CRYPTOLOGIA July 1995 Volume XIX Number 3

RIVERBANK LABORATORY CORRESPONDENCE, 1919 (SRH-050)

From the archives
Background by Louis Kruh

This document is preceded by the following memo, dated 5 May 1947, from William F. Friedman to a Lieutenant Fawcett.

> A blast out of the past. Guess should go in hist files.
>
> This turned up recently – I forget where. Have made some notes on one letter of HOY's [Herbert O. Yardley].

Background to the correspondence: In 1917-1918, Gilbert S. Vernam at AT&T invented the Printing Telegraph Cipher, which AT&T and Army Military Intelligence officials deemed indecipherable. After watching a demonstration at AT&T's New York offices, George Fabyan, owner of Riverbank Laboratories and William F. Friedman, Director of Riverbank's Department of Ciphers, claimed its messages could be solved.

Other key individuals named in the correspondence include: General Marlborough Churchill, chief of the Army's Military Intelligence Division; Colonel Joseph O. Mauborgne (later General and Chief Signal Officer), head of the Signal Corps Research and Engineering Division; and Major Herbert O. Yardley, head of the Cipher Bureau, MID, in New York.

The DeYaub cipher mentioned by Fabyan is an early name given to the U.S. Army Cipher Device M-94 by Mauborgne. The designation comes from the three letter pairs, DA YA UB, which Mauborgne had to use twice instead of only once, when he improved the mixed alphabets proposed by its inventor, Parker Hitt.

Fabyan's reference to Mauborgne's actions with the M-94 probably refers to the first 25 letters of each of the 25 messages enciphered by the device that Mauborgne sent to Riverbank for solution, as a way of testing its security. Friedman (and Yardley, who was also sent the messages) was unable to decrypt any of the messages. Later it was found that they contained unusual and exotic words, e.g., "Phenols are Benzole derivati(ves)."

According to Ronald Clark's *The Man Who Broke Purple*, (Boston: Little, Brown and Co., 1977), shortly after the correspondence on the Printing Telegraph Cipher, which follows, "the cipher tapes of about 150 messages selected from a single day's traffic were sent from Washington to Riverbank on October 6 [1919]." After working on the ciphers for up to twelve hours a day for six weeks without success, Friedman asked his staff to check whether any errors had occurred in transcribing the punched tapes into characters on paper. It was found that a character had been completely omitted and within days of that discovery the cipher was broken.

The correspondence is revealing in many respects and Yardley's ego-driven blunt style, and animosity toward Riverbank, is evident. Some 28 years later, however, Friedman makes sure that Yardley's charges are deftly countered with his own comments for the use of future researchers and historians.

*

GEORGE FABYAN
CHICAGO

PO BOX 435 SEPTEMBER 2, 1919.

Dear General Churchill:

I sent you a copy of the letter we sent to the Signal Corps which will explain itself. I don't want to bother you but I think it is a matter of courtesy to keep you informed. The point of the whole thing is that Riverbank is of the opinion that the Signal Corps do not want the cipher broken and the hit bird flutters. It is entirely possible to use the cipher machine in an impractical sort of a way and get out messages which it would be most difficult to decipher. Our past experience is that Colonel Mauborgne will do the same thing with the cipher machine as he did with the DeYaub Cipher and that is, put in some extra refinements to put one over on Riverbank and this is not our idea of co-operation.

I want to thank you for the disposition shown towards Riverbank and you can rest assured that the Senators and Congressmen whom I know, will be informed as occasion offers in regard to the purposes of a General Staff as compared to a bunch of bureaus with drawers that stick.

If you happen to run across that crippled bugler who can bugle and who would appreciate a good home and lots of work, will you kindly ship him C.O.D. to

Sincerely Yours,

To General Churchill,
Woodward Apartment,
2301 Connecticut Ave.,
Washington, D.C.

GEORGE FABYAN
CHICAGO

Sept. 6, 1919.

Dear General Churchill:

I carefully note letter of September 2nd, over your signature. There is no more guessing in Cryptography than there is in Algebra. "Guessing", is undignified - "assumption", sounds lots better.

I don't question the sincerity of any of the General Officers but some of the subordinates have made us dance without giving us a chance to select the tune, but I suppose we will forget it some day.

If Riverbank had invented a cipher and I had put myself on record that it was indecipherable and had been awarded the D.S.M. and had the cipher printer especially mentioned in the citation and my boss had been made the Knight of St. George and St. Michael on account of the machine printing across the ocean, I doubt if I would be very enthusiastic about anybody proving that "my doll was stuffed with sawdust" and I think I very likely would put as many obstacles in their way. I enclose copy of a message sent us by Mauborgne sometime ago, which we never tried to work on because it was not long enough and yet, when he was here, he said we had no right to jump at any conclusions as to the number of cycles or the length of the message. He knew at the time, we wanted three complete revolutions of the tape and left us to infer that this message covered that and confirmed it when he was here.

I wish, if possible, someone in the M. I. D. could ascertain in regard to this and see if the message is not less than one cycle and for that reason, impossible to decipher.

I don't understand why Mauborgne don't send us the messages. The machine has been set up for over three weeks and yet, he cannot send us two hours work but asks for one delay after another, which Riverbank construes as trying to get another scheme to work out.

Sincerely yours,

To General Churchill,
Woodward Apartment,
2301 Connecticut Ave.,
Washington, D.C.

