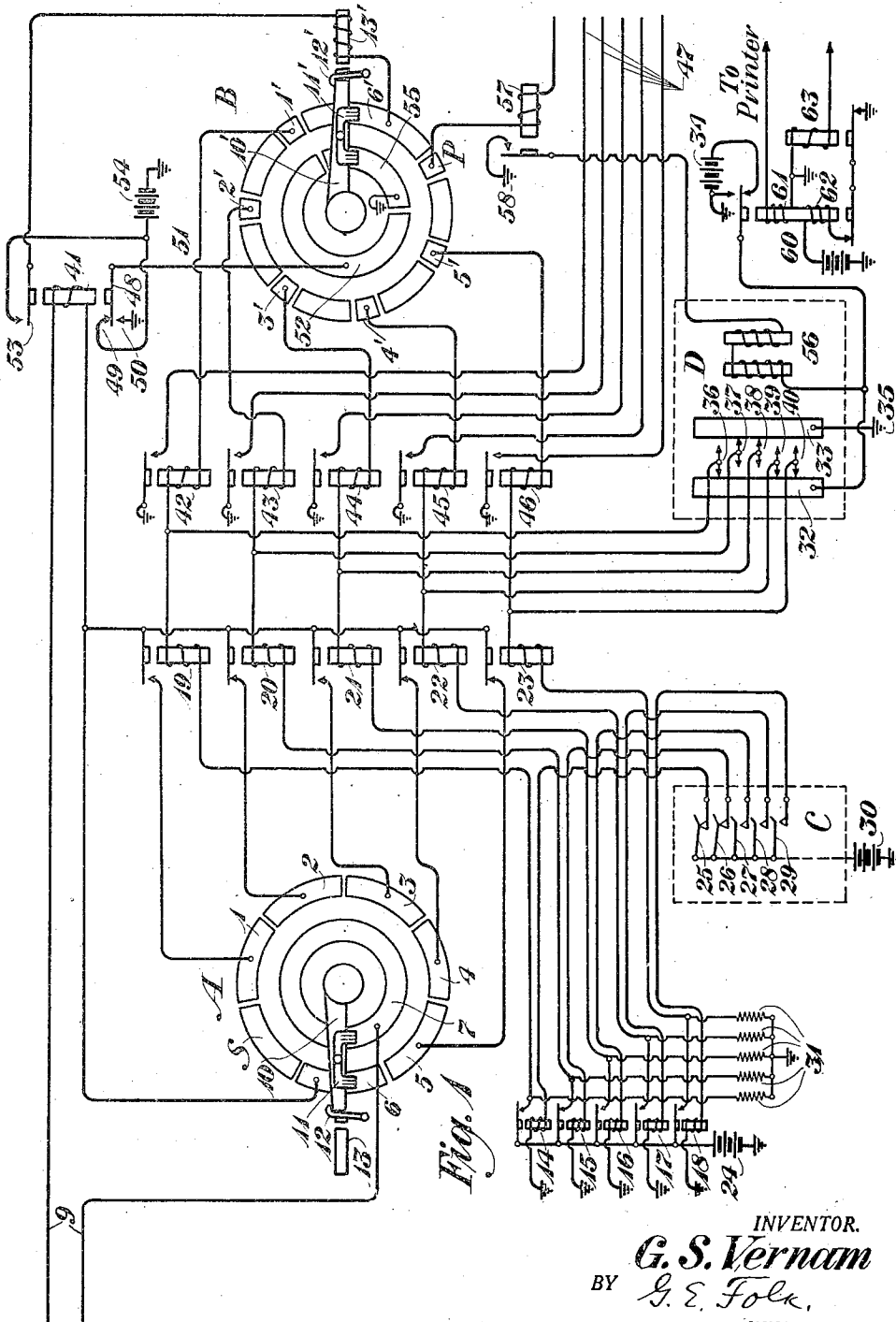


G. S. VERNAM.
 SECRET SIGNALING SYSTEM.
 APPLICATION FILED SEPT. 13, 1918.

1,310,719.

