may be used.[1] If this is done unenciphered system indicators immediately make this fact known to recipients but may require services on messages received in the "undelivered" key list. On the other hand, without the current key list to encipher system indicators there is no immediate solution to handle incoming and outgoing traffic. Incoming messages may be tried in a system known to be held by the originator but the classification will remain unknown.

3. There is no cryptographic system held in common by all holders. Therefore, a system to encipher indicators must be an extension of a present system to all holders or a new system issued to all holders. It is believed that no U. S. Army cryptographic system now in general use is suitable for enciphering system indicators.

a. The Converter M-325 has been proposed as a means of accomplishing encipherment of system indicators.

b. The Converter M-325 is available in quantities and it is believed could fill the needs insofar as distribution is concerned. The security of the Converter M-325 does not appear to be adequate and this question is considered in paragraph 8.

---

[1] It is believed that inherent security in most War Department systems is sufficient to recognize that occasional re-use of a system is not harmful. Every effort is made to have systems in the hands of holders before the effective date.

4. As a practical matter there should be no linkage from day to day or, at least, if a solution is possible on whatever system is adopted the difficulty of solution each day should be the same. If unenciphered system indicators change only when key lists change, as at present, solution of the system indicator system will give the plain-text system indicator for other days prior and subsequent to the compromise.

5. By the very nature of system indicator encipherment, depths will exist in greater numbers than have ever been considered to exist in a cryptographic system.

a. It may be assumed that the enemy is familiar with our administrative nets and there is no reason to believe that these nets will change at the time system indicator encipherment becomes effective. There are a number of holders of only one or two cryptographic systems and these will have been established by observation of present practices. When system indicator encipherment is instituted it would be natural to assume that these holders will continue to use only one or two systems and must be applying encipherment to the same system indicators from day to day. (Not necessarily the identical system indicators used prior to encipherment but changes contingent upon change of key lists.) By collecting all such traffic, study can be directed to these particular cases for intensive analysis. Solution of the indicators on these few messages will compromise the world-wide system.

b. Errors of several forms are certain to occur in encipherment and should be overcome insofar as practicable. For example: Messages will be sent without enciphered system indicators, thus providing plain text,

if it can be recognized. Mistakes in encipherment will occur which might reveal information. Similar unenciphered system indicators may provide a means of entry into the system.

6. It is desirable to limit the amount of information which variations in method of applying the enciphered system indicator may produce.

a. Two alternatives are possible in the encipherment of system indicators with respect to time:

(1) The system indicator of every message to be enciphered.

(2) The system indicator to be enciphered only at stated intervals, i.e., every tenth message, once each day, once each week, etc.

b. In all but strips and double transposition the problem of solution on U. S. Army cryptographic systems is essentially a daily one. That is, a solution on one day does not contribute to the solution of another day except for such information found in the traffic of the solved day which may be extended to contents of messages of preceding and following days. By enciphering the system indicator once each day little will be gained in protection of cryptographic security since the traffic for each day can still be sorted into homogeneous groups. Longer periods add nothing at all, being worse than merely a daily change.

7. With encipherment of the system indicator for each message some means must be provided to vary the encipherment. This means can be found in either the message indicator or in the cipher text of the message. Either of these two sources may be considered to be without order and to provide an unpredictable key to encipher the indicator. In order to apply the procedure uniformly to all systems the message indicator would be better,

although one-time tapes do not at this time contain alphabetical components. Difficult situations would arise in systems operated on-line in being able to obtain cipher text prior to identifying the system to the addressees, and for off-line operation of certain systems the procedure should permit encipherment to be made prior to perforating a tape. Otherwise, splicing or other awkward arrangements would have to be used.

