S & S Files

CONFIDENTIAL

W.P. & T. Div.

WAR DEPARTMENT
aln
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

March 28, 1933

MEMORANDUM TO: Major Hugh Mitchell, Officer-in-Charge,
Research & Development Division.

Attached hereto is a revised report, in duplicate, on Signal Corps Converter, Type M-134, which will be of interest to you and to the Signal Corps Laboratories at Fort Monmouth.

S. B. Akin,
Major, Signal Corps.

Attached:
Report in dupl.

CONFIDENTIAL

REPORT ON SIGNAL CORPS CONVERTER, TYPE M-134

1. A test of the cipher machine disclosed the following:

a. Speed.

(1) The maximum mechanical speed of the machine, determined by depressing the same key repeatedly and as rapidly as possible, is 33 depressions per minute.

(2) The maximum speed of encipherment or decipherment by an operator working as rapidly as possible for a short length of time, approximately five minutes, is 30 letters per minute.

(3) The average speed of encipherment or decipherment by an operator working in a methodical manner for a fairly long period, approximately 30 minutes, is 25 letters per minute. This average is based upon the actual encipherment and decipherment of 1066 five-letter groups, equivalent to approximately 6000 letters.

(4) Comparative speed tests with Cipher Device M-94 and with the Division Field Code, using portions of the same text as above, showed that the cipher machine is approximately twice as fast as the M-94 device, but no faster than the Division Field Code.

(5) Further remarks on the subject of speed will be found under paragraph 2 a. to d., incl.

b. Reliability.

In general it may be said that the machine is quite reliable in operation, but the following mechanical failures were noted during the test:

(1) When the keyboard keys are allowed to come up slowly after depressing, the cipher wheel occasionally fails to rotate and orient itself to its next correct position. This failure seems to be caused by faulty action of the tape-stepping mechanism, and renders all subsequent text incorrect. In normal operation of the keyboard, however, this failure does not appear.

(2) Occasionally, the cipher wheel is brought to a stop in a position slightly off that required to bring the contacts on the wheel in juxtaposition with those on the fixed discs between which it revolves. When this happens the lamps will fail to light and the cipher wheel must be given a slight push by hand in order to establish contact for lamp indication.

(3) Unless the perforations in the keytape are accurately placed with respect to the pins of the keytape transmitter, there will be occasions when the transmitter pins will be set up for a permutation either not represented on the cipher wheel, or not correct with respect to the tape. When this happens the cipher wheel, in the first case, will not stop revolving, and in the second case, will stop at an incorrect position. While the first case happened many times during the test, the second either did not happen, or if it did, remained unnoticed, as it involves only a single-letter error.

c. Security.

Theoretically, the machine can be used to produce cryptograms that are absolutely indecipherable without possession of the key-tape. This method of operation would require the use of a key-tape representing a random-mixed sequence coincident in length with the total length of the traffic to be enciphered. Such a method would obviously involve great difficulties in practice with regard to the production, distribution and manipulation of key-tapes among the offices or organizations provided with the machines. If several offices use the same key-tape and the latter is employed repeatedly, even with different initial points for different messages, an accumulation of traffic that is solvable without possession of the key-tape would undoubtedly result, and the system would not be safe for use between the higher headquarters where communications secrecy for more than a few hours must be maintained.

2. The following comments are made:

a. The present limitation on the speed of operation of the machine is imposed by the fact that the cipher wheel must be displaced through irregular angular distances and brought to a stop at a precise spot. Although it might be possible to increase the speed of this displacement, it would be accomplished most probably at the expense of (1) certainty of operation and (2) a much increased wear and tear on the starting-stopping mechanism, with consequent lack of continued serviceability.

b. If a printing mechanism were added to the machine, the speed of operation would undoubtedly be increased, but to what extent cannot be stated. Certainly it would not be very great because most of the time lost in present operation is due to the necessity for waiting (a variable length of time in each case) until the cipher wheel has stepped to the proper position. This delay would still intervene even if the entire operation from depression of a key to printing of the character were automatic, because it is an inherent feature of the present cipher mechanism.

c. If a printing mechanism is added, full advantage ought to be taken of such a feature by freeing it, if possible, of the indicated limitations imposed by the cipher mechanism. By removing these limitations the speed of operation could be increased to three or four times the present speed in enciphering or deciphering.

d. As noted in paragraph 1 c, the cryptographic security depends upon the use of individual, extremely long key-tapes. If the present model were such that the speed requirements were easily fulfilled, and thus presented great advantages from the point of view of speeding up the cryptographic operations, it would be possible to introduce certain modifications which would reduce to a minimum the disadvantages and difficulties of tape production, distribution, and manipulation.

