VF 108-13

WAR DEPARTMENT
Office of the Chief Signal Officer
Washington

INFORMATION REGARDING CRYPTOGRAPHIC SYSTEMS SUBMITTED FOR CONSIDERATION FOR USE IN THE MILITARY SERVICE

The following are the most important requirements which a cryptographic system for military use must fulfill. They are given under three headings, (A) Practicability, (B) Secrecy, and (C) Speed. In order that a cryptographic system be given any consideration whatever, it must first meet the requirements as to practicability.

A. As to Practicability:

1. The cryptograms must be in a form suitable for economical transmission by International and American Morse telegraphy. This requirement practicall eliminates all systems except those which produce cryptograms composed EXCLUSIVEL of the 26 letters of the alphabet, arranged in regular groups of five letters. Cryptograms composed exclusively of arabic numerals arranged in regular groups of five digits may be worthy of consideration for special use, but not for regular use in the field, because they are slower and more difficult to handle in telegraphic transmission, and because the cryptographic text is usually twice as long as the equivalent plain text. Systems which produce cryptograms composed of mixtures of letters and figures, or of letters, figures, punctuation signs, and the like, cannot be considered under any circumstances because of impracticabilities in their transmission and reception by telegraph or radio.

2. The channels of communication in the combat zone are so limited and so subject to interruption that their most efficient use is absolutely essential. For this reason it is necessary that no more characters than are actually required to transmit intelligence be sent over these channels. In the case of a system for field use, therefore, the cryptographic text should be no longer than the equivalent plain text. In the case of systems for other than field use, the cryptographic text may be somewhat longer than the equivalent plain text, but no system in which the cryptographic text is twice the length of the equivalent plain text can be considered unless it is of outstanding merit otherwise, and unless it is suitable for certain restricted special usages. No system in which the cryptographic text is more than twice the length of the equivalent plain text can be considered under any circumstances.

3. In the United States Army practically all work connected with enciphering and deciphering of messages is done by enlisted men, who very frequently have to perform this work under extremely trying conditions. The method of encipherment and decipherment must therefore be relatively simple and rapid. It must not require the remembering and application of a long series of steps or rules, and must be such as to reduce to a minimum the mental strain upon the operator. As a rule, complex processes involving several distinct steps are not suited to the conditions in the combat zone, but systems involving only two steps provided each is simple and rapid, may be worthy of consideration. In the case of a system for field use, it should require the services of only one operator either to encipher or to decipher messages.

4. Cipher devices or instruments for field use must be light in weight rugged in construction, and simple in operation, requiring the services of only o operator either to encipher or to decipher messages.

5. The system must be such that errors, which invariably occur in cryptographic communication, can be corrected easily and rapidly by the decipher-ing operator, without the necessity of his calling for a repetition of the trans-mission, or a rechecking by the enciphering operator. Systems in which errors are cumulative in their effects, that is, affect many or all subsequent letters, thus making the decipherment of the message very difficult or impossible, are impractical for military use.

B. As to Secrecy:

6. A cryptographic system to be employed in military communications must be composed of two separate and distinct elements:

a. A basic or unchangeable method or process of treating the letters of a message.

b. A specific or variable key which governs or controls the exact steps under the basic method.

7. The secrecy of cryptograms must rest entirely upon the second of these two elements and not at all upon the first element, because in military cryptography it must be assumed that the enemy is in possession of all the details of the basic method and knows exactly how it is used. In case a cipher device or instrument with a fixed mechanism is used, it must be assumed that the enemy possesses a duplicate of it, or at least understands in detail its exact operation.

Note: The peculiar nature of the foregoing requirement is possibly so little understood by those not familiar with the conditions which exist in mili-tary communications during war time that a rather detailed explanation seems advisable. There are several reasons why it must be assumed that the enemy has full knowledge as to the basic cryptographic method underlying the cryptograms he is attempting to solve, the most important of which are the following:

(a) It requires a considerable length of time to instruct several thousand soldiers in the proper handling of any cryptographic method. If the secrecy of cryptograms were entirely dependent upon keeping the method of their preparation secret, it is obvious that once this method became known to the enemy an entirely new system would have to be adopted. If such radical changes had to be instituted every month or two, the whole communications system would become impractical and would break down.

