L. F. MOREHOUSE.

CIPHERING SYSTEM.

APPLICATION FILED DEC. 4, 1918.

1,356,546.

Patented Oct. 26, 1920.

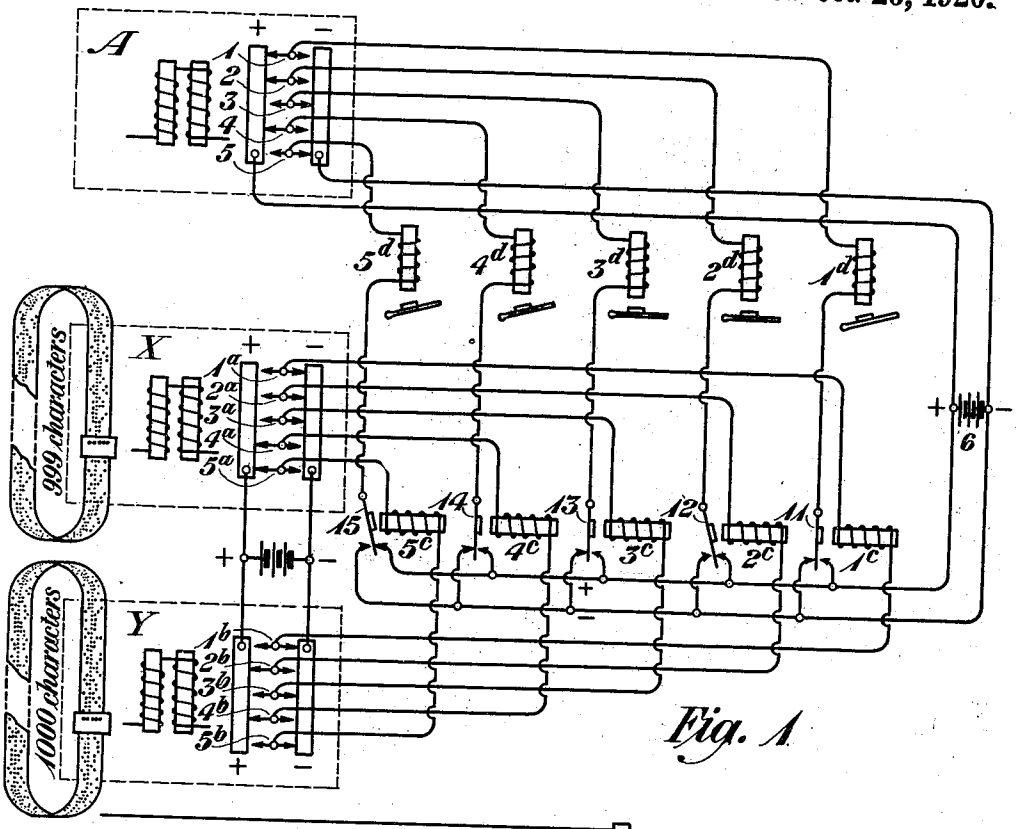

Fig. 1

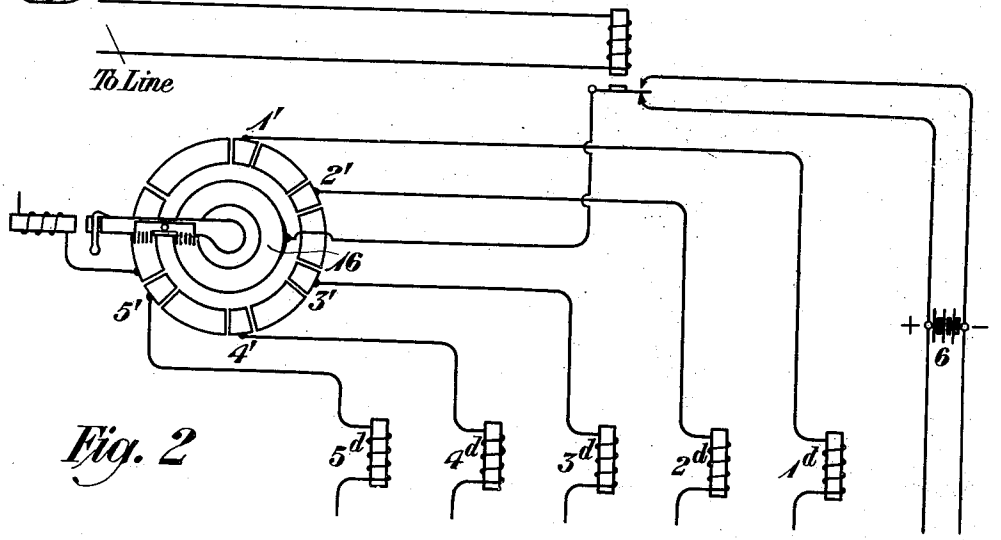

Fig. 2

INVENTOR.

