March 9, 1936

MEMORANDUM ON CIPHER DEVICE TYPE M-138

This morning I disclosed to Lieut. Wenger, Code and Signal Section, Navy Department, my idea for a modification of the Strip Cipher Device as follows:

Arrange the device to consist of serially numbered sections of five channels each. To set up the numerical key for the day arrange the sections in serial order from 1 to 5 and insert the individual alphabets in the successive channels in accordance with the daily numerical key. Each message would begin with an indicator which would indicate arbitrarily the order in which the sections were to be assembled. This would afford 120 different sectional arrangements.

We commented upon this scheme with Mr. Rowlett being present. During the course of the discussion the question came up as to weakness introduced by the fact that the sections were always of the same number of alphabets, in this case, five. During the course of the discussion I brought up the matter of the Treasury Department Device with its 30 alphabets and noted that one of the objections to it was that while we had found it extremely difficult to match lines containing 25 letters by means of statistics based upon coincidences, it might be that with 30 letters, which gives 20% more text, the matching of lines to determine which were in the same generatrix might be much easier. I then went on to say that with an arrangement such as I propose that if the sections were interchangeable this objection to a 30-alphabet device would be eliminated and from that point on I suggested that one might have six sections of which only five would be selected according to the indicator. Continuing I said that I had given some thought to a device in which one could easily vary the number of alphabets in each section, but that I had not arrived at a practicable solution mechanically.

Lieut. Wenger then suggested that we might make the sections themselves of unequal widths. Then I said, for example, supposing that Section 1 had 3 alphabets, Section 2, 8 alphabets, Section 3, 4 alphabets, Section 4, 1 alphabet and Section 5, 9 alphabets, totaling 25 alphabets, the message indicator would indicate the arrangement of these sections for each message so that each message would have 25 alphabets but arranged in different sections. I then said something about the packing of the sections in transporting the device and being able to pack them in a pyramidal arrangement on account of the different widths of the sections. Mr. Rowlett pointed out that if one had six sections varying in widths from 4 to 9 alphabets, this would afford a total of 39 alphabets available of which an individual message would use 30 to 35 alphabets depending upon

the indicator. At the same time this would combine the advantages of the 30 alphabet arrangement which affords 720 different arrangements of six sections.

Lieut. Wenger said that he would give the proposal some thought and would talk it over with his associates. He stated that it seemed to him to have good possibilities.

William F. Friedman

William F. Friedman.

I was present at the above-mentioned conversation and, to my knowledge, the statements made in this memorandum are correct.

Frank B Rowlett

Frank B. Rowlett.