Cipher Development M-134 T-2

WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

February 27, 1934

MEMORANDUM TO: Mr. Rowe, Patent Section, Air Corps.

(Paragraph numbers refer to correspondingly numbered paragraphs on examiner's report.)

1. I see no reason for citing Dirkes et al. It has absolutely no bearing on present invention and deals only with an improvement in tape transmitters. I likewise see no reason for citing Friedman.

2. Nowhere in Hebern is a cipher-key transmitter shown. In Hebern the movements or displacements of the code wheels are purely mechanical; they are regular or periodic in character, and controlled by ratchet mechanisms internal to the device itself. In present invention these movements are controlled by the cipher-key transmitter, in an aperiodic manner, by a tape which is external to and not a part of the device itself.

3. Make it read "an electromagnet and an associated ratchet and pawl, each ratchet and pawl actuating the commutator with which it is associated, the set of commutator stepping mechanisms". . . etc., as before.

4. The examiner fails to distinguish between those parts of the mechanism which are internal to it (viz., the keyboard, commutators, cipher-key transmitter, indicating mechanism) and the external element which is the key tape itself. It is not claimed that the cipher-key transmitter is the external element; this part of the mechanism is controlled by a perforated tape; it is the latter element which is wholly external, can be removed, changed and varied at will. In all other cryptographs known to me the keying mechanism is internal to and a part of the cryptograph itself and therefore inherently presents weakness from the cryptographic standpoing that periodicity can not be prevented, since whatever the keying mechanism be (gears, cams, etc.) the parts thereof must operate upon mechanical principles embodying phase recurrences, or cycles, or periods. It might serve to clarify that which the examiner

regards as "inaccuracy in language" if the following were added at the end of Claim 6: "and which consists of a perforated tape bearing ciphering characters in a plural-unit code."

5. Re Claims 8, 9 10 - Same comment as in Paragraph 4.

6. I am not claiming Morehouse, but the combination of Morehouse with my invention. However, I would not insist on Claim 9 if examiner continues to object, but as regards Claim 10, the final clause "the numbers of such characters in the respective tapes being prime to one another" constitutes an important improvement over Morehouse, from a cryptographic point of view. Studies have showed that if these numbers are not prime to one another, the full combinatory potentialities of the respective keys cannot be realized in practice. For example, if there are two tapes, one containing 1000 characters, the other 500, then after two revolutions of the longer tape the combination of the two tapes produces a resultant which coincides with the resultant of the first revolution. In other words, instead of having a single resultant key of 1000 x 500 = 500,000 characters the resultant is actually only 2000 characters in length. In the case of keys whose lengths are prime to each other, the resultant has a latent length that is the product of their individual lengths.

7. I thought such claims were allowable, but I am willing to drop them.

8. Same comment as in Paragraph 4.

9. We can add some descriptive data in the claims, but the aperiodicity is covered in the specifications.

10 and 11. See comments above in Paragraph 4.

12. Insert "practically" before the word "non-repeating". Substitute "series" for "sequence". Add "said characters consisting of perforations permuted in accordance with a plural-unit code".

13. In next to last line of Claim 23, change the word "bars" to "keys".

I do not quite understand the examiner's objection that they fail to define the invention.

14, 15, 16. These method claims are restricted to the mechanism covered by the present invention. They make no pretense of being basic and general, but are applied to a cryptograph having rotatable circuit changers of the type described. The examiner is certainly in error when he states (16) "Obviously no changes of character or condition are effected by the practice of the alleged method". In order to appreciate the real significance of the method of achieving aperiodicity in the operation of this cryptograph he will have

to learn something of the science of deciphering without the key.

17, 18. You can best answer these yourself but I see many differences and distinctions between the claims cited. Claim 1 is differentiated from Claim 2 by the word "mechanism"; the cipher-key transmitter is one element, the mechanism controlling it is another and a separate element. Claim 12 delimits Claim 11 and is more specific. Does a claim to be valid have to cite a different use for the same element mentioned in another claim? However, I am willing to drop 11, if 12 is allowed.

William F. Friedman.