SUBJECT Cipher Printing Telegraph System.

AMERICAN TELEPHONE AND TELEGRAPH COMPANY

BELL SYSTEM

DEPARTMENT OF DEVELOPMENT AND RESEARCH

195 BROADWAY

NEW YORK February 13, 1926

Major William F. Friedman,

Office of the Chief Signal Officer,

Washington, D. C.

My dear Major Friedman:

As requested in your letter of February 10, I am sending you a number of additional copies of Mr. Vernam's paper on "Cipher Printing Telegraph Systems." I shall be glad to furnish more copies if you should need them.

With kindest regards, I am,

Sincerely yours,

G. S. Vernam

Attached:
6 Copies of Paper
on "Cipher Printing
Telegraph Systems."

GSV:CB

Cipher Printing Telegraph Systems
For Secret Wire and Radio Telegraphic Communications

BY G. S. VERNAM[1]
Associate, A I E E

Synopsis.—*This paper describes a printing telegraph cipher system developed during the World War for the use of the Signal Corps, U. S Army. This system is so designed that the messages are in secret form from the time they leave the sender until they are deciphered automatically at the office of the addressee. If copied while en route, the messages cannot be deciphered by an enemy, even though he has full knowledge of the methods and apparatus used. The operation of the equipment is described, as well as the method of using it for sending messages by wire, mail or radio.*

The paper also discusses the practical impossibility of preventing the copying of messages, as by wire tapping, and the relative advantages of various codes and ciphers as regards speed, accuracy and the secrecy of their messages.

* * * * *

Introduction

THE purpose of this paper is to discuss briefly certain methods for obtaining secrecy in connection with messages sent by wire or radio telegraphy, and to describe in particular printing telegraph cipher systems that were developed for this purpose during the World War.

The desirability of obtaining secrecy in telegraphic communications and the possible advantages of a system that would be capable of sending messages in such form as to be entirely secret, and which at the same time, would be more rapid and accurate than the codes and ciphers ordinarily used, were brought out in conversations with officers of the Signal Corps, U. S. Army. These discussions made it evident to the engineers of the Bell System that it would be very helpful if the well-known automatic features of the printing telegraph art could be made available for enciphering and deciphering telegraph messages, and could at the same time be made practical for use under service conditions.

The engineers recognized that printing telegraphs[2] were rapid and accurate, but were not secret except to the extent that their signals could not be read from a telegraph sounder. With the general requirements for secrecy systems in mind, studies were made of printing telegraph systems to determine how their messages could be made secret. The result of this work was the development of a cipher system that is capable of rendering messages entirely secret, is rapid and accurate, and is practical to use.

This "Cipher Printing Telegraph System" was called to the attention of the Signal Corps. The Signal Corps became very much interested, tested the secrecy of communications handled by the system and tried it out between New York and Washington. This trial proved that the system could be successfully used to send messages secretly and at a speed many times faster than by methods previously in use.[3]

Each message is automatically enciphered at the sending station and deciphered in the same manner at the receiving station. The method of ciphering will be described later in this paper and is such that under certain conditions of use, the messages are rendered entirely secret, and are impossible to analyze without the key, even if it is assumed that the enemy can capture a machine, learn its method of operation in all details, and intercept a large number of messages.

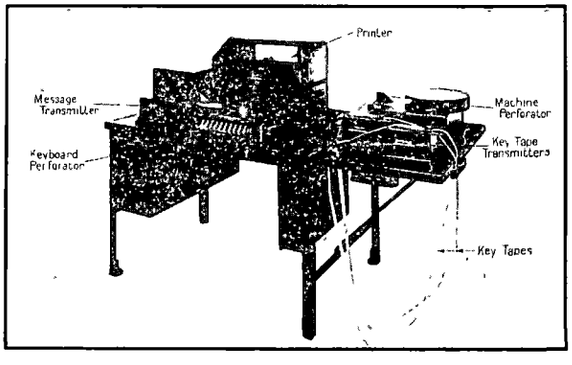

FIG 1—CIPHER PRINTING TELEGRAPH MACHINE

Flexibility of System

This method of ciphering can be used with machines of various types. The electrically-driven machine shown in Fig. 1 was developed during the war particularly for the Signal Corps, U. S. Army. In order to save time in production, standard printing telegraph parts were used wherever possible with the result that this machine has the appearance of a "start-stop" printing telegraph set with some additional units mounted on a shelf at the right end of the table. This type of cipher set is particularly suitable for handling large amounts of traffic at high speed.