L. F. Morehouse

BY G. E. Folk

ATTORNEY.

UNITED STATES PATENT OFFICE.

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

CIPHERING SYSTEM.

1,356,546. Specification of Letters Patent. Patented Oct. 26, 1920.

Application filed December 4, 1918. Serial No. 265,307.

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 Systems, of which the following is a specification.

This invention relates to the secret communication of intelligence and finds a particularly useful application in systems for enciphering and deciphering messages such as set forth in the copending application of G. S. Verman, 253,962, filed September 13, 1918, and assigned to the assignee of this application, but is applicable to any ciphering or deciphering system where the key used is to be changed frequently.

The application above referred to discloses a secret system employing the ordinary printing telegraph equipment using the five unit code and in which the five sending relays and the five receiving relays, are under the joint control of a keyboard or tape transmitter and a second transmitter serving to encipher and decipher the message. The circuits of the sending and receiving relays, instead of being all grounded upon one side, may thus be connected to either battery or ground, depending upon the positions of the contacts of this second transmitter. In such a system it will be obvious that the impulses transmitted to the line, or to the printer, as the case may be, will not represent the character set up on the keyboard or tape transmitter but some other character, depending upon the momentary connections of the opposite ends of the relay circuits. The operation of the sending relays is thus dependent upon the combined effect of the two transmitting devices. If the contacts of the enciphering and deciphering transmitter were set permanently to represent some character such as "A" whose symbol is ++−−−, the character transmitted would obviously be different from the characters of the message, but the message could then be deciphered by an expert with little difficulty. If, however, the arrangement of the contacts in the enciphering transmitter is altered at intervals, the deciphering is more difficult and becomes progressively more so as the intervals are shortened. If the arrangement of the contacts be changed with each character transmitted, the deciphering is well nigh impossible, and if the sequence of changes is never repeated, deciphering becomes absolutely impossible. To insure secrecy in continued operation of such a system, therefore, it is important to provide key tapes or records for the ciphering and deciphering transmitter which gives a series of positions for the contacts thereof, which does not repeat, or which repeats at such unfrequent intervals as to be equivalent to a continuously changing series for all practical purposes. To produce a tape to give such a series of changes in a system such as shown in the above mentioned application would be expensive and burdensome and the use of a tape would be inconvenient because of its extreme length. The present invention provides a system in which a continuously changing series of arrangements for the enciphering contacts may be produced in a simple and convenient manner.

While the invention is here illustrated by an embodiment particularly fitted for use in the system above mentioned, it is to be noted that in its broader aspects it is applicable to ciphering and deciphering systems generally, whether or not they involve the use of mechanical or electrical devices.

In the accompanying drawings Figure 1 is a diagrammatic illustration of one embodiment of the invention and Fig. 2 indicates its application to the receiving distributer of a printing telegraph equipment.

A represents a transmitter upon which the characters of the message to be enciphered or deciphered are set up in succession. This may be a tape transmitter or a keyboard transmitter such as are commonly used in printing telegraphy. In either case there are five contacts 1, 2, 3, 4 and 5 which may be made to form either the positive or negative terminals of five control circuits. For this purpose the contacts may, as shown on the drawing be movable between positive and negative bus-bars, connected to the opposite poles of a battery 6. Two other transmitters X and Y, which may conveniently be ordinary tape transmitters, are used to accomplish the enciphering and deciphering of the characters set up at A. These transmitters, like that above described, are provided with five contacts each, indicated at 1^a, 2^a, 3^a, 4^a and 5^a and 1^b, 2^b, 3^b, 4^b and 5^b respectively, which may be made to form either positive or negative circuit terminals. The correspondingly numbered contacts in the transmitters X and Y

are united through the windings of relays 1^c, 2^c, 3^c, 4^c and 5^c, each of which is provided with a front and back contact connected to the positive and negative poles respectively of the battery 6 or other convenient source of current. The armatures 11, 12, 13, 14 and 15 of these relays take the place of the oscillating contacts of the enciphering transmitter in a system where only one such transmitter is used. The magnets 1^d, 2^d, 3^d, 4^d and 5^d represent the operating magnets or relays of any selectively operated mechanism which is to deal with the enciphering or deciphering of the message, such, for instance, as the selecting magnets for controlling a printer or a perforator, or the selecting relays used in connection with the distributer in transmitting impulses over the line, all of which are instruments now in common use in printing telegraph sets. These relays have their windings connected between the contacts 1, 2, 3, 4 and 5 of the transmitter A and the armatures 11, 12, 13, 14 and 15 of the controlling relays.