Patented July 22, 1919.

2 SHEETS—SHEET 1.



INVENTOR.
G. S. Vernam
 BY *G. E. Folk*,
 ATTORNEY

G. S. VERNAM.
SECRET SIGNALING SYSTEM.
APPLICATION FILED SEPT. 13, 1918.

1,310,719.

Patented July 22, 1919.
2 SHEETS—SHEET 2.

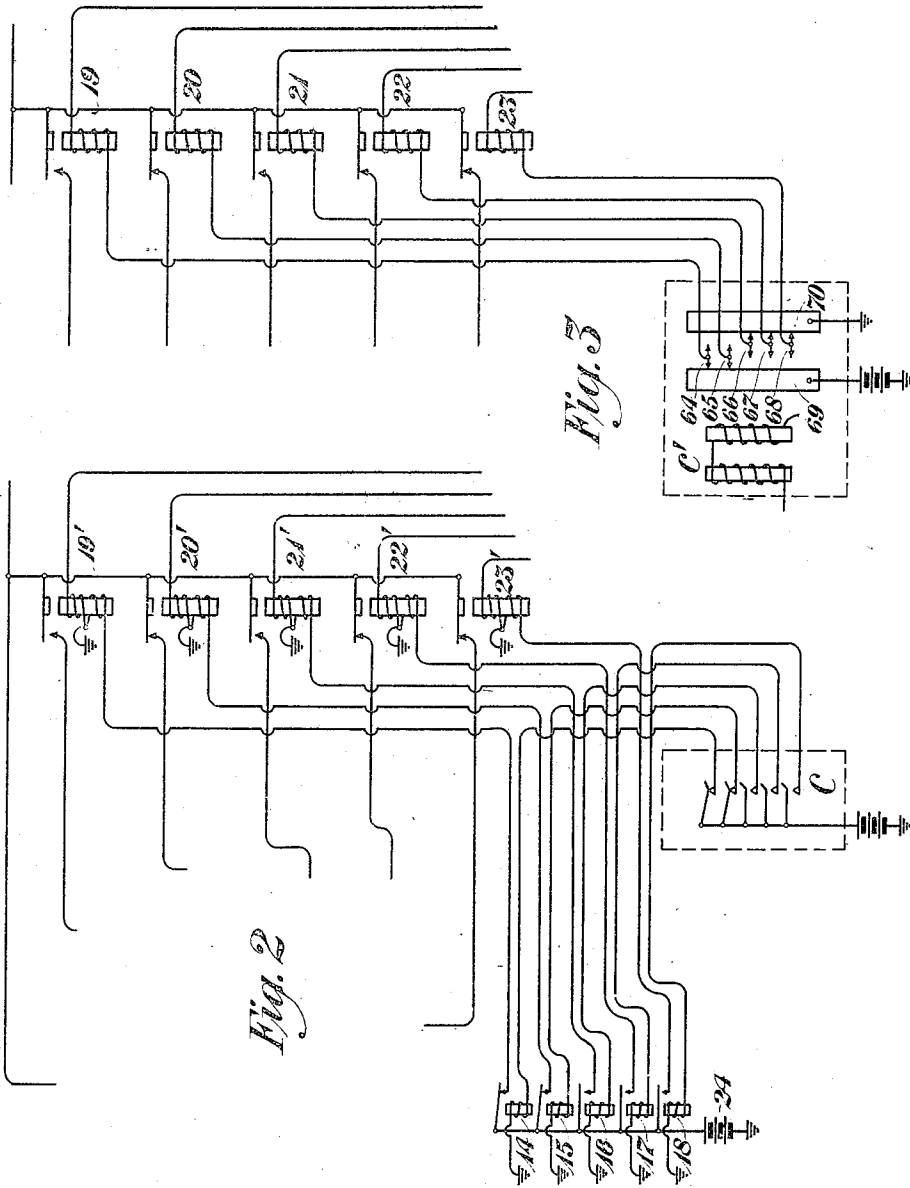


Fig. 3

Fig. 2

INVENTOR.
G. S. Vernam
BY *G. E. Folk*
ATTORNEY.

