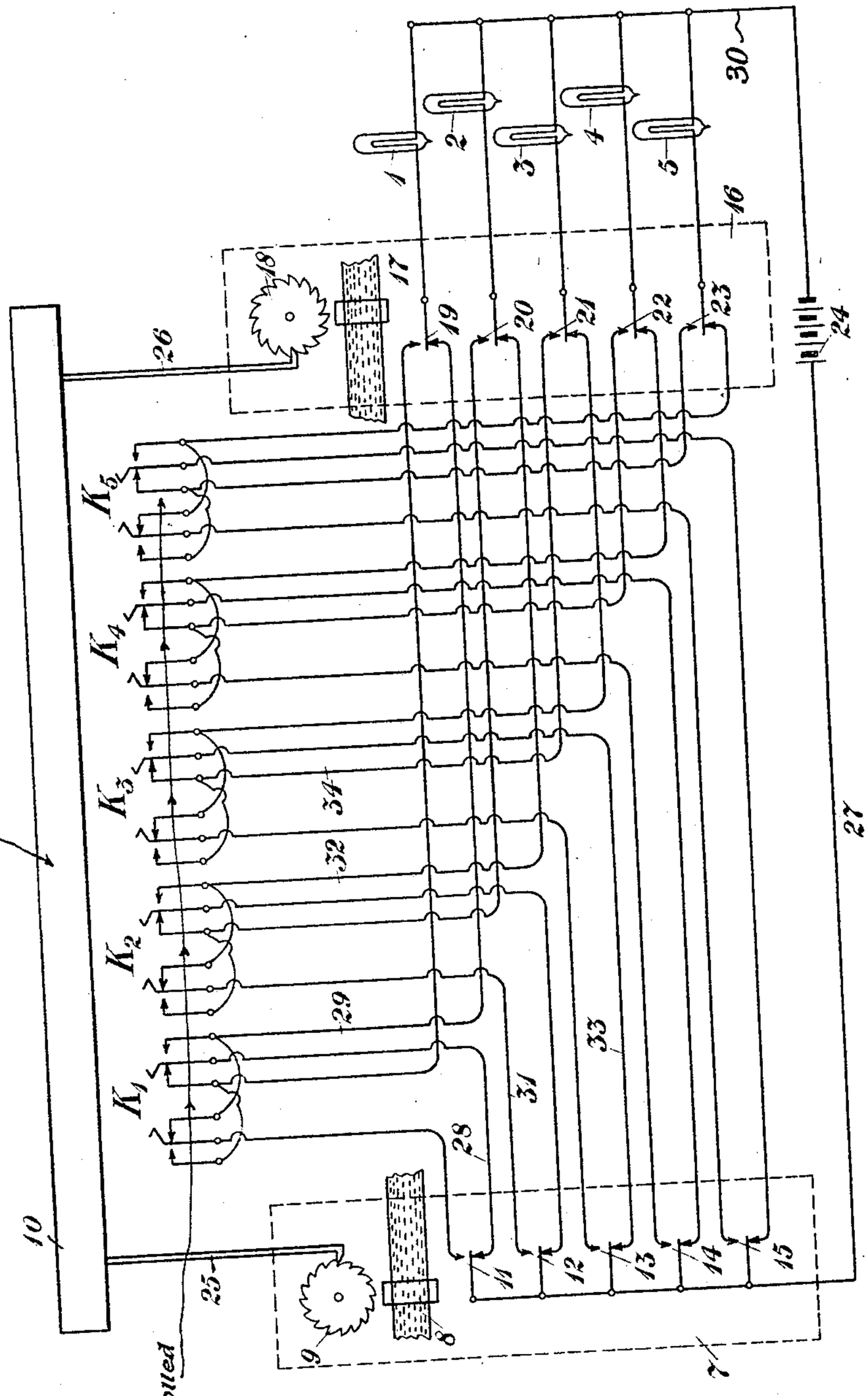
Jan. 12, 1926. **1,568,991**

L. F. MOREHOUSE

CIPHERING AND DECIPHERING DEVICE

Filed April 15, 1920



INVENTOR
L. F. Morehouse
BY
ATTORNEY

Patented Jan. 12, 1926. 1,568,991

UNITED STATES PATENT OFFICE.