1. Engineer, Dept Development and Research, Am Tel & Tel Co

2. See John H Bell, "Printing Telegraph Systems," TRANS. A. I. E. E. for 1920, Vol XXXIX, Part 1, p 167, and A. H. Reiber, 'Printing Telegraph Systems Applied to Message Traffic Handling," TRANS A I E E for 1922, Vol XLI. p. 39

To be presented at the Midwinter Convention of the A I E. E., New York, Feb 8-11, 1926

3 Note See page 140, "Report of the Chief Signal Officer to the Secretary of War" for the year ending June 30, 1919

If something smaller in size and portable is required, the machine shown in Fig. 2 may be used. This machine is light and strictly portable as no electric current is required for its operation. It is slower than the large machine and requires a knowledge of the standard "Baudot" printer code (see Fig. 8) on the part of the operator, but its messages are equally secret.

These machines are considered suitable for general use by government departments, business concerns,

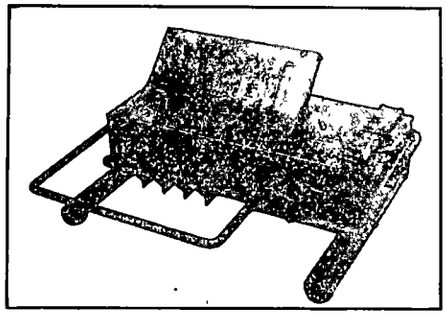

FIG. 2—PORTABLE CIPHER MACHINE

etc., for handling confidential messages rapidly and secretly. The method of using them can be varied to suit conditions and so as to make unauthorized decipherment as difficult as may be necessary up to the point where it becomes impossible even for an expert cryptanalyst.

If an appreciable demand exists for machines of special sizes or having particular operating features for special uses, these can be built to employ the same secrecy principle. For example, the functions of ciphering and transmitting over a telegraph circuit can be combined in one machine, if desired, so that, at the sending station, messages can be simultaneously enciphered and transmitted over the telegraph circuit, and so that, at the receiving station, messages can be received, deciphered automatically and printed directly in plain text; thus avoiding the slight delay caused by separately enciphering and deciphering each message. This method is particularly suitable for cases where the cipher equipment can be directly connected to a telegraph line or to a radio transmitter and receiver and can be operated by the same personnel.

RUIYW TGCZG PIETY RJGUA ELKEJ EZIAO
ISCFE LCXHF CONEC XELVY DXJBT WFEJM
HLGDL DDPYD TPGVQ EZAYI LXSZX

FIG 3—SAMPLE CIPHER MESSAGE IN PRINTED FORM

If the cipher messages are to be turned over to a telegraph or cable company to transmit, they should be in written or printed form. For this purpose, the cipher machine can be arranged to print the cipher messages in groups of five letters each, spaced to form "words." Fig. 3 is a copy of such a message shown exactly as it was prepared by the cipher set. Such messages can be printed by the machine directly on the telegram blank with the address and signature in plain English, and if desired, a carbon copy can be made at the same time for record purposes.

PREVENTING ACCESS TO MESSAGES

There appear to be two general methods for securing secrecy in connection with communications, namely, (1) by preventing or at least attempting to prevent access to the messages or to the lines of communication and, in the case of telegraphic communications by rendering the lines incapable of being tapped, and (2) by the use of codes and ciphers with key systems known only to the proper parties.

As regards wire tapping, sensitive alarm devices arranged to operate on small changes in the electrical constants of the line circuit, are unsuccessful as a means of preventing unauthorized parties from obtaining access to the circuit. The electrical condition of a long telegraph circuit is continually changing as a result of variation in temperature and other weather conditions. This fact limits the useful sensitivity of any such alarm devices, whereas by using vacuum tube amplifiers, a record of the signals passing over a circuit can be obtained without appreciably disturbing the line circuit and even without actual contact with the wire.