UNITED STATES PATENT OFFICE.

GILBERT S. VERNAM, OF BROOKLYN, NEW YORK, ASSIGNOR TO AMERICAN TELEPHONE AND TELEGRAPH COMPANY, A CORPORATION OF NEW YORK.

SECRET SIGNALING SYSTEM.

1,310,719.

Specification of Letters Patent. Patented July 22, 1919.

Application filed September 13, 1913. Serial No. 253,962.

To all whom it may concern:

Be it known that I, GILBERT S. VERNAM, residing at Brooklyn, in the county of Kings and State of New York, have invented certain Improvements in Secret Signaling Systems, of which the following is a specification.

This invention relates to signaling systems and especially to telegraph systems. Its object is to insure secrecy in the transmission of messages and, further, to provide a system in which messages may be transmitted and received in plain characters or a well-known code but in which the signaling impulses are so altered before transmission over the line that they are unintelligible to anyone intercepting them.

The invention is here illustrated as applied to a well-known form of printing telegraph systems but, as will be readily understood, it is applicable to other signaling systems. The invention will be more fully described in connection with the accompanying drawings, in which Figure 1 illustrates circuit arrangements at one end of the line in a system embodying the invention, and Figs. 2 and 3 show modifications in the circuits of the sending apparatus.

Like sending and receiving apparatus is located at each end of the line. Normally the message is recorded by both the local and the distant receiving apparatus and since their operation is identical it will be unnecessary to show and describe the opposite end of the line.

Referring to Fig. 1, A and B represent the transmitting and receiving faces respectively of a known form of distributor used in printing telegraph systems. Only such parts of the distributor and such parts of the circuit of the known apparatus are here illustrated as are necessary to an understanding of the present invention. Accordingly only two of the usual four rows of segments on the distributor are shown. The outer row on the transmitting side comprises five segments 1, 2, 3, 4 and 5 from which the code impulses are transmitted. It also includes the segment 6 on which the distributor arm normally rests, and the starting segment S. The inner contact ring 7 is continuous and is connected to one side of the transmitting circuit 9 which is normally closed through a suitable source of current not shown. The distributor arm 10 carries a brush 11 whose opposite ends con-

tact with the ring 7 and the segmental contacts respectively. When the apparatus is at rest this arm is detained by the latch 12 which may be withdrawn by means of magnet 13 under the control of the operator. The receiving side of the distributor has five segments 1', 2', 3', 4' and 5', corresponding to the five sending segments but shortened to receive only the central part of the current impulses transmitted. It also has a contact 6', upon which the distributor arm normally rests, and a contact P for controlling the energization of a relay whose purpose will appear hereinafter. The receiving distributor arm 10' carries a brush 11' and is controlled by a latch 12' and magnet 13' as in the case of the transmitting distributor arm.

The "sending relays" commonly used in the form of printing telegraph system here shown are indicated at 14, 15, 16, 17 and 18. The circuits controlled by these relays ordinarily run directly to the distributor segments 1 to 5 for transmitting the signal impulses. In accordance with this invention, however, these sending relays control the circuits to the distributor segments through another set of relays 19, 20, 21, 22 and 23 which may be called "cipher sending relays." The circuits through the contacts of relays 14 to 18 accordingly run from the source of current 24 through the windings of the relays 19 to 23 and thence to an automatic ciphering device D.

