3 East 38th Street,
New York, Sept. 15, 1919.

Brigadier General M. Churchill, U.S.A.,
Director of Military Intelligence,
Washington, D. C.

Dear General Churchill:

I have your letter of September 9th with enclosures requesting that I state frankly and fully my idea of Colonel Fabyan's suspicions concerning Colonel Mauborgne's motives.

I doubt Colonel Fabyan's sincerity in this matter, but in order to point out how the decipherer is very often sincerely suspicious of the encipherer of problems, I wish to state briefly the charge that was once made against me by a Lieutenant in the Navy, who at that time was the Navy cipher expert. When I explained to him how messages in a running key could be solved, he asked that I submit him several messages in a running key. I turned the work over to a clerk and sent the cipher to Lt. Smith without even knowing the content. He deciphered the message and in his letter of transmission, which I am unable to find, charged me with a deliberate effort to make the message indecipherable. His charge was that in the cipher of two hundred letters there were three places where the running key and the text stopped at the same point. In my reply I told him that I had had nothing to do with the preparation of the cipher, but that inasmuch as the average length of English words was approximately five letters, according to the law of averages when two lines of English were written without space one above the other the words of each line should end at the same place every twenty-five letters, or at eight points in two hundred letters; that inasmuch as there were only three such places in my test message the problem was three times as easy as it should have been according to the law of averages. I make this point to show how prejudiced the decipherer very often becomes.

My opinion of Colonel Mauborgne can best be explained by reciting briefly some of my experience with him. For a period of two or three years before the war Colonels Mauborgne and Hitt had advertised through the Signal Corps an invulnerable method of using the U. S. Army cipher disk, namely the running key. The running key is a key that is not composed of a group of letters or a word but of a paragraph or a page of some book that is as long as the message to be enciphered. This affords a key that never repeats and was believed by Mauborgne and Hitt to be indecipherable.

I talked to Mauborgne about this in October, 1917. I told him I believed I could decipher messages enciphered in a running key. He laughed at me good-naturedly, saying that he and Hitt had tried it; that I would find when I began to attack the messages that I would get all sorts of things. The cipher bureau immediately began work on a method of solution and it was not until December 1, 1917, that Mauborgne finally submitted test messages. On December 6, I returned to Mauborgne the decipherment of the messages he had

submitted. The letter of transmission is quoted verbatim:

" December 6, 1917

"Major J. L. Mauborgne,
Signal Office, Land Division,
Room 722, Mills Annex.

Dear Major Mauborgne:

"I am enclosing herewith decipherments of the six messages in the same running key enciphered with the U. S. Army cipher disk, that you submitted to the Cipher Bureau.

"In three of the messages you start with proper names; in the entire six messages and key you use only one conjunction, two infinitives, four prepositions, and two adverbs.

"Of course I don't wish to say that this is an unfair problem but I do wish to call your attention to what I mentioned in our conversation; namely, that being an expert cryptographer, you do, unconsciously, select very difficult and unusual passages of "English"!

"Cordially,

1st Lt., Signal Corps, U.S.R."

Please note that in paragraphs two and three of my letter I complain of the sort of language Mauborgne used. I have since learned by experience that the problem was a fair problem, for in the field one can never be certain that messages are in the same key or in the same cipher, as far as that is concerned, and the intercepting stations usually garble the messages about ten per cent. So far as the language is concerned, it was only Saturday that we decoded a message about the shipment of bananas!

In judging Colonel Mauborgne's action when he received this letter, it should be remembered that he and Hitt were responsible for the use of the running key in the Army. He did not wait to write me but called immediately by telephone, was profuse in his congratulations and begged that I immediately submit a memorandum to the Chief Signal Officer of the Army stating that the running key was unsafe and should be discontinued at once. This I did and the Chief of Staff cabled Pershing to discontinue its use unless the cipher was modified with a transposition. Unfortunately I have no copy of the memorandum in my files. You can probably find it in the M. I. D. files.

Colonel Mauborgne like any other cipher expert is very firm in his opinions, but when shown that he is in the wrong is only too glad to admit it and ask for improvements for the benefit of the service. Both Captain Manly

and I have a very deep affection for Colonel Mauborgne, because of his frankness and willingness to accept suggestions for changes in Signal Corps methods.