Telegraph systems have been invented, that will operate successfully on very small line currents, and which use coils and condensers to suppress the harmonics in the signal impulses, or in other words to avoid sudden changes in current value. The currents induced in neighboring circuits by such a system would be small, so that it would be rather difficult, if ordinary methods are used, to obtain a record of the signals by their inductive effect. This can be readily done, however, if modern vacuum tube amplifying equipment is used. It is also obvious that a record can be easily obtained if the wire is tapped.

Many attempts have been made to obtain secrecy during the actual transmission of telegraph messages by making them unintelligible. In one system of this sort, successive signal impulses are sent alternately over two line wires by means of a rotary switch which puts the sending key in connection first with one wire and then with the other at each movement of the key. At the receiving end, the impulses are combined through one relay. With this system, the messages may be readily copied if both wires are tapped, and it is quite possible to decipher the messages even if only one wire is tapped.

Proposals have also been made to use complex devices or methods, or so to mutilate the normal impulses that they become unintelligible to anyone tapping the line circuit or intercepting the signals if sent

by radio. Any secrecy system of this general class can be readily "broken" by anyone having a knowledge of the methods used and the ability to assemble and operate the necessary apparatus.

Tapping Duplex and Multiplex Circuits

It has also been considered that a full duplex circuit or a multiplex printer circuit, in which messages are being transmitted simultaneously in opposite directions, could not be tapped and that circuits of this character insured secrecy to the communications thus being handled. This is not true, however, and means have been invented by which a message originating at one station of an ordinary duplex circuit can be tapped at any part of the circuit, even though a second message is also going over the same circuit simultaneously in the opposite direction. This means that a multiplex printer circuit, in which as many as eight messages, four in each direction, are handled simultaneously, may be tapped and a person who is familiar with the system can readily analyze the multiplex impulses to distinguish between adjacent channels and the letters of each message in each channel.

An arrangement for tapping a duplex circuit is shown in Fig. 4. A single sensitive polar relay may be used to receive the signals from either end of the circuit, or by using two such relays, the signals in both directions may be read simultaneously. Each relay may control a sounder or a suitable recording device. One winding of each relay is connected in series with the line, the other winding being connected in a circuit from line to ground through an "artificial line" composed of adjustable resistances and condensers. The line winding of each relay should have relatively few turns and should be of low resistance, the other winding having a large number of turns. Each artificial line should be adjusted to be substantially equivalent to the impedance of the corresponding section of line including that of the terminal station equipment multiplied by the ratio of turns of the relay windings.

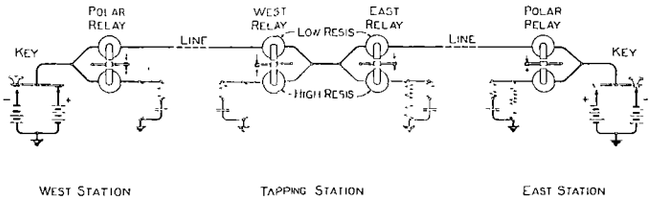

Fig 4—Method of Tapping a Duplexed Line

Signals transmitted from the west station will pass through the line windings of both relays at the tapping station, a small part of the signal currents also going through the lower windings and artificial lines to ground. The signal currents pass through both windings of the west relay in series, the magnetic effects of the two windings aiding each other, so that the armature of this relay will follow the signals. The same signals pass through both windings of the east relay in parallel, the magnetic effects opposing and balancing so that this relay does not respond to signals from the west station.

In a similar manner, signals from the east terminal station will energize the east relay but not the west relay at the intermediate station, so that by using suitable recording devices associated with each relay, a copy of signals in both directions may be obtained.

Tapping A Multiplex Circuit

This method may be used to tap a multiplex printer circuit, in which case a tape record of the form shown in Fig. 5 will be obtained. If this is taken from a "double-duplex" circuit alternate letters must be read as indicated, to get the message from either channel. Every third or every fourth letter must be chosen if the circuit is operated by the "triple-duplex" or "quadruple-duplex" method. The individual letters are in the ordinary five-unit printer code, the polarities of alternate signals being reversed. To decipher such a tape, it should be divided into units of five dot lengths each. The correct starting point can be found in not more than five trials and can be recognized by the fact that the letters of each message then form sensible combinations.

