IN REPLY
REFER TO
WP&T Div.

WAR DEPARTMENT
aln
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

~~CONFIDENTIAL~~

January 20, 1933

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

Attached hereto is a preliminary 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
S. B. Akin,
Major, Signal Corps.

Attached:
Report in dupl.

~~CONFIDENTIAL~~

PRELIMINARY 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) After the machine has been in operation for about an hour, the clutch governing the stopping of the cipher wheel sometimes fails to operate. The cause of this was not determined.

(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 ~~will~~, 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 keytape. This method of operation would require the use of a keytape 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 keytapes among the offices or organizations provided with the machines. If several offices use the same keytape 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 keytape 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. To circumvent these difficulties a fairly simple modification in construction can be made, as outlined below in paragraph 2 e.

2. The foregoing facts lead to the following discussion:

a. 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.

b. If a printing mechanism is added, full advantage ought to be taken of such a feature by freeing it, if possible, of limitations imposed by the cipher mechanism. By so doing the speed of operation could be increased to double or triple the present speed in enciphering or deciphering.

c. The present speed limitation 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.

d. It appears necessary to modify the machine so as to bring about by some simple, practical means a degree of cryptographic security impossible to obtain with the present model without the difficulties of tape production and distribution, as set forth in paragraph 1 c. The following scheme is the one which seems to offer the most promise.

e. If there is inserted in the set of 26 circuits leading from the keyboard to the left-hand fixed contacts of the cipher wheel a set of five cipher wheels of the Hebern type, then the same keytape of length sufficient to encipher a message of average length could be employed

repeatedly to encipher different messages, providing the set-up of the Hebern wheels were changed for each message. Each message would contain an indicator giving the complete key set-up. Means similar to that used in the present Hebern lamp machine would have to be provided to take care of the enciphering-deciphering equivalency. This is accomplished by means of a screw which juxtaposes two sets of 26 contacts for enciphering and two other sets of 26 contacts for deciphering, as per diagram B attached to enclosure. The addition of this modification would make the machine somewhat larger and heavier, but still not beyond the limits of what is feasible in a machine for use in regimental and higher headquarters.

f. Inasmuch as it seems advisable to modify the machine in respect to both speed and cryptographic security, serious consideration should be given to the possibilities of the scheme outlined in the attached description 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 keyboard, but also the degree of cryptographic security afforded by the use of but one, relatively short keytape by all communicants over a period of many days would be sufficient for communications exchanged between even the highest headquarters.

3. The following recommendations are made:

a. That the present model be given a thorough test for speed, ruggedness and reliability by submitting it to an organization such as the 51st Signal Battalion or the 1st Signal Company at Fort Monmouth, and that report thereof be made as promptly as possible.

b. That the development of a printing attachment should proceed without delay, since this attachment would be the same for the present model as for any proposed new machine.

c. That the Laboratories give further consideration to the possibility of increasing the speed of the present model and, if practicable, increase the speed to twice the present speed.

d. That if the latter turns out to be practicable of achieving, then the present model be modified in accordance with the ideas outlined in paragraph 2 e; but if it turns out to be impracticable or impossible of achieving, then consideration should be given to the development of the scheme outlined in the attached description.

William F. Friedman

Attached:
Description.