While mentioning the running key I wish to add another paragraph that has nothing to do with Colonel Mauborgne but which will give you briefly all the facts regarding this particular subject. I think it was in October or November, 1917, that Captain Powell left Riverbank and stopped in Washington for a few days before sailing for Europe. He was asked at this time what Riverbank knew about the solution of messages in the running key, and he replied that Riverbank knew nothing, that Riverbank had never worked on messages in the running key and did not even know that Mauborgne and Hitt had recommended its use to the Army. In the latter part of October General Pershing asked for four code and cipher experts for intelligence duties and the cipher bureau immediately began to select out of some twelve students four suitable men. During the period of training these men were instructed in the methods of solution of the running key and when they went to Riverbank, at Colonel Fabyan's suggestion for further instruction, they explained to Riverbank our methods of solution. I have it from one of the men that when they arrived at Geneva, Riverbank knew nothing about the running key.

This is an absurd falsehood. F

I am enclosing herewith a Riverbank publication entitled "Methods for the Solution of Running-Key Ciphers", on the fly-leaf of which you will find a note to Colonel Van Deman dated March 17, 1918, and signed George Fabyan. You will find also a reprint of a letter to Fabyan dated January 18, 1918, signed by Mr. Friedman, who at that time was a civilian. I quote the letter herewith:

"My dear Colonel Fabyan: January 18, 1918"

Note this date! The mss. was written months before - probably in September if not earlier.

"I have the honor to transmit to you Publication number 16, of the Department of Ciphers, "Methods for the Solution of Running-Key Ciphers."

"Concerning the possibility of the decipherment of a message or a series of messages enciphered by a running-key, it was said until as recently as three months ago, "It can't be done" or "It is very questionable." It is probably known to you that the U. S. Army Disk in connection with a running-key has been used as a cipher in field service for many years, and is, to the best of our knowledge, in use today. I suppose that its long-continued use, and the confidence placed in its safety as a field cipher has been due very probably to the fact that no one has ever taken the trouble to see whether "It could be don." It is altogether probable that the enemy, who has been preparing for war for a long time, has not neglected to look into our field ciphers, and we are inclined

credit him with a knowledge equal to or superior to our own. We have been able to prove that not only is a single short message enciphered by the U. S. Army Disk, or any similar device, easily and quickly deciphered, but that a series of messages sent out in the same key may be deciphered more rapidly than they have been enciphered!

"Hence, since not destructive but constructive criticism is the purpose of the Department, we have earnestly endeavored, by pointing out the defects of the old system, to show how the same may be remedied, and how the system may be made more trustworthy. The final paragraphs of this book state our conclusions, gained from the results of our investigations.

"It is our hope that this booklet will be a source not only of interest to you, but of active benefit in these times when the fate of nations is more than ever dependent upon effective means of secret communication.

"Very respectfully,

W. F. FRIEDMAN,
Director.
Department of Ciphers, "

I shall not discuss this deliberate steal for it is already a Riverbank scandal (the next steal, as I have already pointed out to you, will be of methods developed by the service in the A. E. F.), but I do wish to point out the manner in which they submitted their information to the War Department. Friedman states in paragraph two of the above letter that as far as he knows the method is being used in the army and notes in the last paragraph that "It is our hope that this booklet will be a source not only of interest to you [Fabyan] but of active benefit in these times when the fate of nations is more than ever dependent upon effective means of secret communications." As a matter of fact the Signal Corps and the A. E. F. had been informed that messages enciphered in the running key were unsafe, but Friedman and Fabyan did not or pretended they did not know that its use had been discontinued. Instead of informing us in secret about the "fate of nations", Colonel Fabyan publishes, copyrights, and dedicates a copy to Colonel Van Deman!

But I have got off of my subject, but feel the foregoing may help you to form an opinion.

When I was in Washington the week before Labor Day Colonel Mauborgne took me to the Signal Corps office and showed me the A. T. & T.

cipher machine in operation which had been put up especially to encipher messages for Colonel Fabyan. I heard him give instructions to the Lieutenant in charge how messages for Colonel Fabyan should be endiphered. He merely told the Lieutenant to go to the Signal office, take from the files a day's business and bring the messages back and encipher them just as if he were sending them officially to Hoboken. He did however tell him to change the dates of the messages for he feared some effort on Colonel Fabyan's part to obtain the original text from the files of the Signal Corps.

It is a psychological fact that the decipherer is always suspicious of the encipherer but Colonel Fabyan's charge against Colonel Mauborgne is in my opinion entirely unjustified. It is merely another example of Riverbank's methods.

As you asked that I discuss this subject frankly, I have felt free in the foregoing to call things by their right names.

Very sincerely,

H. O. YARDLEY,
Major, U. S. A.

1 encl.