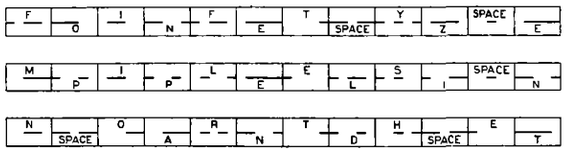

Fig. 5—Tape Record of Multiplex Printer Signals

Codes and Ciphers

Secrecy, in connection with telegraphic communications, is usually obtained at the present time by means of codes and ciphers, the term "code" being applied in cryptography to the method in which entire words, or phrases of a message are replaced by arbitrary groups of letters or numbers usually printed in a code book, identical copies being kept by those using the code, "cipher" referring usually to a system in which the individual letters of a message undergo a change either in arrangement or nature.

It is obvious that the combinations of letters in a cipher message will not form pronounceable groups or genuine words except occasionally by accident, but "code" systems can be arranged to use pronounceable artificial "words" or actual dictionary words, if desired. This is usually done, as such "code words" are handled by the telegraph and cable companies at a cheaper rate than the unpronounceable so called cipher "words."

Each of these two general systems has advantages and disadvantages which cause them to be used for

certain classes of work, depending upon the conditions. The code system has the outstanding advantage, especially for commercial work, of enabling messages to be shortened so that the tolls are reduced, and it is chiefly for this reason that commercial codes are used. Code is not very accurate, as a mistake in a single code group or even a single letter may change the meaning of an entire message, or necessitate its repetition. If secrecy is required, it is necessary to use carefully guarded private code books, the maintenance of secrecy and accuracy during the printing and distribution of which may cause great trouble. Such books must be carefully used to maintain secrecy, and must be immediately replaced, sometimes at great expense and inconvenience if they should become compromised.

Ciphers, in general, are slower than codes unless machines are used, but then they may be very much faster. They are more accurate, and depending on the system used, cipher messages may be more or less secret than code messages.

There are two general classes of ciphers, known respectively as transposition ciphers and substitution ciphers. In the first class, as the name suggests, the letters of the original message are rearranged, according to a definite system, and in the second class, substitutions for the original letters are made according to some prearranged key. In one, the relative positions of the letters are changed and in the other, the letters themselves.

Transposition Ciphers

A transposition cipher may be distinguished from a substitution cipher by a study of the frequency of occurrence of the letters of the message by comparison with a frequency table of the language of the original message. Studies which we have made of the frequency of the different letters of the English language as they occur in telegrams sent over our private wires, indicate that they are used about as shown in Fig. 6. It is apparent that some letters are used very frequently, the vowels a, e, i, o, u, forming approximately 40 per cent. of the total, e being the most commonly used letter of all. [4]This chart is similar to those used by cipher experts.

In a transposition cipher the letters must be rearranged according to a definite system known to the receiving correspondent. Those who make a study of ciphers tell us that such systems are usually easy to discover, particularly if a considerable number of messages are intercepted including two or more of exactly the same length. Transposition ciphers are not suitable for use with machines.

Substitution Ciphers

In substitution ciphers the order of the letters remains unchanged, but for each letter is substituted its equivalent in one or more cipher alphabets. For example, using the table below, for each letter in the plain text alphabet we may substitute its equivalent in the cipher alphabet. To decipher, this process is reversed.