The relays 14 to 18 are under the control of a sending device here indicated at C as a known form of keyboard transmitter, which is provided with a set of contacts 25, 26, 27, 28 and 29, these being under the control of the key levers of the keyboard, as is well understood. The circuit of each of the relays 14 to 18 runs from ground through one of these contacts and to a source of current 30. The relays are in actual practice provided with locking windings, not shown, which facilitate the transmitting of the message; and their circuits are furthermore usually arranged to be transferred at will to the contacts of a tape transmitter which may be used instead of the keyboard transmitter, all as is now well known in the art. The circuit of each of the relays 19 to 23 is provided with a branch to ground through a resistance 31, to enable the relays to be controlled by the ciphering device as will appear hereinafter.

For automatically ciphering the message a well-known form of tape transmitter D may be employed. This transmitter, is provided as usual with two bus-bars 32 and 33, connected respectively to battery and ground at 34 and 35 respectively. Five contacts 36, 37, 38, 39 and 40 vibrate between these bus-bars under the control of a perforated tape in a well-known manner, and the circuits of the five relays 19 to 23 run to these five contacts respectively, so that the energization of the relays depends upon the combined action of the normal transmitter C and the ciphering transmitter D.

The apparatus for receiving the message at the other end of the line is, as above stated, in all respects like that shown at the right hand end of Fig. 1 and it will therefore be explained by reference thereto. In order that the message may be received in plain characters the printer (not shown) is operated through a set of receiving relays 42, 43, 44, 45 and 46, which in turn are under the combined control of the line relay 41 and the deciphering device D, the latter being the same instrument as the ciphering device at the sending end of the line, and at the other end a similar device operating synchronously and with an identical control tape. The windings of relays 42 to 46 are connected on one side to the contacts 36 to 40 respectively of the ciphering device D, and on the other side to the segments 1' to 5' of the receiving distributor.

The line relay 41 controls the armature 48, which has front and back contacts 49 and 50 connected to battery and ground respectively. A conductor 51 connects the armature 48 and the inner segment 52 of the distributor, which is angularly co-extensive with the contacts 1' to 5'. The line relay also has an armature 53 which closes at proper intervals the normally open circuit of the starting magnet 13' of the distributor.

The operating magnet 56 of the ciphering and deciphering device is under the control of the relay 57, which is energized from the distributor contact P, its winding being connected between the grounded contact 55 and a source of current at the printer (not shown) whenever the brush 11' passes over the contact P. The circuit of magnet 56 is thereby closed from ground at 58 to battery at 34 once for each revolution of the distributor to feed the tape and set the contacts in a manner now well understood in the art. It is obvious that the impulses to the ciphering and deciphering devices at opposite ends of the line may step the tapes forward only for every second or every third character transmitted, or at any other desired interval, instead of for each character.

If desired the ciphering device may be provided with apparatus to throw it into or

out of operation at the will of the transmitting operator. For this purpose I have shown a relay 60 provided with an operating winding 61 and a locking winding 62, the circuit of the locking winding being controlled by a relay 63. The circuits of windings 61 and 63 which respectively throw the ciphering device into and out of operation, run to the printer and are arranged to be there connected to battery by predetermined code signals transmitted over the line.

In the modification shown in Fig. 2, a series of cipher sending relays 19', 20', 21', 22' and 23', provided with differential windings, are used in place of the relays 19 to 23, shown in Fig. 1. One end of each of the windings may conveniently be grounded at the relay while the opposite ends of each pair are connected to the sending and ciphering devices respectively. The windings will neutralize each other when both are energized, but the strength of either winding is sufficient to operate the relay when not opposed by the other. In this modification the ground connections, through the resistance 31 shown in Fig. 1, are unnecessary and are therefore omitted. Otherwise the circuits for this arrangement are the same as in Fig. 1.

In the modification shown in Fig. 3 the sending relays (14 to 18) of the usual printing telegraph system are omitted and the circuits of the relays 19 to 23 are run directly to contacts 64, 65, 66, 67 and 68 of a tape transmitter C' of known form whose bus-bars 69 and 70 are connected to battery and ground respectively. It will be seen that this arrangement, while simplifying the circuits, is not as conveniently applicable to the known form of printing telegraph system indicated in Fig. 1, in which the relays 14 to 18 are already present and arranged to be operated from either a keyboard transmitter or a tape transmitter, depending upon the position of a switch controlled by the operator. By connecting the relay windings directly to a transmitter, as in Fig. 3, these windings will always be connected either to ground or to battery at each end and no separate set of grounded connections as in Fig. 1, is necessary.