Two such modifications have already suggested themselves. But it is believed that the present design offers little possibility for increasing the speed of operation to the necessary minimum, 60 characters per minute; and it is safe to say that the desirable optimum, 200 to 250 characters per minute, could never be attained by a machine operating upon the present principle of an irregularly displaced cipher wheel.

3. It should be borne in mind that the present development is to be regarded as representing the initial, experimental phases of a project to produce a safe, automatic, rapid cryptograph. If the first model thus produced presents defects and disadvantages this is not more than might be expected in a field where many trials have been made by commercial interests with little or no success thus far, because so far as is known, no automatic cipher machines are in actual service either in commercial or governmental offices anywhere. While the model produced by the Laboratories represents a fine piece of engineering skill and mechanical workmanship, the defects and disadvantages pointed out above, especially in regard to speed of operation, are such as to lead to the following conclusions:

a. The present model should be regarded as a mechanism resulting from preliminary experiments, and showsthe possibilities and limitations of one type of design.

b. In the belief that the limitations of the present model are serious and difficult if not impossible to overcome in a machine intended for actual service where speed is an essential factor, the two sample machines thus far produced should be set aside temporarily and further work on this type of design should be suspended. It may well be that in the near future special use can be found for this model, in offices where speed is not an essential factor in secret communications.

c. A different basic design should at once be studied, with a view to overcoming the limitations of the first design.

4. Inasmuch as it seems advisable to change the basic design of the machine, serious consideration should be given to the possibilities of the scheme outlined in the attached description (entitled "The Proposed New Cryptograph") and accompanying photostat of a system bearing much resemblance to the present development but which, it is believed, offers much greater advantages than does the present model. It is believed that not only could the newly proposed system be operated as fast as a typist could manipulate a keyword, but also the degree of cryptographic security afforded by the use of relatively short keytapes by all communicants over a period of many days would be sufficient for communications exchanged between even the highest headquarters. In this way the difficulties of tape production and distribution would also be avoided. In fact, the advantages offered by the suggested new model, as set forth in the attached description, are believed to be so great as to warrant the initiation of work on the production of such a model at the earliest possible moment. This is urgently recommended. This office can furnish a machine which will, it is believed, readily lend itself to modification for the purposes in mind. All that would be necessary would be to add to it the present key-tape transmitter, five magnets and associated wheel-stepping mechanisms consisting of simple levers acting directly upon the present cipher wheels. The modification suggested might be accomplished in this manner within a short time and without difficulty.

5. It is further recommended that if work on the proposed printing attachment has not yet been commenced, it be delayed until a model of the new type has been produced, as it may influence the design of the printing attachment.

Attached:
Description.

THE PROPOSED NEW CRYPTOGRAPH

In Figure A, which is merely a diagrammatic representation of the proposed new cryptograph, there are shown the following elements all of which are well-known in the art applicable to modern cryptographs: 1, a standard typewriter keyboard provided with a set of 26 keys for closing a set of 26 contacts corresponding to the 26 letters of the alphabet; 2, a set of 26 indicating devices which may take the form of magnets of a printing mechanism or of lights to indicate by illumination the equivalents resulting from encipherment or decipherment; 3, a set of five rotatable circuit changers constructed in the form of cipher wheels mounted upon a common shaft and arranged in juxtaposition to provide a large series of variable paths for the passage of electric currents representing message characters, the exact path in each instance being determined by the relative rotatory position of the whole set of cipher wheels at that instant; and 4, a tape transmitter of the type employed in Baudot systems of printing telegraphy. In addition to these well known elements, there is shown a set of five magnets, 5, and a connection changer, 6, the purpose of which will now be explained.

In all the previous cryptographs based upon the use of rotatable cipher wheels of the type referred to above, and arranged as indicated, the means embodied in those cryptographs for changing the relative rotatory positions of the cipher wheels are of a definite and predetermined character. For example, in Hebern, U.S. Patent No. 1,683,072, the fixed character of the successive rotatory movements of the cipher wheels is explained in quite a detailed manner, and the same is true as regards similar cryptographs produced abroad. This invariability of motion produces, however, predictable relationships between the plain-text characters and the cipher characters for any given initial arrangement of the cipher wheels. Thus, should the whole cryptograph, and cipher messages fall into the hands of unauthorized parties, the latter can place themselves in a position to decipher the messages largely as a result of the predetermined nature of the successive rotatory displacements of the cipher wheels.