The contacts of the transmitter A are operated either by hand or by a tape to represent the characters of the original or the enciphered message (depending upon whether the message is to be enciphered or deciphered.) Each of the transmitters X and Y is provided with a separate perforated tape or equivalent record having a series of characters represented thereon preferably selected at random. One of these tapes has a greater number of characters than the other, a difference of one character being convenient and sufficient for the purpose in hand. These tapes or records are preferably in the form of closed bands so that each may travel continuously through its transmitter the operation beginning at any selected point thereon. With these bands in place and operating it will be obvious at once that the combination of relays of the set 1^c, 2^c, 3^c, 4^c and 5^c to be operated at any given time depends upon the two characters which happen at the moment to be in the transmitters X and Y, since none of these relays will operate, if the contacts to which its opposite terminals are connected both happen to be upon positive or both upon negative bus-bars, but will operate if either terminal is upon a positive and the other upon a negative bus-bar. When one tape has completed one revolution, the other tape, being of a different length, will have overrun or have failed to complete a revolution and in the following round of the tapes the combination of characters set up in the relays 1^c, 2^c, 3^c, 4^c and 5^c will accordingly be a different series from that set up during the first round. If, for example, one of these tapes be provided with a thousand characters and the other with 999 characters (which are convenient lengths for use) the two tapes can pass 999 times through the two transmitters before the original series of combination will be repeated. Therefore, the two tapes thus operating provide 999,000 character combinations in the relays 1^c, 2^c, 3^c, 4^c and 5^c before they begin to repeat the series. Such a number as this will serve for a considerable period of message transmission and if it is desired to avoid a repetition even as often as this, further key tapes providing other series of like lengths can readily be provided.

The arrangement of contacts shown on the drawing illustrates the manner in which the enciphering, according to this system, will proceed. The transmitter A has its first, second and fourth contacts shifted to the positive bus-bars, thus representing the symbol for the letter J, or $++-+-$. The transmitter X has its fourth and fifth contacts shifted, thus representing the symbol for the letter O, or $---++$. The transmitter Y has its second and fourth contacts shifted, thus representing the symbol for the letter R, or $-+-+-$. In the set of relays 1^c, 2^c, 3^c, 4^c, 5^c, armature 11 will be unaffected since both terminals of the relay winding are connected to the negative pole of the battery. Armature 12 will be shifted since the winding is connected to the negative pole at X and to the positive pole at Y. Armature 13 will be unaffected since the relay winding is connected to the negative pole at both ends. Armature 14 will be unaffected since the relay winding is connected to the positive pole at both ends. Armature 15 will be shifted since the relay winding is connected to the positive pole at X and the negative pole at Y. In this set of relays, therefore, we have the second and fifth contacts shifted, representing the symbol for the letter L, or $-+--+$. The magnet 1^d of the device to be selectively operated will receive current, since its winding is connected to the positive pole at A and the negative pole at 1^c. The magnet 2^d will be unaffected since it is connected to the positive pole at both ends. Magnet 3^d will be unaffected since it is connected to the negative pole at both ends. Magnet 4^d will be operated since its winding is connected to the positive pole at A and the negative pole at 4^c. The magnet 5^d will be operated since it is connected to the negative pole at A and the positive pole at 5^c. That is to say, the first, fourth and fifth armatures of the magnets to be selectively controlled are shifted, thus representing the symbol for the character B. Supposing therefore, the tape in the transmitter A to represent the unciphered message the letter J of this message will be represented in ciphered form by the letter B. Deciphering operation is the same except that the tape having the ciphered message thereon is used in the

transmitter A. At the same point in the message the transmitter A would then have its contact set to represent the letter B and by tracing the resulting circuits it will be found that the controlling magnets 1^d, 2^d, 3^d, 4^d, 5^d will then represent the letter J.