Plain Text–A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher –F Q R U K A H G Z S E M L Y P O B C J V D T X W N I

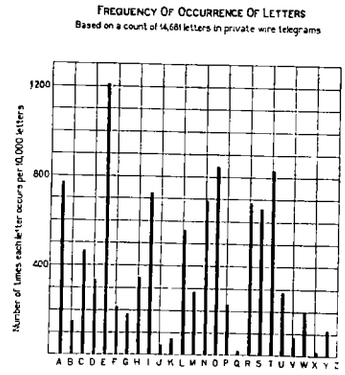

Fig. 6

If a chart is prepared from a frequency count of the letters in such a cipher message, it will have the general appearance of Fig. 6 but the crests will correspond to different letters. Messages of this type are readily deciphered by an expert even when a "mixed" alphabet

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	E	G	F	R	A	C	B	Q	M	J	K	Z	I	O	N	Y	H	D	U	W	S	X	T	V	P	L
B	G	N	Q	T	O	H	A	F	X	L	P	J	S	B	E	K	C	W	M	D	V	U	R	I	Y	Z
C	F	Q	R	U	K	A	H	G	Z	S	E	M	L	Y	P	O	B	C	J	V	D	T	X	W	N	I
D	R	T	U	J	E	K	W	X	P	D	F	N	Y	L	Z	I	V	A	S	B	C	Q	G	H	M	O
E	A	O	K	E	D	S	N	Y	V	R	C	W	X	G	B	Q	P	J	F	Z	U	I	L	M	H	T
F	C	H	A	K	S	J	Q	B	L	F	D	I	Z	P	Y	N	G	U	E	X	R	W	V	T	O	M
G	B	A	H	W	N	Q	L	C	S	Z	Y	G	M	E	O	V	F	T	I	R	X	P	D	U	K	J
H	Q	F	G	X	Y	B	C	O	J	I	N	P	T	K	H	L	A	V	Z	M	W	R	U	D	E	S
I	M	X	Z	P	V	L	S	J	W	H	T	F	A	Q	U	D	N	Y	G	K	O	E	I	B	R	C
J	J	L	S	D	R	F	Z	I	H	A	U	B	Q	T	W	X	M	E	C	N	K	Y	O	P	V	G
K	K	P	E	F	C	D	Y	N	T	U	A	X	W	H	Q	B	O	S	R	I	J	Z	M	L	G	V
L	Z	J	M	N	W	I	G	P	F	B	X	T	C	D	R	H	S	O	Q	L	Y	V	E	K	U	A
M	I	S	L	Y	X	Z	M	T	A	Q	W	C	G	U	V	R	J	P	B	H	N	O	K	E	D	F
N	O	B	Y	L	G	P	E	K	Q	T	H	D	U	W	A	F	I	Z	V	J	M	S	N	X	C	R
O	N	E	P	Z	B	Y	O	H	U	W	Q	R	V	A	G	C	K	L	X	T	I	M	J	S	F	D
P	Y	K	O	I	Q	N	V	L	D	X	B	H	R	F	C	T	E	M	W	P	Z	G	S	J	A	U
Q	H	C	B	V	P	G	F	A	N	M	O	S	J	I	K	E	Z	X	L	U	T	D	Y	R	W	Q
R	D	W	C	A	J	U	T	V	Y	E	S	O	P	Z	L	M	X	R	K	G	F	H	B	Q	I	N
S	U	M	J	S	F	E	I	Z	G	C	R	Q	B	V	X	W	L	K	D	Y	A	N	P	O	T	H
T	W	D	V	B	Z	X	R	M	K	N	I	L	H	J	T	P	U	G	Y	O	Q	C	A	F	S	E
U	S	V	D	C	U	R	X	W	O	K	J	Y	I	N	M	I	Z	T	F	A	Q	E	B	H	G	L	P
V	X	U	T	Q	I	W	P	R	E	Y	Z	V	O	S	M	G	D	H	N	C	B	L	F	A	J	K
W	T	R	X	G	L	V	D	U	T	O	M	E	K	N	J	S	Y	B	P	A	R	F	Z	C	Q	W
X	V	I	W	H	M	T	U	D	B	P	L	K	E	X	S	J	R	Q	O	F	G	A	C	N	Z	Y
Y	P	Y	N	M	H	O	K	E	R	V	G	U	D	C	F	A	W	I	T	S	L	J	Q	Z	B	X
Z	L	Z	I	O	T	M	J	S	C	G	V	A	F	R	D	U	Q	N	H	E	P	K	W	Y	X	B

Fig. 7

is used, such as that illustrated above in which the letters of the cipher alphabet are not in the usual alphabetic order.

