S

141 East 37th Street,
New York, July 21, 1922.

Dear Moorman:

Regarding your note of the 19th I spent one evening looking over the cipher messages and the alphabets enclosed in your letter of July 6th. I have made no reply as I expect to be in Washington the first of next month and thought that I would wait until I came to discuss the matter with you and, if possible, Commander Gresham of the Navy.

Although I have had no time actually to attempt to read the messages I presume that the 50 alphabets are joined together making 25 alphabets of 52 characters, and that these alphabets are then used in some modified method of the Bazerie cylinder which we are now using in the Army. I presume that, after enciphering a number of letters as we do with the Bazerie cylinder, one sends the letters in the horizontal lines in one of the three following methods: (1) any line as we do in the Bazerie cylinder, (2) a line indicated by the key, or, (3) a line automatically indicated by an open shutter.

If my presumptions are at all correct the method of attacking the cipher is the same as attacking the Bazerie cylinder with a few modifications.

Of course I am not prepared to state whether the cipher is indecipherable or not, but if my presumptions are correct I rather think that with the information at hand the messages could be read. As you are

(Major Moorman)



of course aware the method of attacking the Bazerie cylinder is a long and tedious one and we have not the time here to try to work puzzles unless there is some profit in it. If Commander Gresham is really desirous of learning the strength and weakness of his cipher I should think that he would be willing to turn over the machine to us (if he presupposes that the enemy already have the 50 alphabets there is no reason that I can think of why he should not presuppose that they either have the machine or understand how it works). Of couurse there are a thousand and one different ciphers that are indecipherable if the cryptanalyst has not any information as to the method and without this information this cipher might very well be one of them. If Commander Gresham does not care to go into the matter further it might be well to show him the Bazerie cylinder and to tell him of the different precautions that we would take in time of war to make the decipherment of the messages more difficult. I would also suggest, in order to impress upon him the difficulty of making an indecipherable cipher, that even with the precautions we are prepared to take, we would not maintain that the messages could not be read. Our only point is that the information would be of no value by the time the messages were read on account of the length of time it would take to read them.

(Major Moorman)



I shall be in Washington the first of next month and I should be only too glad to discuss the cipher with you and Commander Gresham and if he is willing to give us all the information that we presume that the enemy has in our use of the Bazerie cylinder, I shall be glad to make every effort to find time to work on the messages enclosed in your letter of July 6th.

Very sincerely yours,

H. O. YARDLEY

HOY-jcm

Major Frank Moorman, G. S.,
Military Intelligence Division,
Washington, D. C.