LYMAN F. MOREHOUSE, OF MONTCLAIR, NEW JERSEY, ASSIGNOR TO AMERICAN TELEPHONE AND TELEGRAPH COMPANY, A CORPORATION OF NEW YORK.

CIPHERING AND DECIPHERING DEVICE.

Application filed April 15, 1920. Serial No. 374,159.

To all whom it may concern:

Be it known that I, LYMAN F. MOREHOUSE, residing at Montclair, in the county of Essex and State of New Jersey, have invented certain Improvements in Ciphering and Deciphering Devices, of which the following is a specification.

This invention relates to systems of communication and more particularly to ciphering and deciphering devices whereby secrecy may be provided in the transmission of messages over such systems.

A well known method for providing secrecy in the transmission of messages, which has been developed in connection with printing telegraph systems, has been to combine the code combinations or characters of one or more key tapes with the code combination or characters of a message to produce an enciphered message and to combine the code combinations or characters of similar key tapes at a receiving station with the code combinations or characters of the enciphered message to reproduce the original message. Such a result has been obtained by perforating the true message on a paper strip or tape in accordance with a well known code, perforating a similar tape with another message or jumble of characters, running these two tapes in synchronism through two tape transmitters which jointly control the transmission of impulses to the line or the energization of the electromagnetic punch selecting members of a local perforator which perforates a third tape with an unintelligible sequence of characters representing a combination of the message tape and the cipher tape. This unintelligible or enciphered message is then transmitted over the line and may be recorded by any suitable receiving device, preferably a reciving perforator which will then perforate a tape duplicating that used for the transmission of the enciphered message. For deciphering such a message it is essential that the receiving operator be provided with a duplicate of the original key tape. When so equipped, he can by running the key tape and the enciphered message tape in synchronism through two local tape transmitters, exert a joint control on the selecting mechanism of a local printer that will result in the printing of the original message in deciphered form.

The above described printing telegraph ciphering and deciphering arrangements involve the use of heavy and bulky equipment which must be connected furthermore to a suitable source of electrical power supply and this type of apparatus may only be utilized in practice when it can be more or less permanently installed. Accordingly it is the general purpose of this invention to provide a device whereby code combinations, which represent characters of a message, may be enciphered and rendered unintelligible and whereby the enciphered and unintelligible code combinations of an enciphered message may be deciphered and the message rendered intelligible, which device will be characterized by the following features. It is a cardinal feature of the invention to provide a device for the above purposes which will be exceedingly simple in structure, will be portable, and will not be dependent for its operation on an outside source of power supply. While the ciphering and deciphering device of this invention may be utilized for the preparation of messages which may be transmitted over telegraph or other lines, its use is not so limited, as the code messages prepared thereby may be transmitted over a variety of systems of communication, such as by mail or by carrier or other means. Accordingly the device will not depend for its usefulness upon its proximity to a telegraph or other transmission line and it is a feature of the invention that the device may be utilized in situations where it would not be practicable or desirable to install permanent apparatus. Other and further purposes and features of the invention will appear more fully from the detailed description hereinafter given.

The device of this invention operates on the principles heretofore mentioned with respect to printing telegraph systems in that the code characters of the original message are combined in effect with the code characters of one or more key tapes to produce an enciphered message, and to reproduce the original message the code characters of the

enciphered message are combined in effect by the device with the code characters of one or more key tapes similar to those utilized for enciphering the original message. In the device of this invention there is combined in a simple and compact piece of apparatus two tape transmitters, a group of manually operated keys and a group of signals. In enciphering a message the code combinations representing characters of the message are set up on the keys and the signals will indicate different code combinations representing different characters which make up the enciphered message. The characters represented by the signals may then be written down or typewritten in suitable form for transmission by telegraph or other means. To decipher a message the code combinations or characters of the enciphered message, as represented by the signals, should be set up on the keys and the signals will then indicate code combinations representing the letters or characters of the original message. The key tapes utilized in the ciphering device and the deciphering device should be identical. These key tapes will be constantly varying the method of enciphering the code combinations of the original message. By maintaining secrecy as to the key tapes utilized and by constantly changing the key tapes it will be practically impossible for an unauthorized person to obtain information from the messages. Furthermore the device of this invention is not limited in use to the well known five unit code utilized in printing telegraphy as by changing the number of keys and signals to be employed it may operate with other codes, such for example as a four unit code.