(b) Military experience throughout history has proved that it is impossible to maintain absolute secrecy about a cryptographic method which must be used by a very large personnel, for a very voluminous traffic, at many and widely separated headquarters. Without bringing into considera-tion the possibility of treason, or the activities of enemy agents, it is

necessary to take into account the fact that the legitimate operations in combat, such as the capture of prisoners and of command posts, and the information obtained by an efficient intelligence organization sooner or later results in the accumulation of data sufficient to disclose the details of the cryptographic method.

(c) Military experience has likewise proved that even if attempts to maintain complete secrecy regarding the cryptographic method are successful, the large number of messages exchanged during active operations makes it possible for the enemy to obtain a very great volume of traffic for study, amounting to thousands of messages. These may be in hundreds of different keys, but with a large staff of experts available for studying this traffic, together with the very considerable amount of collateral information obtainable from military intelligence, and the valuable information often available as a result of the almost inevitable blunders committed by cryptographic personnel working under difficult, hazardous conditions, the basic method sooner or later becomes known. If the secrecy of messages depends almost entirely upon this factor, then the system would have to be discarded immediately and a new one adopted. This, as stated above, would be impractical if it had to be accomplished at frequent intervals. It may be said that a whole year is required to instruct a large army in the proper use of even the most simple cryptographic system, the details of which a single individual may be able to grasp within an hour.

8. The specific key, upon which secrecy is entirely dependent, must therefore be susceptible of easy and rapid change by prearrangement between correspondents. In the case of a system for field use it may consist of a letter, word, phrase, or sentence which can be easily remembered, or of a number which can be easily remembered or derived from a word, phrase, or sentence. In the case of a system for use in the larger offices in the rear, the specific key does not have to be such that it can be remembered, and may be in the form of written memoranda, prepared tapes, etc.

9. In general, the specific key must be the same throughout one day and for as many offices or individuals as may exchange communications within a given area. The latter requirement may result in the interception, by the enemy, of as many as 100 to 200 cryptograms, each averaging 200 letters, <u>all in the same specific key</u>. On the other hand, if the same cryptographic system but with different specific keys is employed in separate areas, the situation will arise, as in the past, where the <u>same</u> message is enciphered by different specific keys. An alert enemy will intercept <u>all</u> the messages transmitted by his adversary; he will not have merely a great many messages for study and comparison, but will have some cryptograms representing different plain texts in the same specific key, other cryptograms representing the same plain text in different specific keys, and he may even have a cryptogram or two with their exact or paraphrased translation, obtained by one means or another, often purely as the result of blunders or carelessness on the part of personnel intrusted with the handling of codes and ciphers.

10. Conforming to all the preceding requirements, therefore, the system must be of such a nature that despite the enemy's full knowledge of all the details of the basic method (or his possession of the apparatus, if one be used), and despite the fact that he may have available for study as many as 1000 cryptograms, it must nevertheless be practically impossible for him to read or translate the cryptograms within a sufficiently short period of time for the information obtained in this manner to be of any real value to him unless he also knows the specific keys applicable to the cryptograms.

11. It is obvious that in making a peace-time, miniature, theoretical test of any proposed cryptographic system for military use, it is impossible to duplicate the conditions which actually exist in war time, not only as regards the volume of traffic available for study, and the extensive personnel and establishments usually set up for cryptographic studies, but also as regards the very great amount of general and specific information usually collected by an efficient intelligence service, all having a rather direct bearing upon the success of cryptographic efforts. The best that can be done in such a test is to attempt to bring about the situation that would exist in war time after a given cryptographic system has been in use for a few days and after the cryptographic unit has obtained a fair start in its labors. For this reason, it has been found necessary to adopt the rule that persons who desire to submit cryptographic systems for consideration for use in the military service should submit the data listed under Paragraph 8 (6) of the form to which this enclosure is applicable.

C. As to Speed:

12. The increasing mobility of modern military forces has of late put a new conception on the speed requirements of cryptographic systems. Methods which were considered fairly rapid in 1918 are today hopelessly slow. It has become necessary to fix the minimum speed requirement for cryptographic processes at 20 words (100 letters) per minute. Furthermore, the necessity for speed is gradually assuming almost paramount importance. Even secrecy must, if necessary, give way to speed.