Problem 2

8. Several methods have been considered as a means of accomplishing the encipherment of system indicators.

a. As mentioned in subparagraph 3b, the Converter M-325 has been considered as a means of enciphering system indicators. Preliminary security tests on this device in connection with the problem revealed serious weaknesses that make the Converter M-325 undesirable for the purpose. The natural selection of a variable for each message is the alignment of rotors. As indicated in paragraph 7 the external message indicator could be used for this purpose and would therefore indicate the alignment of the rotors. The external message indicator being sent in clear, initial alignment of rotors for each system indicator enciphered would be known. From this information, and with an assumption of identical plain text (see the discussion in subparagraph 5a) it would be possible to reconstruct the rotor wirings, end-plate plugging, and reversing rotor. Reconstruction of these elements is sufficient for the day since the alignments of each system indicator are given in the message and all system indicators for that day can be found easily merely by deciphering the indicators.

b. A second method proposed for the encipherment of system indicators is the system used at the present time by the U. S. Navy for enciphering call signs. This is a tetragraphic fractionating system that

uses a 4th order matrix as an enciphering equation.[1] Such a system would have to be changed to a pentagraphic type to accommodate 5-letter indicator groups.

(1) As in any device which may be required for encipherment of system indicators, design and procurement would have to be instituted sometime prior to the date planned to place the encipherment of indicators into effect. The system would require that each holder possess a 64-page document each month containing the matrices for enciphering and deciphering.

(2) The method can be applied by pencil and paper alone but still requires the monthly keying information. However, with paper and pencil the job is rather slow and is subject to errors in addition and subtraction by using personnel.

(3) The type of analysis that is used for solution with this system consists in solving a large number of simultaneous linear equations, about 34 as the minimum for a 4th order matrix. For this purpose it is necessary to find about 35 encipherments of texts which overlapped, as ABCD, ABCE, AFGE, etc., with equivalent plain text. If such overlapping encipherments cannot be found, it is necessary to have about 150 encipherments with equivalent plain text. Solution of these equations

[1] The principles of the method are well known, having been published in mathematical journals several years ago.

compromises the system for the day. With a different matrix used for each day the solution of encipherments for the next day is a new problem to be treated as indicated above.

(4) Solution of equations of the above mentioned type, while not difficult, is laborious and time consuming. Moreover, in the solving of these equations, the Navy has ~~been~~ found that only a few people (3 to 5) are able to work at one problem, and that additional personnel hinders rather than aids in the solution because more interfere with each other. Machines of the kind necessary to solve these equations are not in common use; but since they need only perform a large number of arithmetical processes, there is no reason to doubt that such equipment could not be constructed to perform the job daily.[1]

c. A literal one-time system with normal alphabets offers no security at all because the specific key will be known from the message indicator (see paragraph 7) thus determining the plain text. With an unknown alphabet relative values can be established which will be as effective as the genuine indicator. Relative values may be linked from day to day by analysis of transmission data.

d. Numerical additive systems will involve conversion from letters to numbers and from numbers to letters. Such a procedure is subject to error during the conversion as is any additive process involved.

[1] The calculating machine recently constructed by International Business Machines for Harvard University may be capable of such work.

e. From studies of various systems proposed for use as methods for enciphering system indicators there are indications that any method which makes use of a letter for letter substitution based upon a known key is subject to a great many objections from a security viewpoint. The best that may be expected from the system is a delay in solution.

f. It appears that of the various systems considered, the only type which will provide the necessary security is either an additive system with one-time characteristics or a fractionating system. A fractionating system which includes all the letters of the indicator and a key contained in the message seems to offer the greatest protection. A fractionating system, since it involves all letters of the indicator, will require solution to be based upon the indicator as a unit. To achieve a solution, much material will be necessary and although it is likely that this may be obtained, some delay in solution should be expected. A one-time system would require an enlarged production plant to produce the system.

Problem 3

9. The primary result to be expected of system indicator encipherment is increased security in all cryptographic systems. This may be desired because of inherent lack of security in the cryptographic systems employed. On the other hand, if the systems used do provide a great deal of inherent security, or control is exercised over elements which may be weak in otherwise strong systems[1], encipherment of system indicators may not be necessary. That is, the question may be asked, "If the traffic can not be solved what degree of security is gained by increasing the difficulty of solution?"

[1] For example: Message length, traffic volume.