The invention may be more fully understood from the following description together with the accompanying drawing in the figure of which is illustrated a circuit diagram of the ciphering and deciphering device of the invention.

The device illustrated in the drawing includes a plurality of keys such as keys K_1, K_2, K_3, K_4 and K_5 and a plurality of signaling means such for purposes of illustration as lamps 1, 2, 3, 4 and 5. The circuits for lamps 1, 2, 3, 4 and 5 are controlled by the contacts of keys K_1, K_2, K_3, K_4 and K_5 and the switches 11, 12, 13, 14 and 15 of the tape transmitter 7, and the switches 19, 20, 21, 22 and 23 of the tape transmitter 16. The tape transmitters 7 and 16 may be of a well known type utilized in printing telegraph systems. In order to simplify the circuit the above mentioned switches of the transmitters are shown as insulated from each other instead of being associated with the usual bus-bars. The switches of transmitters 7 and 16 are controlled by the perforated tapes 8 and 17 respectively. The keys K_1, K_2, K_3, K_4 and K_5 may if desired be of the mechanically locking type, which will be locked in position when depressed. To release the keys there is provided the space bar 10, such as may be provided on a typewriter, which when depressed will restore the keys to normal. An arrangement whereby a number of keys may be mechanically locked in position and may be released by the operation of another member is illustrated in Figures 6 and 8 of the United States Patent to A. Kneisel, 1,204,884, November 14, 1916. It is pointed out, however, that any other well-known arrangement of this character may be employed herewith. The space bar 10 may also serve to move the perforated tapes 8 and 17 along step by step when operated through any suitable mechanism which is herein illustrated as the pivoted arms 25 and 26 and the ratchet wheels 9 and 18 respectively. To operate the lamps the local source 24 of current is provided.

The invention may be more fully understood from the following description of its operation. For purposes of illustration let it be assumed that it is desired to send the letter E over the system and furthermore that the well known five unit printing telegraph code is being utilized in which the letter E is represented as + — — — — —, where + represents a "marking" impulse and — represents a "spacing" impulse. Accordingly the operator will depress key K_1 to correspond to the "marking" impulse and will leave the keys K_2, K_3, K_4, K_5, unoperated to correspond to the "spacing" impulses. Let it be assumed that, when key K_1 is thus operated, that the perforations on tape 8 are in the following combination of "marking" and "spacing" impulses such as — + — — +. Accordingly switch 11, being subject to a "spacing" impulse, will allow its normal contact to remain closed. Switch 12, being subject to a "marking" impulse, will close its upper contact. Switches 13 and 14, being subject to "spacing" impulses, will allow their normal contacts to remain closed. Switch 15, being subject to a "marking" impulse, will close its upper contact. Let it also be assumed that, when the key K_1 is operated, the perforations on tape 17 are in the following combination of "marking" and "spacing" impulses, such as — — + — +. Accordingly switch 19, being subject to a "spacing" impulse, will allow its normal contact to remain closed. Switch 20, being subject to a "spacing" impulse, will allow its normal contact to remain closed. Switch 21 being subject to a "marking" impulse, will close its upper contact. Switch 22, being subject to a "spacing" impulse, will allow its normal contact to remain closed. Switch 23. being subject to a "marking" impulse, will close its upper contact. With the above described arrangement of the switches of

