

Riverbank Laboratories
Geneva, Ill.

Department of Ciphers

Sept. 24, 1919.

From: George Fabyan, 160 W. Jackson Blvd., Chicago, Illinois.
To: The Chief Signal Officer of the Army, Washington, D. C.
Subject: Printing Telegraph Ciphers.

1. Your communication of September 19th, with enclosures as stated, was received. Diligent, conscientious work, consistent with the importance of other work we have on hand, will be made on the problems presented and the result, if any, reported to its source.


GEORGE FABYAN.

RECEIVED
1919 SEP 26 AM 9 33
OFFICE
CHIEF SIGNAL OFFICER

WAR DEPARTMENT
Office of the Chief Signal Officer
Washington

(25)

Engineering
and Research

19 September, 1919

The Chief Signal Officer of the Army

Colonel George Fabyan, Geneva, Illinois

Printing Telegraph Cipher

1. With reference to our letter of September 2nd, there are forwarded herewith one hundred and thirty-five cipher tapes prepared from the total number of messages actually sent in one day by the four stations of the Printing Telegraph System now operated by the Signal Corps between Washington, Norfolk, New York City and Hoboken.

2. All these tapes have been prepared by the use of one set of key tapes. In this case one fourth of the A key tape was allotted as the limit for each station.

3. A small number of typographical errors have been found in some of the messages, but as these were actual incidents of the day's transmission they are enciphered exactly as they existed. They have not been introduced to add difficulty to the encipherment. In order to be assured that no trick or unusual encipherment was entered into, an uninterested officer was called in to verify this fact by actual observation of the method used as demonstrated by the decipherment, in his presence, of the messages being sent you.

4. This office retains exact copies of the cipher tapes forwarded to Riverbank as well as the original English tapes, the key tapes, and the page proof sheets usually made during the encipherment.

5. One message was so long that it required six sheets to print it, hence parts of this message are to be found on six separate tapes enciphered in accordance with the existing Signal Corps traffic rules. [It is to be noted that all the messages are enciphered exactly as prescribed in the copy of operating rules furnished to you by Lieutenant Colonel J. O. Mauborgne upon his last visit to the Riverbank Laboratories] and that no attempt has been made to disguise the cipher

WAR DEPARTMENT
Office of the Chief Signal Officer
Washington

-2-

indicators. However, it is to be noted that, in all future work of the Signal Corps with this cipher machine, the cipher indicators will be sent in enciphered code so as to prevent the arrangement of the messages in cycles, which is understood to be the basic requirement in the system developed by the Riverbank Laboratories for the attack on the Printing Telegraph cipher.

6. It is to be regretted that the meager office force now on duty with the Cipher Printing Telegraph System and its constant employment on official business make it necessary to send the messages to you in the original tape form instead of being translated into English characters with suitable substituted figures for the so called "stunt" signals. One advantage, however, which will accrue is the fact that when the work is done by your own force, errors in transcribing which might otherwise occur will be eliminated.

[7.] The outcome of this experiment will be awaited with great interest, as will any further information which you may develop about this cipher which might be taken advantage of in the future.]

George O. Squier,
Major General,
Chief Signal Officer.

1st ind.

jom:ho

O.C.S.O., September 11, 1919 - To Director, M. I. D.

1 civil
4131-626
24
1919

1. Returned, acknowledging receipt of cipher indicator code which is approved, and which will be used in all future work with the cipher machine in question.

WAR DEPARTMENT

2. Precaution will be taken to see that the three key alphabets for enciphering this code are changed as often as the key tapes and that the instructions for the use of this code are carried out to the letter.

George O. Squier,
Major General, U. S. A.,
Chief Signal Officer.

31
5
17

~~CONFIDENTIAL~~
MILITARY INTELLIGENCE ~~SECTION~~ Division

In replying refer to

4131-526
O.C.P.B.

WAR DEPARTMENT
OFFICE OF THE CHIEF OF STAFF
WASHINGTON.

encl
4131-526
23
WAR DEPARTMENT

September 2, 1919.