By using more than one alphabet, the cipher may be made more difficult to "break." The method may

4. See "Manual for the Solution of Military Ciphers" by Lt. Col. Parker Hitt.

be described by referring to the "cipher square" shown in Fig. 7. In this table, the top alphabet represents the plain text, while below it are shown 26 cipher alphabets, each designated by a "key" letter given in the left-hand column. Some form of key, usually a word, is used, the letters of this key word designating the alphabets and the order in which they are to be used. A different cipher alphabet is used in a repeating manner, with each successive letter of the message.

This type of cipher may be distinguished by the fact that the frequency chart is rather flat, the frequency of occurrence of all letters being roughly the same. Each cipher alphabet is used repeatedly at regular intervals. By first finding this interval and then studying each alphabet separately, messages of this type can be deciphered readily by an expert.

Running Key Ciphers

If the key used with this type of cipher is made very long, so that it never repeats and if any portion of this key is never used for more than one message, the operation of "breaking" the cipher becomes very much more difficult. If, now, instead of using English words or sentences, we employ a key composed of letters selected absolutely at random, a cipher system is produced which is absolutely unbreakable.

This method, if carried out manually, is slow and laborious and liable to errors. If errors occur, such as the omission of one or more letters, the messages are difficult for the recipient to decipher. Certain difficulties would also be involved in preparing, copying and guarding the long random keys. The difficulties with this system are such as to make it unsuitable for general use, unless mechanical methods are used.

Cipher Printing Telegraph System

By using machine methods, this type of cipher may be made practicable for use. Fig. 1 is an illustration of the cipher machine previously referred to, and which operates on this principle. As previously mentioned, this machine was developed during the recent war and adopted by the Signal Corps, U. S. Army.

Certain parts of this machine are the same as those used for ordinary printing telegraphs, such as those described in recent papers before the Institute. For this reason, it will not be necessary to describe in detail the parts which are commonly used in such systems, such as the keyboard perforator, the transmitters, and printer.

Cipher Machine—Method of Operation

The messages are first punched in a paper tape by means of the keyboard perforator. The code used is shown in Fig. 8. This is the well-known five-unit printing telegraph code. Each letter is represented by a small feed hole and one or more larger holes which may be punched in five different positions across the tape. Since in each of these five positions a hole may or may not be punched, there are $(2)^5$ or 32 possible different combinations in this code of which 26 are used to designate letters, the other 6 representing the so-called "stunts," which are the "space," "carriage return," "line feed," "figure shift," "letter shift," and the "blank" or "idle" signal.

The cipher "key" may take the form of another tape of similar form having characters punched in it at random and with every tenth character numbered, so that the tape may be set to any designated starting position. The key tapes are prepared in advance, the original key being perforated by hand, as by working

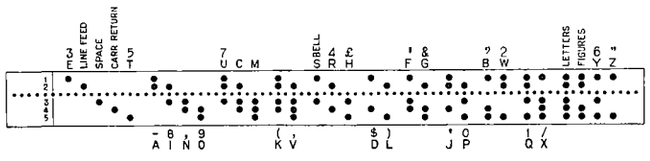

Fig. 8—Tape Showing Printing Telegraphic Code

the keyboard at random, additional copies being made automatically by the machine.

The message tape is passed through a unit known as a transmitter, where the holes in the tape serve to control the positions of five contact levers, each of which makes contact with either of two bus-bars. The key tape controls the contacts of a second tape transmitter. The contacts of the two transmitters are connected to a set of five magnets or relays as shown in Fig. 9. Each magnet will be energized if the correspondingly numbered contacts of the two transmitters are against opposite bus-bars, but not if they are ma-

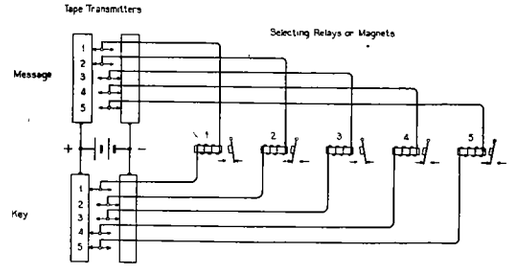

Fig. 9

king contact with similar bus-bars. In the diagram, contacts 1 and 2 of the message transmitter, are against the left or positive bus-bar, this setting representing the letter *A*. Contacts 1, 4 and 5 of the key transmitter are against the positive bus-bar, representing the letter *B* in the printer code. This will energize magnets 2, 4 and 5, which combination represents the letter *G*.

