WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

8

April 15, 1937

MEMORANDUM FOR: Chief Signal Officer
(THRU: Channels)

1. Attached hereto is a brief description, accompanied by two sketches, of a proposed cipher machine invented by me in 1936. The invention as embodied in the enclosure was conceived in three successive modifications or stages which were processed through the Signal Corps Patent Board.

2. The first stage was described in a memorandum dated March 24, 1936. In its Meeting No. 2, on April 17, 1936, the Board recommended "that the invention be not considered important in the National Defense, and that a non-exclusive license to the Government, in writing, be required." This recommendation was approved by the Chief Signal Officer.

3. The second and third stages, although conceived at separate dates, were described in a single memorandum dated April 29, 1936. In its Meeting No. 3, on May 26, 1936, the Patent Board considered the second and third stages jointly and recommended "that the invention be not considered important in the National Defense and that a non-exclusive license to the Government, in writing, be required." This recommendation was approved by the Chief Signal Officer.

4. On the basis of the two actions of the Patent Board, as noted in Pars. 2 and 3 above, there would appear to be no objection to a possible sale of commercial rights to the invention. However, it is deemed advisable to call attention to the following facts.

5. One of the elements in the invention as submitted to the Patent Board in the memorandum of April 29, 1936, included a mechanico-electrical means of providing for a relatively long cipher key, this means comprising a set of cam wheels for operating a set of electrical contacts instead of a tape. This means and method of providing a key was incorporated in another invention which was described in a memorandum dated March 23, 1936, and dealt with a proposed modification in Converter Type M-134-T2. This was processed through the Patent Board also at its Meeting No. 2, on April 17, 1936. The Board found that "Whereas, the original invention (i.e., the one applicable to Converter Type M-134-T2) was not considered of such importance as to be placed in the category which provides for its being kept secret, the improvements described in the description accompanying his memorandum of March 23, 1936, to Research and Development Division,

through War Plans and Training Division, are considered as, Important in the National Defense." The Board therefore recommended "that, under the provisions of Par. 6 g AR 850-50, Dec. 31, 1934, a complete assignment be requested, and that the invention be kept secret." This recommendation was approved by the Chief Signal Officer and such assignment was promptly made by me. It should be added that as a result of a detailed discussion, with the OIC, Research and Development Division (Lieut. Colonel Colton), of the action of the Patent Board in the cases of reference, steps were taken in time to place the basic invention covering Converter M-134-T2 into the secret category also, so that both the basic patent on this converter and the patent application covering a proposed modification thereof are now in a secret status.

6. In view of the fact that the proposed cam-wheel modification of Converter M-134-T2 is in the secret category, and that a similar mechanism constitutes a part of another invention not in the secret category and forming the subject of this memorandum, I hesitate to proceed with any negotiations that might lead to the sale of commercial rights to the latter invention, until this situation is clarified and all possibility of future misunderstanding is obviated.

7. In my opinion, there is nothing novel in the use of a cam-wheel assembly for producing a cipher key and it is doubtful whether this is in itself a patentable idea. It is embodied in several cipher machines invented and constructed by commercial firms, for example, those of the International Telephone Laboratories, the International Business Machines Corporation, Hebern, Damm, and others. The <u>combination</u> of such a cam-wheel assembly with the rotating commutators of Converter M-134-T2 is perhaps novel, and patent has already been applied for as stated in Par. 5 above. First action of the Patent Office has been received recently and a copy thereof is attached. It will be seen that only limited claims will be allowed, if at all.

8. It is my belief that the outright sale of commercial rights to the accompanying invention would in no way jeopardize the secrecy or security of Converter M-134-T2 either in its present form or in a later form, should this machine be modified in future by the substitution of the cam-wheel assembly for the key tape transmitter.

9. On the basis of the foregoing facts in the case, information is requested first as to whether the Chief Signal Officer has any objections to my entering into negotiations which may lead to the outright sale of commercial rights to the invention described in the accompanying papers.

10. Reference is made to previous papers in this case: Letter dated June 16, 1936, from OIC, Research and Development Division, OCSigO, to Director, Signal Corps Laboratories, Fort Monmouth, Subject: Invention (File OCSigO 370), and three indorsements thereto.

William F. Friedman

Enclosures.

Brief Description of a Cryptographic System and Machine Employing a Single, Aperiodically-Displaced Cipher Commutator.