transmitters 7 and 16 and with the key K_1 operated, the circuits for signal lamps 1, 2, 3, 4 and 5 will be effected in the following manner. A circuit will be completed for signal lamp 1 as follows; from one pole of battery 24, conductor 27, normal contact of switch 11, conductor 28, right hand make contact of key K_1, conductor 29, normal contact of switch 19, filament of lamp 1, conductor 30, to the other pole of battery 24, thereby operating signal lamp 1. A circuit will be completed for signal lamp 2 as follows: from one pole of battery 24, conductor 27, upper contact of switch 12, conductor 31, left hand normal contact of key K_2, conductor 32, normal contact of switch 20, filament of lamp 2, conductor 30, to the other pole of battery 24, thereby operating lamp 2. A circuit will be completed for lamp 3 as follows: from one pole of battery 24, conductor 27, normal contact of switch 13, conductor 33, right hand normal contact of key K_3, conductor 34, upper contact of switch 21, filament of lamp 3, conductor 30, to the other pole of battery 24, thereby operating lamp 3. With the normal contacts of switches 14 and 22 closed and with key K_4 unoperated no circuit will be completed for lamp 4, and it will not be lighted. With the upper contacts of switches 15 and 23 closed and the key K_5 unoperated no circuit will be completed for lamp 5 and it will not be lighted. Accordingly it will be seen that when the keys K_1, K_2, K_3, K_4 and K_5 are operated in accordance with the code combination + — — — — representing the letter E, that the signal lamps 1, 2 and 3, will be lighted and 4 and 5 will not be lighted, thus forming a code combination + + + — — representing the letter U. Accordingly the operator will copy down the letter U to represent in the enciphered message the letter E of the original message. It is pointed out that should the letter E appear in the original message later on when the perforations on tapes 8 and 17 have assumed different code combinations that it will not necessarily appear in the enciphered message as represented by the letter U but may be some other letter or character as determined by the combined effect of the perforations of the tapes. Accordingly as the tapes move along and the perforations thereon change, the method of enciphering the letters of the original message is constantly being varied. In a similar manner to that described for the letter E, the other characters or letters of the original message will be changed in a constantly varying manner into other characters which will make up the enciphered message. As has been pointed out the message thus enciphered may be transmitted by any desired means to its destination.

To decipher the enciphered message at the receiving station a device identical to the one utilized at the sending station is provided and accordingly reference will be again made to the figure illustrated and described with respect to the ciphering of the message. The operator at the receiving station must be provided with key tapes identical to those utilized at the sending station and inserted in the transmitters in the same position with respect to their perforations as the tapes at the sending station. For purposes of illustration let it be assumed that the first character of the enciphered message received is the letter U which represented the letter E of the original message. Accordingly when the tapes 8 and 17 have been properly inserted in the transmitters the operator will depress the keys in a manner to represent the code combinations, such as + + + — —, for the letter U. This may be done by operating keys K_1, K_2, K_3 and leaving keys K_4 and K_5 unoperated. Tape 8 will have assumed the code combination of "marking" and "spacing" impulses such as — + — — +, and tape 17 will have assumed the code combination of "marking" and "spacing" impulses such as — — + — +. Accordingly the switches of transmitter 7 and 16 will have arranged themselves in the same manner as formerly pointed out in the description of the enciphering operation. With such an arrangement of switches and with the keys K_1, K_2, K_3, thrown and with key K_4 and key K_5 unoperated the circuits of the signal lamps will be effected in the following manner. A circuit will be completed for lamp 1 as follows: from one pole of battery 24, conductor 27, normal contact of switch 11, conductor 28, right hand make contact of key K_1, conductor 29, normal contact of switch 19, filament of lamp 1, conductor 30, to the other pole of battery 24, thereby operating lamp 1. With the upper contact of switch 12 closed, the normal contact of switch 20 closed, and key K_2 operated no circuit will be completed for lamp 2 and it will not be operated. With the normal contact of switch 13 closed, the upper contact of switch 21 closed, and key K_3 operated no circuit will be closed for lamp 3 and it will not be operated. With the normal contacts of switches 14 and 22 closed and key K_4 unoperated no circuit will be closed for lamp 4 and it will not be operated. With the upper contacts of switches 15 and 23 closed and key K_5 unoperated no circuit will be closed for lamp 5 and it will not be operated. Accordingly when the code combination representing the letter U of the enciphered message is produced on the keys, the signal lamp 1 will be lighted and lamp 2, 3, 4, and 5 will not be lighted, thereby producing the code combination representing the letter E of the original message. In a corresponding manner the remaining letters or characters of the enciphered message

when produced on the keys will cause the lamps to produce the remaining letters or characters of the original message.