All of the possible combinations resulting from various characters in the two tapes might be shown in a cipher square similar to that of Fig. 7 except that it would have 32 characters on a side instead of 26.

The characters of the cipher messages, formed in this

way, may be recorded as perforations in a third tape. For this purpose a "machine perforator" is used. This device is similar in many respects to a keyboard perforator and is shown in Fig. 10. The tape, from a reel on the top of the machine, passes through the punch block at the front left corner of the machine. Here it passes under a die plate and over a group of six punches, which may be forced up through the tape by the action of an electromagnetic hammer. Five of these punches are too short to be acted on directly by the hammer and are pushed through the tape only when an individual "selecting finger" is interposed between the punch and hammer. The five selecting fingers are actuated by five magnets which may be controlled by the relays shown in Fig. 9. A ratchet-operated star-wheel feeds the tape forward after each character has been punched.

The cipher message tape prepared in this way is unintelligible in form and may be sent to the receiving station by messenger or by mail, or if desired, it may

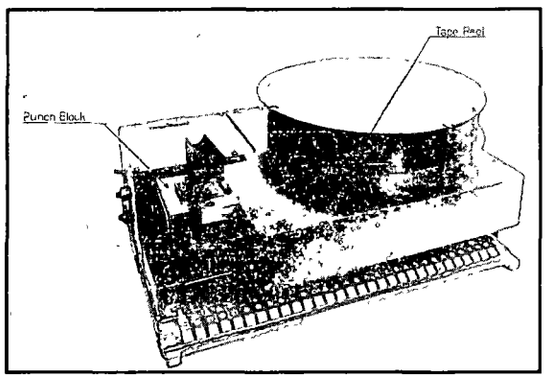

FIG. 10—MACHINE PERFORATOR

be transmitted by wire or radio and reproduced by another machine perforator at the receiving point. The cipher tape is there run through the message transmitter, where its characters combine with those of a duplicate key tape to reproduce the original message, which will be printed out in page form and in "plain text."

LENGTH OF KEY TAPE

With the system as described above, the key tape must be at least as long as the sum of all the message tapes used with it, as the messages will lose their secrecy to some extent if the key tape is used repeatedly. The use of a short repeating key may give sufficient secrecy for some uses however.

A roll of tape eight inches in diameter contains about 900 feet of tape and would serve to encipher about 18,000 words counting five printed characters and a space per word, without repeating the key. If sent at an average speed of 45 words per minute this number of words would require 400 minutes or nearly 7 hours to transmit.

In order to reduce the amount of key tape required for handling large amounts of traffic, the "double key" system was devised. In this system two key tapes are used, the ends of each tape being glued together to form a loop preferably about seven feet in circumference. The tapes should differ in length by one character or by some number which is not a factor of the number of characters in either tape. A separate transmitter is used for each tape, and the characters of the two key tapes are combined, by a method similar to that shown in Fig. 9, with those of the message tape to form the cipher message.

The result is the same as though the two key tapes were first combined to produce a long single non-repeating key, which was later combined with the message tape. This long, single key is not, strictly speaking, a purely random key throughout its length as it is made up of combinations of the two original and comparatively short key tapes. The characters in this key do not repeat in the same sequence at comparatively short regular intervals, however, as would be the case if only one key tape loop were used.

The number of characters in this equivalent single key is equal to the product of the number of characters in the two tape loops, and may easily exceed 600,000 before any part of the key begins to repeat. If proper care is taken to use the system so as to avoid giving information to the enemy regarding the lengths of the two key tape loops or their initial settings and to avoid the possibility of ever re-using any part of the resultant single key, this system is extremely difficult to break even by an expert cryptanalyst having a large number of messages and full knowledge of the construction of the machine and its method of operation.