1. This invention deals with a cryptographic machine in which the cryptographic principle is basically as follows:

Power is delivered to the keyboard at the enciphering position at a specific instant in a period of 26 possible instants, the cipher resultant of a given plain-text letter depending therefore upon the specific instant the keyboard is made "alive", since for each of the 26 different instants a different mixed cipher alphabet is presented for encipherment. The order of presentation of cipher alphabets is regular but the exact instant of the selection of a specific cipher alphabet is very irregular and depends upon a keying factor.

2. The machine consists basically of a single, constantly rotating, 26 segment, 26 character cipher commutator, labeled 1 in Figure #1, controlled by a keying system including a set of rotatable, differential cam wheels or an equivalent electrical cam arrangement. This control system comprises 5 or a multiple of 5 cam wheels which operate contact levers, shown at 2. The inter-action of the 5 contact levers results in setting up at the 5 relays, 3, 4, 5, 6, 7, a permutation in the Baudot code. Corresponding to this permutation there is set up a permutation of 5 translater bars, labeled 8, 9, 10, 11, 12. These are slotted members and when a specific permutation is set up, one of 32 stunt bars falls into place and closes a contact. Several of these contacts are shown in the sketch at 13. These circuits lead to a switchboard 14, on one side of which there are 32 positions and on the other side of which there are only 26 positions. Referring to the cam wheels these are of different diameter and of different numbers of intervals, preferably all prime to one another. They are individually rotatable in step-wise manner, under control of the keyboard. The potential cipher key which results from such an arrangement is in length the product of the individual interval numbers of the several cam wheels. For example, if there are 5 cam wheels the first of 100 intervals, the second of 99, the third of 97, the fourth of 91 and the fifth of 89 intervals, the total length of the cipher key would be 7,777,469,700. This merely means that the cipher key would consist of an unintelligible sequence of ciphering key characters of corresponding length.

3. The 32 possible resultant Baudot permutations which are led to switchboard 14 are for the purposes of this invention reduced to 26 by consolidating 6 of the 32 circuits into the other 26, so that there will be only 26 different resultant effects for cryptographic keying purposes. In this invention this is accomplished quite simply by taking what are usually known as the 6 extra functions and throwing them in with 6 of the other 26 letter-representing Baudot permutations. Which 6 will be selected to be "double-representations" can be determined and varied at will at the switchboard 14.

4. In this invention the 26 specific effects thus rendered possible by cam action merely determine which one of 26 segments will be made "alive" (that is, will be connected to a power source) on a set of 26 segments in the distributor head 15, over which brush 16 sweeps in synchronism with commutator wheel #1. As shown in the figure, this action merely means that at a given instant relay 17 is energized, the instant of energization being controlled by the cam arrangement and will be different for each key operation at the keyboard.

5. When a specific segment of the distributor 15 is made "alive" by being connected to a power source, and when the brush 16 reaches this live segment, the keyboard of the cryptograph is made "alive" at that instant by the completion of the circuit from power source 18 at contact 19. If a key is depressed during that cycle, the letter corresponding to that key will be enciphered in the specific cipher alphabet determined by the specific angular position of the cipher commutator 1 at the instant that the brush 16 reaches the live segment on distributor 15. In other words, the keyboard is made "alive" at 1 of 26 different instants in the cycle passed through by the commutator wheel; each of these instants corresponds to a different mixed alphabet of which there is a total of 26. It is to be understood that the cam wheel assembly is set at an initial keying position by pre-arrangement and that the cams advance one step or interval per depression of the keyboard and no more.

6. The cipher commutator may be made a reciprocal cipher commutator; or by suitable switching arrangements a nonreciprocal enciphering-deciphering relationship may be provided for, if desired.

7. The keyboard 20 is connected to the lefthand stator 21, and the circuits pass from 21 through cipher commutator 1 to the righthand stator 22 and thence to the bank of indicating devices 23, back to power source 18.

8. Means and circuits must be provided to prevent the cryptograph from recording or indicating a resultant more than once for the same set up of keys, so that there may be one and only one cipher equivalent per keying operation.

9. Instead of a set of 6 translater bars and 32 stunt bars an arrangement of multiple contact relays as shown in Figure 2 at 24 may be provided if deemed more practicable than translater bars.

10. For decipherment, having a reciprocal ciphering commutator the key setting of the cam wheels being the same as the initial setting at the enciphering end the sequence of keying characters would be identical at the deciphering end and the reciprocity between plain-text and cipher characters is established through the cipher commutator and the decipherment is effected in a simple manner, that is, if at encipherment at a given instant A equals K then in decipherment at that homologous instant (with respect to the cipher key) K would be deciphered as A.