

In replying refer to

WAR DEPARTMENT
OFFICE OF THE CHIEF OF STAFF
WASHINGTON.

April 11, 1919.

Lt. Col. Joseph O. Mauborgne,
Office of Chief Signal Officer,
Virginia & 18th Streets,
Washington, D. C.

Dear Colonel Mauborgne:

My time has been often and seriously interrupted since you called my attention to the T. and T. cipher and Colonel George Fabyan's claim that he had shown its insecurity, but I am now able to send you the following:

a) A decipherment of a large portion of message No. 4, which Colonel Fabyan, as I understand, has not yet deciphered.

b) A draft of a reply to Colonel Fabyan's presentation of his results to us through Captain Powell.

c) A draft of a letter from the Secretary of War in reply to Fabyan's letter to him, transmitting his decipherment of message No. 2.

I did not wish to reply until I had deciphered message No. 4; partly because I was interested in the problem, and partly because - having had no previous experience with the T. and T. cipher - I wished to see whether in practice it developed any weakness which did not appear in theory.

My work merely confirms the conclusions which you and Captain Yardley reached and expressed last year, namely, that two messages enciphered with the same key are easily decipherable by modern methods of attack and that a single message is absolutely indecipherable, both theoretically and practically.

The problem of deciphering message No. 4 was very interesting in two or three particulars. As you will recall, Mr. Gherardi originally informed Fabyan that "Message No. 4 utilizes a portion of the enciphering tape employed with messages Nos. 2 and 3 but extends to a character in the enciphering tape beyond the end of either of these two messages." The first problem was therefore to discover at what point in Nos. 2 and 3 No. 4 began to run parallel. As you will readily see, this

In replying refer to

WAR DEPARTMENT
OFFICE OF THE CHIEF OF STAFF
WASHINGTON.

April 11, 1919.

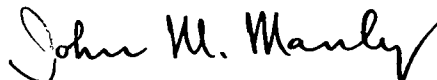
Colonel Mauborgne - 2

was not very difficult. The process is mechanical and inevitable and can be carried on by several clerks working at the same time; so that although it actually took me, working alone, about five hours to solve the problem, if there had been need of haste fifty or a hundred clerks could have got a solution in less than ten minutes.

I am especially glad that I worked on this problem, because in the course of work I developed a considerable simplification of the method of attack on two messages with the same irrational running key. It is so simple that others have no doubt discovered it before, but I had overlooked it until now. I will expound it when I see you.

The other matter of special interest was the discovery of the extent to which familiarity with the operations of the machine and a visualization of the form of the message when deciphered aided in deciphering; but this of course is not new to you. Fabyan apparently took these operation-signs as nulls.

Sincerely yours,



John M. Manly,
Captain, U. S. Army.

encls.
bbm