In the above described operation of the device of the invention reference has been made to the well known five-unit code utilized in printing telegraph systems. It is pointed out that the device of the invention is not limited in use to a five unit code, but may operate with other codes, such as a four unit code. The five-unit printer code consists of 32 signal combinations of which 26 are used to represent the letters of the alphabet and the remaining 6 signal combinations are used either to control printer operations or to represent figures or characters other than the letters of the alphabet. If the five unit code is used with the device of this invention the enciphered message will include these six extra signals as well as the 26 letters. These 6 extra signals appear in the enciphered message as a result of combining certain letters in the tapes with certain letters set up on the keys, and, therefore, their appearance in the enciphered message cannot be avoided. Furthermore in order that the message may be deciphered at the receiving station, it is necessary that these 6 extra signals be represented in the enciphered message as transmitted to the receiving station. The presence of these 6 extra figures or characters other than letters in the enciphered message transmitted may at times be undesirable for the following reasons. In charging for ciphered messages it is the usual practice on land lines to count at the rate of one word for every five letters, but in groups consisting of letters and characters other than letters, such as figures, each letter and figure is counted as one word. Therefore, if numerals or characters other than letters are used to designate these 6 extra signals a considerable increase in telegraph tolls will result. Accordingly if the enciphered message is intended for transmission over a telegraph line the five-unit code may involve considerable expense.

It is possible to avoid this additional expense caused by the appearance of numerals in the enciphered message by utilizing a four-unit code. With a four-unit code only the keys K_1, K_2, K_3 and K_4 and the lamps 1, 2, 3 and 4 of the device would be utilized. Furthermore the key tapes would only have four-unit perforations thereon and the switches 15 and 23 would not be used. By reducing the number of units in the code from 5 to 4, the number of signal combinations may be reduced from 32 to 16. In order to represent the 26 letters of the alphabet with only 16 signal combinations certain of the signal combinations must be used to represent either of two letters. Accordingly one of the signal combinations may be utilized as an arbitrary signal, termed a shift signal, and the other signal combinations, which may normally represent certain letters, will when preceded by the shift signal represent other letters. Such a code, for purposes of illustration, might be arranged as shown in the following table.

Column 1.	Column 2.	Column 3.
Keys operated.	Normal letters.	Shifted letters.
None	Shift signal	
1	E	F
2	T	Y
3	O	W
4	A	G
12	N	B
1 3	I	V
1 4	R	K
23	S	J
2 4	H	X
34	D	Z
123	L	Q
12 4	U	.
1 34	C	?
234	M	"
1234	P	,

In using the above code it should be understood that the signals in the first column are used to ordinarily represent the letters in the second column, but that these same signals if preceded by a shift signal will represent corresponding letters or punctuation marks in the third column. The shift signal consists in merely depressing the spacing bar and operating none of the keys. Accordingly the code combinations of the enciphered message, which will be the combined result of the operation of the keys and the tapes, will be combinations represented by letters in the second column. In writing down the enciphered message for transmission the letters in the second column should be used and when a shift signal occurs it should be represented by any one of the eleven letters in the third column. In deciphering such a message all the "shifted letters" which appear in the enciphered message should be set up on the keys as shift signals. With the above described four-unit code a method of signaling is provided whereby the enciphered message will only include the characters in column 2 and the shift signal which is represented by the letters in column 3 and accordingly will not include numerals or characters other than letters and by the use of such a code a substantial saving in expense will result when the enciphered message is intended for transmission over a telegraph system. While a specific four-unit code has been illustrated, it is understood that the arrangement of the invention may operate with other codes of a similar nature.

While the invention has been disclosed as embodied in certain specific arrangements which are deemed desirable it is understood that it is capable of embodiment in many and widely varied forms without departing

from the spirit of the invention as defined in the appended claim.

What is claimed is:

In a ciphering and deciphering device, a telegraph transmitter including a tape provided with prearranged groups of perforations therein and a set of contacts controlled in accordance with said groups of perforations, a set of contacts controlled by key mechanisms operable in accordance with the code combinations of the original message, a group of signal lamps under the joint control of said sets of contacts for displaying the code combinations of the enciphered or deciphered message, means for locking said key mechanisms in operated position, and means for releasing said key mechanisms and for advancing said perforated tape.

In testimony whereof, I have signed my name to this specification this 10th day of April 1920.

LYMAN F. MOREHOUSE.