WAR DEPARTMENT
OFFICE OF THE CHIEF OF STAFF
WASHINGTON

September 9, 1919.

My dear Yardley,

I enclose two letters from Colonel Fabyan and my answer, both of which are included in one letter, dated today.

Please send me a memorandum explaining frankly and fully exactly what your idea is of Colonel Fabyan's suspicions concerning Colonel Mauborgne's motives.

In eighteen years' service in the Army, I have never yet come across a genuine case in which an officer, who was in any way representative of the Regular Army, has permitted himself to be influenced by the ulterior motives assigned to Colonel Mauborgne by Colonel Fabyan. Colonel Mauborgne's frank manner in discussing the matter with me gives me an additional reason for believing that the suspicion is entirely unjustified; but I should like to have you throw a little light on it.

I do not think it advisable to have Colonel Mauborgne learn through us that Colonel Fabyan feels this way, but I do think it very essential that ill feeling and suspicion be removed.

I enclose a draft which you prepared concerning the general question of publication, and also a copy of my letter to Colonel Fabyan on the same subject.

Very sincerely yours,
M. Churchill.
Brigadier-General, General Staff,
Director of Military Intelligence.

Major H. O. Yardley,
No. 3 East 38th St.,
New York, N. Y.

*

September 9, 1919.

My dear Colonel Fabyan:

During my visit to Riverbank, we discussed the general question of publication in connection with codes and ciphers.

Colonel [Ralph H.] Van Deman has returned from France, and after a month's leave will be here in Washington. If you can see your way clear to come to

Washington some time after October 9, I should like very much to have you see M. I. D. as it now functions, and also to have the opportunity of discussing with General [Dennis E.] Nolan, Colonel Van Deman and myself the general subject of publicity. Obviously, peace-time conditions are not war-time conditions and certain modifications of our policy are inevitable. But it will always be desirable, I think, to keep from other nations any information which would lead them to have any particular respect for our methods of cipher attack, or which would give allied nations any cause for offense in connection with the publication of notes which they had entrusted to us.

Very sincerely yours,

Colonel George Fabyan,
PO Box 435,
Chicago, IL.

*

September 9, 1919.

My dear Colonel Fabyan:

I desire to acknowledge your letters of September 2nd and 6th, and to express my regret that in our letter of September 2nd the word "assumption" was not used in place of "guess". I assure you that the word "guess" was not used with any unpleasant connotation.

I will do everything in my power to obtain the information you request in your letter of September 6.

Very sincerely yours,

Colonel George Fabyan,
PO Box 435,
Chicago, IL.

*

Colonel George Fabyan, etc.

My dear Colonel Fabyan:

The subject of the conversation I had with you while I was at Riverbank has been on my mind from time to time, but it was not until today that I was able to give it further consideration. You will recall that you asked whether Lt. Friedman had my permission to insert in his manuscript anything that he desired, and without foreseeing at the time exactly what this question involved, I stated that I had no objection.

The information about codes and ciphers collected at our General Head quarters in France was the result of a liaison with our Allies and of the combined efforts of some fifty officers, field clerks, and enlisted men who for the period of the war devoted their time to the breaking of enemy codes and ciphers.

As this information is not the result of the efforts of one man, but of the efforts of the Services of France, England, Italy and the United States, in justice to our Allies, to the men and to our Service, I feel that if this information is compiled or published, it should be compiled, published, and issued by the service whether for limited or wide circulation.

In arriving at this decision, I have your interests in mind as well as my own, for besides being a reflection on the Service, it might by some be interpreted as a reflection on Riverbank which would be put in a position that might lend color to an intimation that it was assuming credit for work done by the Service, a position that both of us wish to avoid.

This opens up the entire subject of publication and distribution which I feel should be settled. The Military Intelligence Division will continue to remain silent about codes and ciphers. We may lose some publicity by our silence, but I am concerned with results only.

But I do not want you to feel bound to our policy. I shall offer no objection to Riverbank publications even though we remain silent; in fact, now that conditions have changed I wish to withdraw my objection to the distribution of the Riverbank publications held during the war.

The disposition of these and future publications I feel however should be made by Riverbank rather than MID, for we cannot refuse to publish and consent to distribute and maintain a consistent policy.

I have a report from Major Yardley that your latest exposition on the A T & T is highly interesting, but that he has not been able to reach a joint conclusion with the Signal Corps.

Very sincerely yours,
MC

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 [Parker] 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 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 [John] Manly and I have 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 [J. A.] 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 [John J.] 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.[1] I have it from one of the men that when they arrived at Geneva, Riverbank knew nothing about the running key.

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[2]"

"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

[1] "This is an absurd falsehood," is pencilled in here in Friedman's handwriting and signed with his characteristic "F."

[2] In Friedman's handwriting here is, "Note this date! The ms. was written months before - probably in September, if not earlier."

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 done." 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 to 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 those times when the fate of nations is more than ever dependent upon effective means of secret communications.

"Very respectfully,
W.F. FRIEDMAN,
Director.
Department of Ciphers,"[3]

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

[3] Pencilled in with the initial "F" as the signature here is, "What happened is what often happens – people working in the same field and not in contact are likely to make similar discoveries about the same time. I'm sure MI-8 had their solution – but so did Riverbank, independently, conceived and worked out some weeks before MI-8 did it."

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 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 enciphered. 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.