EXECUTIVE DIVISION
MILITARY INTELLIGENCE BRANCH
In replying refer to

WAR DEPARTMENT
OFFICE OF THE CHIEF OF STAFF
WASHINGTON.

July , 1919.

Mr. George Fabyan,
Riverbank,
Geneva, Illinois.

My dear Mr. Fabyan:

As information has reached me from various sources that you do not feel that M. I. 8 has given the result of your efforts on the A. T. & T. cipher the serious consideration that you believe it deserves, I have carefully gone over the entire file and offer the following as my views. In order that there may be no further misunderstanding, I beg you to correct anything that may seem to you incorrectly stated.

In Mr. Gherardi's letter to you of June, 1918, transmitting text messages enciphered by the A. T. & T. cipher machine, I note that he states:

> 'I am not a cipher expert and would not presume to say what can and cannot be done, but should you and Professor Friedman decipher messages Nos. 1, 5, 6, and 7, I shall feel that I owe you both a good dinner. I have no doubt that you can decipher Nos. 2, 3, and perhaps 4. These, however, as you understand are not the arrangement which we propose.'

Your letter of March 23, 1919, to the Secretary of War, expresses the opinion that the enemy can decipher messages sent in the A. T. & T. cipher, and you enclose as proof of your statement the decipherment of one of the messages sent to you by Mr. Gherardi of the American Telephone and Telegraph Company. This message, however, is No. 2, concerning which Mr. Gherardi said when he sent it to you, 'I have no doubt that you can decipher Nos. 2, 3, and perhaps 4. These, however, as you understand are not the arrangement which we propose.'

In Mr. Gherardi's letter to you of March 27, 1919, he again stated, 'The messages which you have deciphered are Nos. 2 and 3 which I stated I had no doubt you could decipher.....When you have deciphered Nos. 1, 5, 6, or 7, something will have been accomplished in breaking the system in question.'

I can find in our files no record of your having deciphered Nos. 1, 5, 6, or 7, In view of this I must agree with M. I. 8's statement and the Secretary of War's reply to you that the foregoing offers no basis other than an opinion for Riverbank's contention that the A. T. & T. cipher is unsafe.

As further confirmation of your contention that the A. T. & T. cipher is not invulnerable, in your letter of May 5, 1919, to The

Adjutant General of the Army,--subject, 'Warning to the Department for the good of the service that the A. T. & T. Company machine is not invulnerable, and does not give the security claimed for it by the Department experts,' you state in paragraph 4 that 'Captain Powell is conversant with the A. T. & T. machine cipher system and we asked him to furnish us with four messages, using that system. Captain Powell did so, under the impression that they could not be deciphered. They were deciphered within two hours, and the clear text given to Captain Powell over the long distance 'phone.'

However, in his letter of April 22, 1919, to Captain Manly, then in charge of M. I. 8, Captain Powell states that before he enciphered the messages referred to you named the conditions and method of encipherment. I beg to quote from his letter:

> 'Colonel Fabyan asked me to encipher four test messages by means of two arbitrary keys of as many letters as I pleased, the second key to be one letter less than the first and the messages to be of sufficient length to contain <u>three cycles of the two keys</u> ..... and ..... 'I was also requested, <u>contrary to what I believed to be the custom in actual practice</u>, to return to the first letter of the upper key, when beginning the encipherment of the second and succeeding messages.'

This gave you a variation of the real problem under discussion. The variation you were able to decipher within two hours; the real problem you have not been able to decipher after nearly one year's effort. Success in two hours and failure in one year spells the difference between incorrect and correct encipherment.

If you will consider the foregoing I feel sure that you will see nothing personal; as stated in your letter of May 5, 1919, to the Adjutant General, in M. I. 8's refusal to consider as important the decipherment by Riverbank of messages made to order and admitted by Captain Powell to be enciphered in a manner 'contrary to actual practice.'

After all, if the enemy were attempting to decipher our messages, he would not be in a position to dictate to us just how they should be enciphered. As a matter of fact Mr. Gherardi gave you more information than I should be willing to admit would be in the hands of an enemy. He wrote approximately five hundred words explaining the method of the encipherment of each message, the operation of the machine, the number of characters in the alphabet, the system of operation of the two running keys, and even enclosed a copy of the alphabet itself, which can be changed as can the key. To assume that

the enemy has all this information is to assume that he has an agent in the code office, and an enemy agent in the code office will cause no end of embarrassment no matter how, or by what system, the cables are enciphered.

You have now had Mr. Gherardi's test messages since,July, 1918, I appreciate the time and labor you have devoted to this cipher, but in justice to the Department experts I must state that it seems to me that you have proved nothing not already known to them.

The form of code or cipher the Department has used, is using, or will use in the future, I consider a very dangerous topic for public discussion. Personally I do not approve of The American Telephone & Telegraph Company's detailed explanation of this cipher. The alphabets, the keys, the length of the keys, and the operation of the keys, should not and will not in the future, if my recommendations are approved, be known to anyone unless in the employ of and in the control of the War Department. If disclosed disciplinary action should be taken.

I can readily understand your letters regarding the responsibility you feel in this matter. In order that you may no longer feel any further responsibility, I consider myself justified in telling you, though as already stated I do not believe that information of this sort should be divulged to anyone not controlled by the War Department, that since shortly after the armistice of last November the use of the A. T. & T. cipher was discontinued. This I shall ask you to consider confidential.

M. CHURCHILL,
Brigadier General, General Staff,
Director of Military Intelligence.

jcm