The basic feature of the proposed new system is the substitution of a variable mechanism for displacing the cipher wheels for the fixed mechanism referred to above, and this is accomplished by means of the tape transmitter, 4, and the set of five magnets, 5, controlled by the tape transmitter.

Tape transmitter, 4, consists of the usual five movable contacts 6, 7, 8, 9, 10, operated by a tape bearing a series of perforations corresponding to a random, unintelligible sequence of characters in the Baudot code. The perforations control the action of the five contact members, 6-10, which, in turn, control the action of the five magnets, 11, 12, 13, 14, 15, as a set of elements operating in a permutative manner. The connection between the magnets, 11-15, and circuit breakers, 6-10, is also subject to variation through the connection changer, 16, which is similar in form and function to that disclosed in U.S. Patent 1,522,775 of January 13, 1925. For the setting shown at 16 in Figure 1, where conductor 17 is connected, through the switchboard 16, to conductor 23 by a plug and jack arrangement, conductor 18, to conductor 22, and so on, the effect of the passage of Baudot character + - - - + would be to actuate magnets 12 and 11, respectively, equivalent to the Baudot character - + + - -.

The magnets 11 to 15, control, respectively, the displacement in step-wise manner, of the cipher wheels 27 to 31, and thus determine the rotatory positions of the five cipher wheels in encipherment or decipherment. It is assumed naturally that correspondents must be equipped with similar cryptographs, wired identically, and provided with identical key tapes for controlling the movements of the cipher wheels. The exact initial settings of the cipher wheels, the permutation set up at 16, and the initial point of action of the key tape must also be the same between correspondents, and can be predetermined by agreement.

The working arrangement may be such that on the back stroke of any key of the keyboard, a contact 32, controlled by a universal bar on the keyboard is closed, and the circuit for operating the tape step-forward magnet is closed. The next character on the tape is brought into play, the cipher-wheel magnets, 11 to 15, are operated and the cipher wheels are set to a new position for the encipherment (or decipherment) of the next character of the message.

Since the cipher equivalent for a letter depends upon the rotatory position of all five cipher wheels, and since this position is subject to variability by means of the connection changer, 16, it is obvious that for the same key tape set at the same initial point the cipher resultants will be different for each permutation set up at 16. Again, with the same permutation set up at 16, and the same key tape, the cipher resultants will be different for each different initial setting of the key tape. In addition to these sources of variability there are, of course, also those arising from changes in the initial settings of the cipher wheels, and their relative arrangement horizontally upon the shaft. Thus, with but a single key tape an enormous series of different encipherments of the same plain-text message can be produced by changing the other variable factors embodied in the system.

In order to provide for equivalency between encipherment and decipherment, there must be interposed between the whole set of connections leading from the keyboard and the whole set of connections leading to the magnets of the printer (or lamps of the lightbank) means for interchanging the connections to the left and the right fixed sequences of cipher wheels, 27 to 31. Figure B shows diagrammatically how this may be accomplished by means of a plate, which, actuated by a screw, can be moved to establish one or the other set of connections as required for encipherment or decipherment. This means is, however, not novel and already exists in at least one cryptograph already on the market.

A very important advantage which this system offers is that it will permit of using two keytape transmitters associated in an interacting relationship, as in the original American Telegraph and Telephone Company's Printing Telegraph Cipher System. Thus, by employing two keytape transmitters controlled by two relatively short, circular tapes, say 100 and 99 characters in length, respectively, a resultant single key of 9900 elements can be brought into play to actuate the cipher wheels 27 to 31. A tape containing 100 Baudot characters is approximately 10 inches in length, so that such tapes would involve very little difficulty in production, distribution and handling. Moreover, the mechanism of the cryptographic system is, in this case, such that the fact that two interacting, revolving

~~CONFIDENTIAL~~

keytapes are employed to produce a single resultant key does not, as in the American Telegraph and Telephone system, introduce any cryptographic weakness which can lead to solution of messages without the key.