If it is desired to use the double tape system above described for deciphering messages as they are received over the line, the windings of the magnet 1^d, 2^d, 3^d, 4^d and 5^d are connected on one side to the five contacts of the receiving distributer as shown in Fig. 2 instead of to the five contacts of the transmitter A and the line relays over which the impulses are received will operate an armature which is connected to the continuous ring 16 of the distributer and the front and back contacts of the relay armature will be connected to the opposite poles of the battery 6. The magnets 1^d, 2^d, 3^d, 4^d and 5^d will then receive the same impulses as if their terminals were connected to the transmitter A, except that the impulses will be successive instead of simultaneous. Existing apparatus is arranged to use them in either way.

By the use of two key tapes as herein described, it is obviously possible to transmit messages for an indefinite period without repeating the series of characters used to encipher and decipher the message, and do this without the inconvenience of using excessively long tapes or an extremely large number of tapes as would otherwise be necessary. Obviously the combining of the effects of key tape in accordance with this invention is not limited to the use of a single pair. Any desired number may be used by combining them so as ultimately to have their effects united in a single set of contacts such as those indicated herein at 11, 12, 13, 14, 15.

It will be clear that the invention is not limited to the use of perforated tapes, or any other particular form of record for the series of ciphering characters nor to any particular electrical or mechanical means for combining the characters from the several series to produce the running key by which the enciphering and deciphering are accomplished. It is not important in the use of the invention that the effect of combining the two or more characters from different series should be actually manifested in a discernible form. In the embodiment of the invention above described, characters or symbols representing the running key are not recorded, though they could be discerned from the position of the armatures of relays 11 to 15 if these are so located as to be visible. But even this is not necessary since the same result is obtained if the successive effects of the combination of two symbols from different series are combined by predetermined rule in any convenient way with symbols representing the successive message characters. To practice the invention it is only necessary that there shall be plurality of series of ciphering characters, differing in length, so that they may be used repeatedly for combining with another series without producing a cyclic repetition of the same character or sequence of characters in the resulting series, and that each character be assigned a definite form, position, value or other characteristic (the electrical symbols, such as ++−−− for A, in the embodiment above described) such that those for characters of different series may be combined, in accordance with some predetermined rule, to produce definite effects, indications or symbols, which in turn are similarly combinable with characteristics assigned to the characters of the message.

Even in the specific embodiment of the invention herein described, it will be clear that it is not limited to the particular arrangement of circuits and contact devices shown and described, as various modifications will readily suggest themselves without departing from the spirit of the invention.

What is claimed is:

1. The method of enciphering or deciphering messages which consists in forming a plurality of series of ciphering characters with the number of characters different in each series, selecting characters from each series in a fixed order to form a continuous sequence by retraversing the series as it is exhausted, and altering the message characters in accordance with a predetermined rule whose effect upon successive message characters is dependent upon the concurrent use of characters so selected from different cipher series.

2. The method of enciphering or deciphering messages which consists in forming a plurality of series of ciphering characters, assigning to each character a characteristic combinable, in accordance with a predetermined rule, with the characteristic of any character in another series to produce a definite effect, and determining the characters of the enciphered or deciphered message by combining representations of the successive message characters to the successive effects produced by such combination.

3. The method of enciphering or decipering, which consists in forming a plurality of series of ciphering characters, assigning to each character a characteristic combinable according to a predetermined rule with the characteristic of any character in another series to produce a definite effect, assigning to each message character a characteristic combinable according to a predetermined rule with the effects so produced,

and combining the characteristics of the successive message characters with successive effects produced by combining the characteristics of characters in the different series to determine the characters of the enciphered or deciphered message.

4. The method of enciphering or deciphering messages which consists in combining the successive code symbols of a plurality of predetermined series of unequal length, repeatedly used to produce a cipher key having a long series of symbols without cyclic repetition of the same symbol or sequence of symbols, and combining the successive symbols of the cipher key so produced with the code symbols of the successive message characters to indicate the successive characters of the enciphered or deciphered message.

5. The method of producing a cipher key, free from cyclic repetition of the same character or sequence of characters, which consists in forming a plurality of series of ciphering characters with the number of characters different in different series, selecting characters from each series to form a continuous sequence by retraversing the series as it is exhausted, and combining the successively selected characters from different series.

6. The method of producing a cipher key free from cyclic repetition of the same character or sequence of characters, which consists in forming a plurality of series of ciphering characters with the number of characters different in each series, selecting characters from each series to form a continuous sequence by retraversing the series as it is exhausted, and combining the successively selected characters from different series in accordance with a predetermined rule.