10. Enciphering system indicators must be integrated with other changes in cryptographic systems if it is to achieve its purpose. For example: Disregarding the system indicators altogether, other characteristics in the traffic will reveal some information about the various U.S. Army cryptographis systems.

a. Teletype systems (except Converter M-294, of which more shortly) can be separated immediately from all other traffic. Converter M-228 and SIGTOT can be separated on the basis of differing forms in the message indicators. This type traffic is characterized by lack of grouping in the cipher text. Other individual characteristics are present.[1] The traffic from Converter M-294 is spaced into groups when used off-line but may be differentiated from all other teletype traffic by the eight letter message indicator. Traffic from the Converter M-294 may be difficult to distinguish from traffic from the Converter M-228 when the Converter M-294 is operated on-line.

b. These three types of systems can be screened from the total mass of traffic without any difficulty. To break them down into separate systems will involve the techniques of traffic analysis and a more detailed analysis of the systems than indicated here. Without going into a detailed analysis of this problem it is sufficient to state that a good knowledge of the various nets and with a knowledge of the systems those nets are accustomed to use it is believed that a separation could be made with some success.

c. Literal one-time pads, Converter M-134-C, Converter M-325, and strip systems have the same general characteristics. The screening

[1] The group count, for example, is a word count and is immediately apparent.

will be more difficult without system indicators but certain screenings can be made. Messages in one-time pads and Converter M-134-C can have a longer length than messages in strips or Converter M-325. Strip systems carry message indicators without repeated letters[2]. The possibility exists that strip systems may be identified by characteristics of inverse frequency of letters. Again, knowledge of the communication pattern and previous usage of systems in a net will aid considerably in sorting individual systems.

d. Double-transposition systems and the War Department Telegraph Code can be separated immediately by their individual characteristics.

e. Any other systems which may be in use or will be placed in use in the future can be judged as to individual characteristics by comparison with existing systems. A more detailed analysis of the characteristics of each type of system would undoubtedly add other items of assistance in classifying each system. Such a study is not pertinent to this analysis.

11. Another consideration for enciphering system indicators is the concealment of any information which may be helpful to the enemy in traffic analysis.

a. There is a correlation between classification and precedence, and certain other characteristics of the transmission. The classification, if it can be determined for each message, permits analysis of flow of traffic to be made on the basis of classification which may reveal information as to order of battle, troop movements, etc.

---

2 This practice can readily be changed and should be as soon as there is certainty that the enemy has learned of the change in message indicator encipherment for strip systems.

b. There is other information, however, which can be gained from the heading without reference to the system indicator. File time and transmission time can be used to gain information. The volume of traffic, its direction of flow, and precedence are other items which may be subjected to analysis to gain valuable information.

Problem 4

12. System indicator encipherment could be applied to all types of systems namely, War Department system, Theater system, and tactical systems used by combat troops.

a. War Department systems require an indicator to identify the specific system and in conjunction with this information to indicate the classification of the message. Theater systems for the most part also require individual identification but systems in use by tactical units can dispense with indicators to a large extent. Indicators are necessary in some cases, perhaps, to avoid confusion but it may be that a revision of the distribution in tactical units could eliminate all need for system indicators. It should be noted, though, that the theory under which these systems are used is a distribution of traffic loads to protect the security of the system. (The need for this has been evident in use of the Converter M-209 and distribution of traffic loads still could be improved.) In many instances system indicators are not used and relation between the system indicator and other items cannot be established.[1]

b. Evidence is slight of the Japanese using the system indicators in traffic analysis. There is evidence that other items are made use of and also that only low echelon traffic is studied. Much is made of

[1] TB SIG 11-380-2 suggests that key list indicators (equivalent to system indicators) not be used unless there is confusion caused by leaving the indicator off the message.

information transmitted in clear. Some evidence exists that nets of higher echelons are not monitored but as yet this is inconclusive.[2]

c. If system indicator encipherment were applied to War Department systems and related Theater systems there are two plans which may be considered. One is to apply the encipherment to all systems. The other is to encipher the system indicators of only certain systems.

(1) To answer the second point first. Regardless of any considerations of cryptographic security, if advantage could be taken of the system indicator in traffic analysis it would seem desirable to encipher all system indicators in order to avoid this condition.

(2) The work involved in enciphering all system indicators is but little more than for part of them. Production would be about the same as would distribution.

(3) Easily identifiable systems (WDTC) may be a weakness if the system indicator is enciphered. Provision would have to be made to change this indicator frequently.