Attached:
Figs A+B

William F. Friedman
O.C.Sig.O., Washington
March 28, 1933

Contacts a, b, c, and d (four of a set of 52 similar contacts) are all mounted upon the same plate which can be moved to the left or to the right of neutral position shown. When plate is moved to right, contacts are made for enciphering; when moved to left, for deciphering. Thus, if in enciphering A (Plain) = Y (Cipher), then Y (Cipher) = A (Plain) in deciphering.

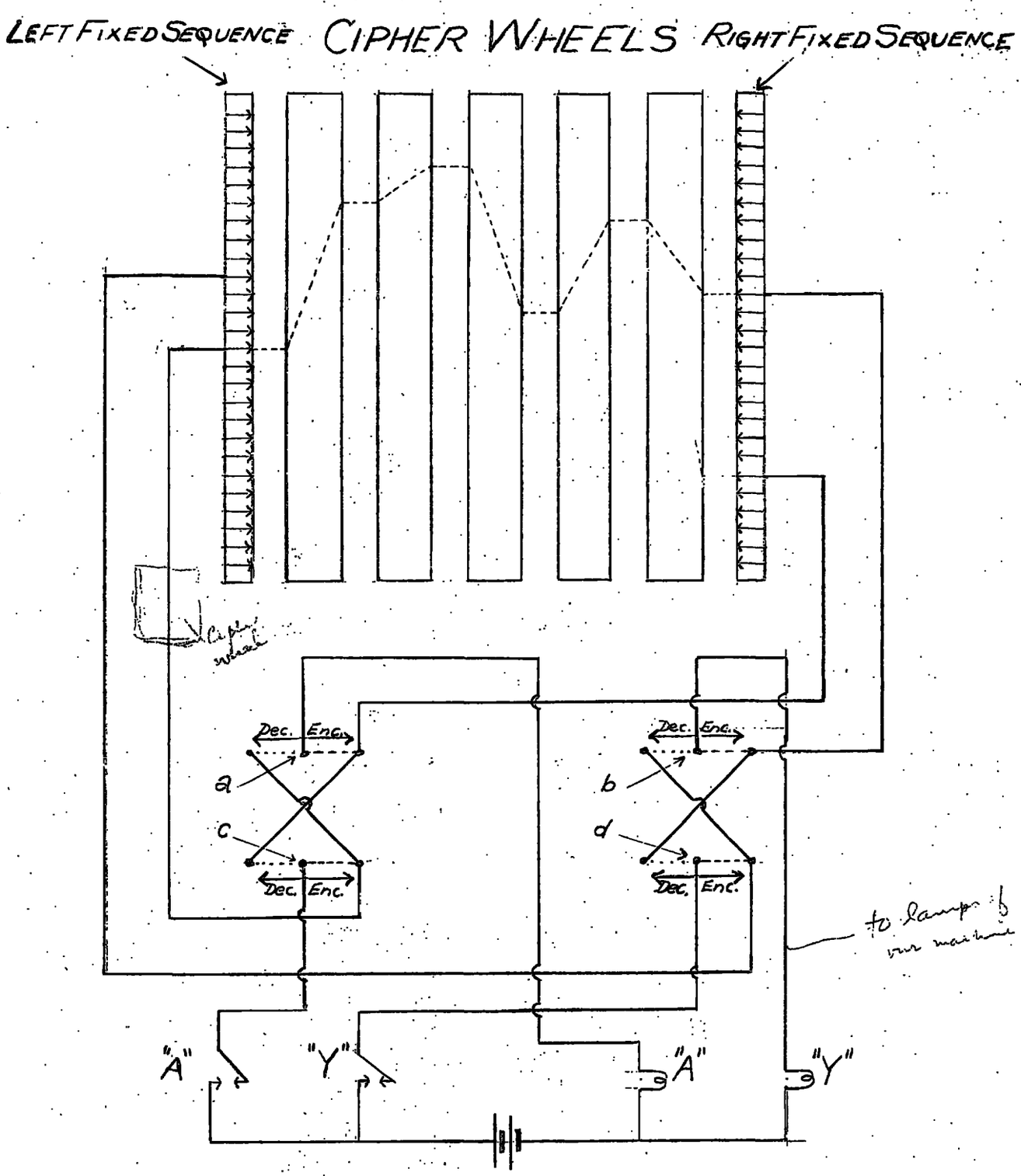

FIGURE B