4131-539

4131-524 1919
37
WAR DEPARTMENT

September 2, 1919.

My dear Colonel Fabyan:

The Military Intelligence Division and the Signal Corps have gone over the exposition on the A. T. and T. Company cipher machine enclosed with your letter of August 21st. I wish to express to you my appreciation of the interest you have taken in this matter, and to point out some of the more important premises that you have confused.

You are correct in your statement in paragraph 3, page 4, that the unequal shifting of tapes after each message may result in "an over lap", but this is true only provided that A tape is shifted farther forward than B tape, a method that the Signal Corps has always avoided. The Signal Corps method consists in always adding to the B tape one or more numbers more than the number added to the A tape.

Referring to your statement in paragraph 5, page 5, it is A tape instead of B tape that is used as a basis for limiting the combinations to be used by different stations. It is necessary that each station begin the day's business "within bounds", but the operator never could be "out of bounds", in case of there being four stations, until he has sent enough messages to use up one-quarter of the total possible combinations. The difference between the two cipher indicators may be as great as the length of the longer tape instead of being limited as outlined in your memorandum.

The confusion concerning the manner of shifting tapes between messages outlined in paragraphs 1 and 2 on page 7 should be cleared by the foregoing. Beginning within bounds, each station after the end of each message need only add an arbitrary number of any size to B tape only or to both A and B tapes, except that A tape is never shifted forward more than B tape. These are the only restrictions.

The solution outlined in your memorandum appears to depend upon so many correct guesses of the unknown, as well as upon a coincidence of cycles, that I feel that the only satisfactory adjustment of the entire matter is for you to accept the plan outlined in General Squier's telegram to you of August 28th, in which he states that the cipher machine is in operation and that the Signal Corps is prepared to send as test messages an actual day's business from their files. We cannot question General Squier's sincere interest in this matter and the messages which will be submitted to you will, of course, have no trick encipherments.

(23)

I should like to add that as a result of your investigations of the A. T. and T. cipher, we have submitted to the Signal Corps methods for disguising the cipher indicators, which will make impossible the arrangement of the messages in correct cycles. Such an arrangement is the first and essential step in the methods of solution that you have pointed out to us.

I wish to express to you my deep appreciation for your interest in this subject, and to assure you that both the M. I. D. and the S.C. are anxious for any additional information that you may develop in the future.

Very sincerely yours,

Colonel George Fabyan,
P. O. Box 435,
Chicago, Ill.

hcm

ac.