(4) Messages to and from Military Attaches are easily identifiable and while traffic information available from these sources may be slight, encipherment of the system indicators may become points for analysis of the system indicator encipherment system.

---

[2] A detailed study is planned to investigate thoroughly the amount of information gained by the Japanese through traffic analysis. "A" Branch has been making studies on correlation of information received from Japanese sources and other available information relating to traffic analysis.

SECRET

Problem 5

13. If encipherment is applied to all echelons, coordination will have to be effected by Theaters within the Theater for production of systems to encipher system indicators. In this connection one point must not be overlooked. It is known from a study of SOI's that a multiplicity of systems exist throughout the various theaters. (Many SOI's from SWPA and POA have not been received for examination so that a knowledge of systems in low echelons is scanty.) While many of these do not use a system indicator any which do make use of a system indicator must be suitable for encipherment or provision made to change it so that it can come within the limits necessary.

14. Unless a system is devised which requires very little production and compilation in the preparation of a key list, planning would have to include considerations for production of these keys for theaters by the Signal Security Agency.

Problem 6

15. It is possible that encipherment of system indicators would not be immediately acceptable to the U. S. Navy for use in the Navy. In any event consideration should be given to handling of Joint systems. These systems will immediately become evident the instant they are placed on an Army circuit which handles Army traffic with enciphered system indicators. Many of the same situations will exist in combined systems.

Problem 7

16. A somewhat similar situation to that of Problem 6 arises in the case of other U. S. governmental agencies for which the U. S. Army acts as

SECRET

adviser on matters concerning codes and ciphers. In some cases the Army produces the systems used by these agencies. It is desirable to make all systems which pass over Army circuits resemble Army traffic. In many cases (OSS, for example) these agencies have peculiarities in their traffic which would establish it as distinct even though the system indicators were enciphered. These differences should be adjusted before any final steps are taken.

III Conclusions.

17. Before the encipherment of system indicators can be accomplished practically a number of minor problems will have to be worked out, as indicated in the Discussion. Many of these are unrelated to each other and entail relatively little change from the security viewpoint. Many will be serious from a practical operational viewpoint. For instance, the length of SIGABA messages was changed from a limit of 100 groups to 350 groups. This was done primarily to expedite handling of long messages. Since security of SIGABA is not known to suffer under this usage a great advantage has resulted in practical application of the SIGABA.

18. There is no positive evidence that U. S. Army systems above tactical level are being read by the enemy. There is considerable negative evidence which tends to show that the enemy is not reading any of the "high-grade" systems generally used above the level of Division or comparable units. It is known that tactical systems such as the Converter M-209 and small operations codes used within Division have been read by the enemy. There is some indication that a few scattered strip systems may have been read. From the viewpoint of cryptographic security the need

for enciphering system indicators to provide protection for other than tactical systems does not exist.

19. From various sources it is known that several factors contribute to solution of tactical systems by the enemy. Use of system indicators does not have a direct bearing on the solution because many of the systems use no system indicators. Inexperienced operators and code clerks are indicated to be the greatest single source of errors which lead to cryptanalytic compromise in these systems.

20. It appears likely that no system can be developed which will meet all requirements for a system indicator enciphering system. The best that may be attained is a delay. For security of a cryptographic system merely delaying is not sufficient unless it is for an appreciable period of time. There seems to be no point in proposing to use a system which serves only to delay. It is difficult to establish the "time of delay" and it may be more apparent than real. The need for causing unnecessary confusion and work does not appear to be justified by the results to be expected in only a delay.

21. There will be considerable confusion resulting in a change of the magnitude occasioned by encipherment of system indicators. Careful thought and planning will be absolutely necessary in preparing to place such a scheme into effect so as to avoid throwing chaos into a communications system that is now taxed, at times, to move traffic. Small changes in procedure designed to further the project should be studied with care before being put into effect, otherwise, subsequent changes based upon later information may make the first unnecessary or required still further modifications in it.

22. Three other phases of an over all communication security plan which are related to the present problem must be kept in mind:

a. Protective Security.

b. Conventional encipherment of call signs.

c. Concealment of all information including the total amount of traffic by means of ciphony, cifax, or similar schemes.