WAR DEPARTMENT

OFFICE OF THE CHIEF SIGNAL OFFICER

WASHINGTON

December 1, 1924.

Memorandum For: Commander Kingman.

1. The study to which you referred this morning was made at the informal request of your predecessor, Commander Godwin, and Lieut. Loventhal, in connection with a rather complicated cipher machine, which was being considered for use in the Naval service.

2. This investigation extended over a period of about six months, but I did not, of course, devote all my available time to it - only such as could be spared from my more immediate duties in the office.

3. The study passed through several stages. First, a careful survey was made of the type of cryptogram produced by the apparatus. This involved research into the mechanico-electrical features of the machine, many of which were novel, and resulted in producing cryptograms of considerable complexity. Detailed investigation, however, convinced me that claims for indecipherability, even of a relative nature, put forth by those interested, were not warranted, if all the factors connected with the use of the machine in the military or naval service were taken into consideration.

4. The next step was, of course, to attempt to establish a body of principles and a method of procedure for dryptanalytic reduction of the dispatches which would be produced under service conditions. In this I was successful, and satisfied myself that such reduction was not only possible but very practicable.

5. There remained, however, the question of demonstrating the truth of the various hypotheses established. A set of ten test messages was prepared by the Code and Signal Section, based upon the assumption that the enemy would know all that there is to be known as regards the machine and its functions, but would not know the wiring of the cipher wheels. The indicator word for each message, in order to enable the recipiant to set his machine properly for deciphering, was shown in clear on each message, as this would be the case in actual practice unless the system were further complicated by the use of a code book, or some other subsidiary cipher system for disguising the indicators.

6. The first of these dispatches was solved after approximately one week's intensive study of the data based on all ten messages. This length of time, however, gives no reliable index of the length of time that would be required in actual practice, because many other factors, such as personnel, volume of data, special information from general intelligence, and so on, would all have a very definite and important influence on this question, as you are well aware. I was all alone, as regards the analysis of the data, and had not the slightest idea as to what any message was about. It is my opinion that with a large, well-trained staff, and sources of outside intelligence that are usually available, the process could be accomplished within a space of time short enough

to make the analysis of messages of major importance very valuable to an enemy.

7. Regardless, however, of how long it took to solve that first message, the solution of the rest of them was made very much simpler as a result of a most interesting series of analytic steps developed coincident with the solution of the first message. In fact, it was shown that the solution of but two or three lines of text of one message was all that was necessary. This would be difficult, perhaps, depending on how much text was available, but once done, the rest follows rather easily. I do not mean to say that only two or three lines of cipher text are necessary, but that the analysis of the data based on a considerable volume of text, when applied only to two or three lines of one message, will result in the solution of those lines, and from that, the rest follows in rapid order.

8. It is necessary to say that the wiring of the plate in the rear of the machine was known to me in this test, it having been assumed that this part of the electrical arrangements would be the same for all machines. It seemed necessary, of course, to establish procedure for analysis when the latter is unknown. While no actual messages were presented for solution, on account of the lack of time and personnel, nevertheless a set of about 100 messages had been prepared some time previously, and the cipher dispatches were carefully examined in connection with their plain text, and diagrams of the wiring of the cipher wheels. The data showed that given a sufficient number of messages (the traffic of NAA for one day during active operations would be more than sufficient) solution could be achieved within a practicable length of time. I would even go so far now as to venture the opinion that it might be done with thirty or so messages.

9. Of course, with an understanding of the mechanics of the analysis, suggestions for the improvement of the apparatus, with a view to increasing the degree of secrecy, presented themselves. These, and the method of solution were communicated to members of your section.

10. I wish to take this opportunity to say that Mr. Bogle of your section rendered very valuable assistance in the way of compiling special tables, under my direction. I also wish to add that I was very glad to have had the opportunity to conduct this investigation, for I had the good fortune to develop several new principles in analysis, the value of which will no doubt manifest itself in my own work at some future time.

W. F. Friedman,
Cryptanalyst, Signal Corps.