Captain W. F. Friedman, Cryptanalyst of the Signal Corps, U. S. Army, has recently invented some modifications[5] of this system intended to eliminate the loss in secrecy that results from using the two more convenient comparatively short repeating key tapes instead of the single long non-repeating key tape. These modifications consist of changing at intervals the order of connection of the five contacts of one or more of the tape transmitters or of adding a third key tape and transmitter so arranged that the extra key tape does not step ahead in unison with the other two key tapes, but starts and stops at irregular intervals. Either of these methods, properly used, makes unauthorized decipherment practically impossible and, at the same time, does not unduly complicate the machine or its method of operation.

With the double key tape system, the handling of large volumes of traffic is greatly simplified. The tapes should be numbered so that the deciphering operator can set them at the correct starting point for each message, and rules should be adopted so that both key tapes will never be set twice at the same

5. See Patents 1,522,775 of Jan. 13, 1925 and 1,516,180 of Nov. 18, 1924.

starting point. Information regarding the proper settings for the key tapes for deciphering each message must be sent to the deciphering operator. These settings may be prearranged or they may be selected arbitrarily by the sending operator. In the latter case the numbers representing the key tape settings should be prefixed to the message. These "key indicators" should preferably be enciphered by running them through the machine together with a special key tape which is used only for this purpose.

Speed of Operation

This type of machine was operated by the Signal Corps over its private wire telegraph circuits. In service tests made by the United States Army, each outgoing message was checked by running it again through the machine to decipher and print it, and the deciphered copy was then compared with the original message, so that each message tape was run through twice. A certain amount of time was lost, due to setting and resetting the key tapes, checking, etc., for each message, but an average enciphering speed of 10-15 words per minute was readily maintained. We understand this to be many times faster than those manual methods for enciphering or coding, which are used where a high degree of secrecy is required. Incoming messages were deciphered at the rate of 30-40 words per minute.

Operation by Radio

This cipher system was demonstrated before the delegates to the Preliminary International Communications Conference in October, 1920. During this demonstration, cipher messages were sent over a circuit containing a radio link, as illustrated in Fig. 11. The radio equipment was the same as that employed a year previous in tests on the operation of multiplex and start-stop printing telegraphs by radio and is described elsewhere.[6]

6. "Printing Telegraph by Radio" by R. A. Heising, *Journal* of the Franklin Institute, January 1922, pp. 97-101

A considerable number of cipher messages were transmitted over this radio circuit during this demonstration, these messages being automatically enciphered before and deciphered after transmission, so that they they were absolutely secret, even though transmitted by radio. No interference from atmospherics or from other radio stations was noticed, all messages being received without error.

In conclusion, we wish to express our appreciation of the assistance given us by the officers of the Signal Corps and the General Staff, of the United States Army, in making tests and trials of cipher printing telegraph systems; and we wish particularly to acknowledge our indebtedness to Lt.-Col. J. O. Mauborgne, of the Signal Corps, for his advice in connection with this development and for his assistance in arranging to have tests made to determine its secrecy and demonstrations and service trials to determine its practicability for Army use. We also wish to express our appreciation of the services rendered by the Cipher Department of the Riverbank Laboratories, Geneva, Illinois, and by Col. George Fabyan, the head of these laboratories, in making tests of the secrecy of messages enciphered in various ways with these machines.

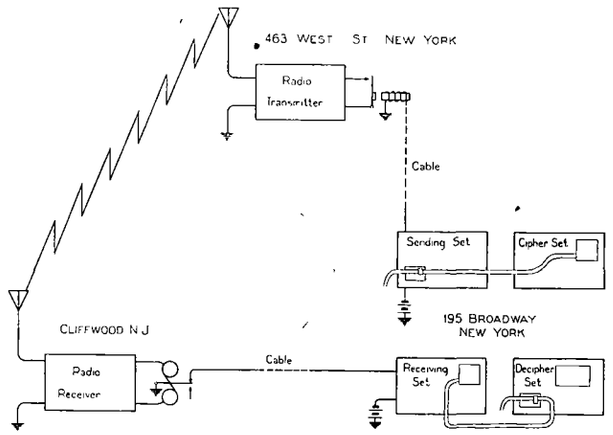

Fig 11—Circuit for Radio Cipher Demonstrations