7. The method of producing a cipher key free from cyclic repetition of the same character or sequence of characters, which consists in forming a plurality of series of ciphering characters with the number of characters in at least one series different from that in the others, assigning to each character a characteristic combinable in accordance with a predetermined rule with the characteristics of characters in the other series, selecting characters from each series to form from each a continuous sequence by retraversing the series as exhausted, and combining the successively selected characters from different series in accordance with a predetermined rule.

8. A ciphering and deciphering device comprising a plurality of key records each composed of a series of ciphering characters with the number of characters different in each series, and each character having a characteristic combinable in accordance with a predetermined rule with the characteristics of characters in another series, and means responsive to the combined effect of successively selecting characters from the different series for indicating the character of the enciphered or deciphered message corresponding to a given message character.

9. In a ciphering and deciphering device a plurality of key records, each bearing a number of code symbols arranged in an endless closed series, the number of symbols in the two series being different in different series, groups of controlling members, one group associated with each key record, and adapted to represent successively the symbols thereon, another group of controlling members adapted to represent successively the character symbols of the message to be enciphered or deciphered, and means under the joint control of said groups of members for indicating characters of the enciphered or deciphered message.

10. In a ciphering and deciphering device, a plurality of records, each bearing a number of code symbols arranged in an endless closed series, the number of symbols being different in different series, groups of controlling members, one group associated with each key record and adapted to represent successively the symbols thereon, mechanism responding to the joint control of said groups of members to represent the combined effect of the symbols momentarily controlling the groups, another group of controlling members adapted to represent successively the character symbols of the message to be enciphered or deciphered, and means under the joint control of said mechanism and said other group of members for indicating the characters of the enciphered or deciphered message.

11. In a ciphering and deciphering device, a plurality of key records, each bearing a number of code symbols arranged in an endless closed series, the number of symbols being different in each key, groups of controlling members, one group associated with each key record and adapted to represent successively the symbols thereon, a group of devices adapted to represent successively the character symbols of the message to be enciphered or deciphered, and means under the joint control of said groups of controlling members and said devices for indicating the characters of the enciphered or deciphered message.

12. A ciphering and deciphering device comprising a plurality of key tapes, each in form of a closed loop bearing a continuous series of character symbols thereon whose number is different on at least two of the tapes, mechanism under the control of said tapes for combining the effects of single symbols from each of the several tapes, and means for simultaneously moving the tapes forward to bring successive symbols on each tape into position to affect said mechanism,

whereby a series of key symbols may be produced which is long, compared with either of the tape series and is free from cyclic repetitions of the same symbols or sequence of symbols.

13. A ciphering and deciphering device comprising two key tapes, each in form of a closed loop bearing a continuous series of character symbols thereon, whose number is different on the two tapes, mechanism under the control of said tapes for combining the effects of two symbols, one from each tape, and means for simultaneously moving the tapes forward to bring successive symbols on each tape into position to affect said mechanism, whereby a series of key symbols may be produced which is long, compared with either of the tape series and is free from cyclic repetitions of the same symbol or sequence of symbols.

14. In a device for enciphering and deciphering messages, mechanism for recording the enciphered or deciphered message, means for indicating successively the code symbols of the message to be enciphered or deciphered, a set of devices capable of representing a long series of code symbols corresponding to the key used for the enciphering and deciphering, and means for controlling said devices comprising a plurality of mechanisms and means for operating each mechanism to represent a shorter series of symbols, the number of symbols being different in at least two of each of the shorter series and the series being retraversed as it is exhausted.

15. A device for enciphering and deciphering messages comprising two controlling devices, a key tape for operating each device, each key tape bearing a series of code symbols, the number of symbols on one tape differing from that on the other, and mechanism under the joint control of said devices for indicating the enciphered or deciphered message characters.

16. A device for enciphering or deciphering messages comprising two key tapes in the form of closed loops bearing character symbols thereon the number on one tape differing from that on the other, a set of electrical contacts under the control of each tape for representing successively the symbols thereon, a set of contacts for representing successively the characters of the message and mechanism responsive to all three sets of contacts for indicating the characters of the enciphered or deciphered message.

17. A device for enciphering and deciphering messages, comprising two key tapes in the form of closed loops bearing character symbols, of unequal number on the two tapes, a set of contacts under the control of each key tape for representing the successive characters indicated thereon, a group of relays whose windings are controlled respectively by the corresponding contacts in said sets, a group of contacts for successively representing the characters of the message, and mechanism responsive to the condition of said relays and said last mentioned set of contacts for indicating the characters of the enciphered or deciphered message.

In testimony whereof I have signed my name to this specification this thirtieth day of November, 1918.

LYMAN F. MOREHOUSE.