The operation of the system shown in Fig. 1 is as follows: The sending arm of the distributor will be started in the usual manner through the operation of the magnet 13 and will transmit an open or "start impulse" as it passes over the segment S of the distributor. This opens the circuit 9, thereby deenergizing the line relay 41, which permits switch 53 to close, whereupon magnet 13' of the receiving distributor is energized. This releases the arm 10' which starts to rotate in approximate synchronism with the sending arm 10. The "start impulse" of course puts into operation the receiving distributor at

both ends of the line simultaneously, or at any other station which may be connected into the line circuit.

Let us suppose that the first character of the message to be transmitted is "A." The code signal of "A" is "+ + - -," where "-" represents an "open" or "spacing" impulse and "+" represents a "closed" or "marking" impulse in the system here illustrated, although it will be understood that positive and negative current impulses may be used instead of closed and open circuit operation if desired. For ciphering and deciphering the message the ciphering devices at the opposite ends of the line are provided with identical sections of tape upon which are recorded a series of code signals which are preferably selected at random but if desired may themselves represent a predetermined series of letters or words. Let us suppose that the letter "B" happens to be in the ciphering transmitter at the same moment that the letter "A" is being sent from the normal transmitter. The code for the letter "B" is "+ - - + +." The sending of "A" from the normal transmitter means that the contacts 25 and 26 will be closed, while the contacts 27, 28 and 29 are open. Thus, relays 14 and 15 will be energized and close their contacts, while relays 16, 17 and 18 remain unenergized. The presence of the letter "B" in the code transmitter means that contacts 36, 39 and 40, representing the plus impulses for "B," will be in contact with the bus-bar 32, which is connected to battery and that contacts 37 and 38, representing the negative impulses for this character will be in contact with bus-bar 33 which is grounded.

As a result of this combination of contacts in the two transmitters, it will be seen that the relay 19 is connected at both ends to battery; that relay 20 is connected at one end to battery at 24 and at the other end to ground at 35; that relay 21 is connected at one end to ground through the resistance 31, and at the other end to ground at 35; that relay 22 is connected at one end to ground through resistance 31, and at the other end to battery at 34, and that relay 23 is connected to ground through the resistance 31 at one end and the battery 34 at the other. Therefore, relays 20, 22 and 23 will close their contacts, and relays 19 and 21 will remain open. Consequently, as the distributor arm 10 rotates over the contacts 1 to 5, impulses will be transmitted to the line from contacts 2, 4 and 5 and none from contacts 1 and 3. This means that the signal "- + - + +" will be transmitted over the line and this signal represents the letter "G" and not the letter "A" which is the character of the message to be transmitted.

The transmitted impulses will be received

at the distant end of the line and at the receiving apparatus of the local station in exactly the same manner, since both are operating with identical ciphering tapes. A reference to the operation of the receiving apparatus B will, therefore, serve to explain the operation at the distant end.

