COPY

Subject Cipher Printing Telegraph Systems.

AMERICAN TELEPHONE AND TELEGRAPH COMPANY

BELL SYSTEM

DEPARTMENT OF DEVELOPMENT & RESEARCH

195 Broadway,

New York, October 26, 1925.

Major General Charles McK. Saltzman,
Chief Signal Officer of the Army,
Washington, D.C.

My dear General Saltzman:

As you know, we undertook during the war to develop fast and accurate methods for enciphering and deciphering telegraph messages, making use of printing telegraph apparatus. The arrangements proposed turned out to have such merit, and were used by the Signal Corps in this country and preparations were made for rather extensive use in France.

It has seemed to me that the work which was done in this connection and the results which were obtained would make a suitable paper for presentation to the American Institute of Electrical Engineers, and with that in mind the one attached hereto has been prepared, with the thought that it would be presented at the national convention of the American Institute of Electrical Engineers to be held in New York early in February.

The paper, as you will note, is, in the main, of a descriptive character and deals almost entirely with the features of the particular system which has been worked out.

Before going any further with the matter I should appreciate receiving your comments on the proposal to give such a paper and, if you see no objection to its presentation, to have the benefit of such detailed comments in regard to the text as you may be willing to make. Some time ago when Captain Friedman was here I spoke to him about the matter, and gathered from what he said that he thought such a paper would be timely and helpful.

In connection with this development we had some helpful comments from some of the Signal Corps people, and I want to be sure that full credit is given for their help; also for the recent improvements which have been suggested by Captain Friedman since the system was worked out.

In the event that the paper is presented it would be our plan, I think, to have some equipment and to make a demonstration, as I think such a demonstration would be very interesting to the members of the Institute.

As papers for the February convention should be in the hands of the Meetings and Papers Committee early in December, I should be obliged to you if you would let me have your comments at an early date, and I trust you will be entirely frank both as to the wisdom of presenting such a paper and as to any comments concerning the material therein.

With kindest regards, I am,

Very sincerely yours,

L. F. Morehouse,
Equipment Development Engineer.

Attached:
Draft of paper, "Cipher Printing Telegraph Systems for Secret Wire and Radio Telegraphic Communications."

RDP-BMW

Notes on A. T. & T Co's. Paper on
Cipher Printing Telegraph Systems for Secret
Wire and Radiotelegraphic Communications.

---

1. It is suggested that the designation "U.S. Signal Corps" be changed to "Signal Corps, U.S. Army."

2. Several times in the paper the apparatus, system, and method are referred to as being "secret", and reference is made to sending messages secretly. To be ~~technically~~ technically accurate, it is not the apparatus, system, method, or actual transmission which is secret, since the latter are fully described in the letters patent covering the details concerned them, and are therefore available to the public. The point is that the messages produced by the system are secret. One of the requirements of a cipher system suitable for use in the military service is that there be no secrecy about the method or apparatus. See Par. 75b, page 114, Signal Corps Training Pamphlet No. 3, copy of which was sent some time ago to Mr. R. D. Parker ~~which you have~~.

3. Page 11. To telegraph engineers who are familiar with the rules regarding word count as applying to telegraph or cable communications, ~~and rates~~, but not with the principles of cryptography, the distinction between code and cipher, as stated, will appear to be unusual and perhaps faulty. The distinction as stated is strictly true in the technical cryptographic sense, and the distinction made in commercial practice had its origin in this cryptographic difference, but it has become obscure in recent years. In commercial count, messages are regarded as being in code if the words are (1) real dictionary words taken from one of eight authorized languages or (2) artificial words that are pronounceable

In other words, the secrecy feature is inherent not in the apparatus or methods, but in the cryptograms produced by them.

The qualifying phrase "having a secret meaning" is a bit ambiguous, but is used to distinguish groups of figures or letters that are common commercial abbreviations, such as CIF, FOB, etc., from groups of figures or letters having a secret significance in the cryptographic sense.

according to the current usage in these eight specified languages; cipher messages are those in which either groups of figures or unpronounceable groups of letters having a secret meaning are employed. It is obvious that cipher systems, as correctly defined, can produce pronounceable or genuine words only by accident, whereas code systems employing artificial ~~words~~ groups can be designed to produce pronounceable "words" ~~groups~~ regularly. It might be well to add that the present distinction employed in the telegraph and cable administrations has led to such great practical difficulties in the interpretation and application of the rules that a revision of the latter, toward clarification and simplification, forms the subject of much discussion at the International Telegraph Conference now in session at Paris. I might also add in passing that in my opinion cipher systems and apparatus will never supplant or even become real competitors of code systems in the commercial world until the present rules and rates for cablegrams are modified to reduce the advantages which the code count now has over the cipher count in cablegrams. This is because two code groups, if combined in one ten-letter group that is "pronounceable", can be sent and are charged for as one word in a cablegram. Thus, a code ~~telegram~~ cablegram, even one in which each plain text word is merely replaced by a five-letter code word, can be sent at half the cost of a cipher ~~telegram.~~ Cablegram. When one further considers the abbreviating or con-~~cending~~ condensing ~~of~~ features of code, where a phrase of three or four words, or even a long sentence can be represented by a single code word of five letters, the handicap that cipher systems encounter is most striking. Perhaps the use of rapid, efficient, and inexpensive cryptographic apparatus will reduce this handicap to a considerable extent, because of the saving in time and labor in the preparation of cryptograms, and in their reduction to clear text upon their receipt.

cablegram, provided the code words are pronounceable according to the definition adopted

4. Page 20. The statement that the double-key system can be used "without appreciably reducing the secrecy of the system" ~~is~~ considerably underestimat~~ing~~es the degree of success that the expert cryptanalyst may have in attacking messages prepared in this way as compared with the case wherein a single non-repeating key is used.

5. Page 24. May it not be worth while to include a mention of the services rendered by the Cipher Department of the Riverbank Laboratories, Geneva, Illinois, in connection with the tests to determine the degree of secrecy? These tests were ~~of a semi-official~~ in character and were made at the request and with the cooperation of this ~~Signal Corps~~ Office; the expense connected with the test ~~to a considerable sum of money~~ was entirely borne by Col. George Fabyan, the head of the Riverbank Laboratories. He is the director of the cipher department at the time this investigation was conducted, with a staff of four able assistants,

W. F. FRIEDMAN,
Cryptanalyst, ~~Signal Corps.~~ O.C.S.O.

I was fully aware of the not inconsiderable sum of money that it involved, and for this reason I suggested that Col. Fabyan's patriotism may well be commended. deserve to be mentioned in connection with the commendation of the services rendered by Signal Corps personnel.