From: Director of Military Intelligence.
To: Chief Signal Officer of the Army.
Subject: American Telephone and Telegraph Cipher Machine.

1. I am informed that recently Lieutenant Colonel Joseph O. Mauborgne, Signal Corps, of your office, and Major H. O. Yardley, U. S. Army of the Code and Cipher Section of this Division, have been in consultation regarding some means of disguising the cipher indicators that precede messages enciphered in the A. T. and T. Cipher Machine. A practice of sending these indicators en clair makes it possible under certain circumstances for the enemy engaged in the solution of intercepted messages to arrange the messages in cycles. All the methods of solution of this cipher known to the Military Intelligence Division are possible only when messages are placed in correct cycles.

2. With a view of preventing the solutions obtainable as indicated above, enclosed herewith is a proposed A. T. & T. Cipher indicator code to be used for encoding cipher indicators. This code is prefaced with full instructions both for encoding cipher indicators and for enciphering the code groups.

3. It is recommended that this cipher indicator code be brought to the attention of Colonel Mauborgne for his consideration with a view, that if approved, in future should the A. T. & T. Cipher Machines be taken out of storage and used again, the cipher indicators be encoded in the proposed A. T. & T. cipher indicator code, and that the three alphabets for enciphering this code be changed as often as key tapes.

M. Churchill
M CHURCHILL

jvk

Brigadier General, General Staff.

~~XXXXXX~~ DivisionMID
JOHN M DUNN

4131-526

RECEIVED
SEP 2 1919

AUG 29

4131-526

22

WAR DEPARTMENT

SEP 2, 1919.

From: Director of Military Intelligence.

To: Chief Signal Officer of the Army.

Subject: American Telephone and Telegraph Cipher Machine.

1. I am informed that recently Lieutenant Colonel Joseph O. Mauborgne, Signal Corps, of your office, and Major H. O. Yardley, U. S. Army of the Code and Cipher Section of this Division, have been in consultation regarding some means of disguising the cipher indicators that precede messages enciphered in the A. T. and T. Cipher Machine. A practice of sending these indicators en clair makes it possible under certain circumstances for the enemy engaged in the solution of intercepted messages to arrange the messages in cycles. All the methods of solution of this cipher known to the Military Intelligence Division are possible only when messages are placed in correct cycles.

2. With a view of preventing the solutions obtainable as indicated above, enclosed herewith is a proposed A. T. & T. Cipher indicator code to be used for encoding cipher indicators. This code is prefaced with full instructions both for encoding cipher indicators and for enciphering the code groups.

3. It is recommended that this cipher indicator code be brought to the attention of Colonel Mauborgne for his consideration with a view, that if approved, in future should the A. T. & T. Cipher Machines be taken out of storage and used again, the cipher indicators be encoded in the proposed A. T. & T. cipher indicator code, and that the three alphabets for enciphering this code be changed as often as key tapes.

M CHURCHILL

jvk

Brigadier General, General Staff.

MEMORANDUM FOR CHIEF SIGNAL OFFICER OF THE ARMY.

Subject: Am.Tel. & Tel. Cipher Machine.

1. The Mil.Int.Divn, is informed that the cipher indicators that precede messages enciphered in the A T & T Cipher Machine, indicating the exact position of the two Cipher Key tapes, are sent en clair.
2. Such a practice makes it possible under certain circumstances for the enemy, engaged in the solution of intercepted messages, to arrange the messages in cycles. All the methods of solution of this cipher known to Mil.Int.Divn, are possible only when messages are placed in correct cycles.
3. Enclosure one, is a proposed "A T & T Cipher Indicator Code" to be used for encoding cipher indicators. This code is prefaced with full instructions both for encoding cipher indicators and for enciphering the code groups.
4. It is recommended that should the A T & T Cipher machines be taken out of storage and used again, the cipher indicators be encoded in the enclosed "A T & T Cipher Indicator Code" and that the three alphabets for enciphering this code be changed as often as key tapes.

M.Churchill.

3 East 38th Street,
New York City.

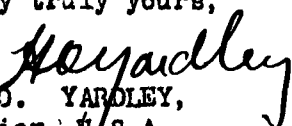
Colonel John M. Dunn,
Chief, Positive Branch,
Military Intelligence Division,
Washington, D.C.

My dear Colonel Dunn:

Referring to my letter of August 20th to General Churchill, telling of my recent visit to Riverbank, and Colonel Mauborgne's request for a method of disguising the cipher indicators of the A.T. & T. cipher, I enclose herewith memorandum to the Chief Signal Officer, together with a proposed "A T & T Cipher Indicator Code" which is prefaced with appropriate instructions.

I respectfully urge that this memorandum be sent directly to the Chief Signal Officer as a recommendation, rather than through the Chief of Staff and the Adjutant General as a positive instruction, inasmuch as the entire procedure in this cipher is tentative. If it is necessary in order to conform with army practice that the memo. be sent through the Chief of Staff, I urgently request that I be informed before any action is taken. Will you kindly send me a copy of your memorandum as it goes to the Chief Signal Officer.

Very truly yours,


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

3 ENCL.

Engineering
and Research

2 September, 1919

The Chief Signal Officer of the Army

Colonel George Fabyan, Geneva, Illinois

Cipher Printing Telegraph Messages

1. Acknowledge receipt of your telegram in answer to our telegram of August 30th, and also your letter of August 31st, which requests the encipherment of all the messages sent in one day by all the stations of the Signal Corps' machine telegraph service now in use in the United States.

2. The idea in suggesting that we use a complete day's business was, first of all, to obviate the necessity of writing a considerable number of fictitious messages; and, secondly, it is believed that by this method the messages will be more typical of actual army work, more concerned with messages pertaining to the service of Supply than to tactical movements.

3. We will, therefore, accept your condition and give you, within a few days, a day's business consisting of about one hundred and fifty messages of representative length and text. Unfortunately, as we are handicapped by lack of office force, we will be unable to translate the tapes into written form. Instead we will send you actual tapes such as you would have taken off the line with your tapping instrument, marking the beginnings of the tapes so that that will present no difficulty, and we will have to rely upon your generosity to provide the personnel to translate the punched characters into written letters and figures.

4. With reference to your statement that "you would like to have Colonel Mauborgne's opinion on the theoretical aspects of the solution as elucidated in Addendum 1 to the original presentation" - Colonel Mauborgne states that his views have, in effect, been presented in the letter of the 29th of August, 1919, signed by General Churchill, which was prepared after a consultation between Major Wardley and Colonel

Mauborgne. You undoubtedly have received that paper by this time, and no doubt have noted the exceptions taken to some of your underlying premises. He believes that nothing further need be added at the present time, and is consistent in his belief that no matter how much theoretical demonstration may be presented, your solution depends upon so many correct guesses as well as upon so many other coincidences that the only satisfactory adjustment of the entire matter is for you to actually break some messages prepared by the Signal Corps, which, up to the present time, has never been done.

5. Your work, however, as Colonel Mauborgne points out, has been of inestimable value to the Signal Corps because it has pointed out at least two salient points which will be taken advantage of by the Signal Corps. The first is that, in future work with this machine, cipher indicators should be coded. Secondly, your development of the overlapping feature resulting from the use of key tapes having a total number of characters such that the number on one tape may be divided without remainder into the number on the other tape, or that the number on both tapes may be divided by the same number, will prove of decided advantage in the selection of the length of key tapes. These two features alone, regardless of other features which may develop as your work progresses, have proved of immense value to the Signal Corps and I take this occasion to express my thanks not only for the expenditure of time, labor and money which you have made on this cipher, but also on the other ciphers submitted to you in the past by the Signal Corps. It is to be trusted that you will continue to give to the Signal Corps Riverbank's heartiest co-operation and you may be assured that your efforts will always be reciprocated.

6. We expect to be able to furnish you the messages you desire within a week and trust that you will concentrate your efforts on the practical work of deciphering them.

George O. Squier,
Major General,
Chief Signal Officer.