The character to be recorded at the printer depends upon the combination of impulses transmitted to it over the conductors 47. These conductors run to ground through the normally open relay contacts of the relays 42 to 46, and these relays are under the joint control of the contacts of the device D and the contacts 49 to 50 of the line relay 41. Thus in receiving the transmitted signal above referred to, "- + - + +," the absence of an impulse over the line when the transmitting distributor passes the contact 1, leaves the line relay 41 unenergized. The switch 48 is therefore on the back or grounded contact 50. Hence, when the receiving distributor arm passes over the contact 1', the circuit of the relay 42 will be closed from battery 34 through contact 36 of device D, relay winding 42, contact 1', brush 11', segment 52, conductor 51 and to ground at 50. When the distributor arm is passing over the contact 2', the line relay 41 will be energized, due to an impulse transmitted from contact 2 of distributor A through the contact of relay 20. Switch 48 will therefore be on its front or battery contact 49 and relay 43 will therefore be energized, being connected at one end to the battery 54 and at the other end to ground at 35. When the distributor arm is passing over contact 3' the line relay will be again unenergized and the switch 48 upon its grounded contact and the relay 44 will therefore remain unenergized, since it will be connected to ground at both ends. While the arm is passing over contacts 4' and 5' the line relay 41 is energized, due to impulses through the contacts of relays 22 and 23, so that switch 48 is upon its front or battery contact, and relays 45 and 46 therefore remain unenergized, since they are connected at both ends to battery. In other words, relays 42 and 43 are successively closed and transmit impulses to the printer, while relays 44, 45 and 46 remain open.

The code signal upon which the printer operates is therefore, "+ + - -" which is the symbol for the letter "A" and the printer accordingly prints the letter which it was desired to transmit.

As the distributor arm 10' passes the contact P, relay 57 is energized which closes the circuit of magnet 56, thereby feeding the tape one step and readjusting the contacts of the ciphering and deciphering device for the new ciphering letter. If it is

desired to throw the ciphering and deciphering devices out of operation, the operator may transmit a prearranged signal as above suggested, thereby causing an impulse to pass from the printer through the winding of relay 63 to ground. This opens the circuit of the locking winding 62 of the relay 60, which releases its armatures and whereupon both bus-bars of the ciphering device will be connected to ground, bar 33 at 35, and bar 32 at the grounded side of the battery 34. The take feed magnet 56 is likewise rendered inoperative. When it is desired to again throw the ciphering device into operation, another predetermined signal is transmitted, whereupon an impulse passes from the printer through the winding 61 of the relay 60 and to ground, which energizes the relay and re-establishes the connections shown on the drawing.

The operation of the modification shown in Fig. 2 is the same as that just described except that the operation of the relays 19' to 23' will depend upon the combined effect of their two windings instead of upon the effect of the connections at the opposite ends of a signal winding. Thus if both of the windings of any relay are connected to battery at the normal and ciphering transmitters respectively, the relay will remain unoperated because the magnetic effects of the two windings will neutralize each other. If they are both either open or grounded at the opposite ends, the relay will, of course, not operate, but if either winding is connected to battery while the other is grounded or open-circuited, the relay will operate, and obviously the circuit conditions which make a relay operate in Fig. 1 will likewise make it operate in Fig. 2. No separate description of the details of the operation in connection with this figure is therefore necessary. The use of the grounded differential windings does away with the necessity for the resistances 31 shown in Fig. 1, since there is always a ground connection for any winding connected at the opposite end to battery.

The operation of the modification shown in Fig. 3 will be clear from the foregoing description. The ends of the relay windings 19 to 23, which run to the normal transmitter C' will always be connected either to battery or to ground, depending upon the position of the contacts 64 to 68 and there is, therefore, no need of the resistances 31 shown in Fig. 1.

The system as above described will therefore serve to change the impulses of the character to be transmitted into another set of impulses representing some other character of the same code and anyone attempting to intercept the message by tapping the

wires will receive the impulses so altered. A consideration of the circuits will show that even if the contacts of the ciphering transmitter are left in one position, a series of varying characters will be transmitted by the line which are different from the characters of the message to be sent, while if the contacts of the code transmitter are altered by shifting the tape thereof each time a letter of the message is to be transmitted, the rule by which the variation made will be changed for each letter, in other words the cipher employed will be changed for each letter transmitted. It will also be clear that the set of impulses actually transmitted may represent some printer operation other than the printing of a letter, such as the line shift or carriage return when a letter is in the normal transmitter. So that a printer tapped onto the line would show an indescribable confusion of signals unless it were provided with a deciphering device and was using the same deciphering tape as used at the transmitting station.

It is obvious, of course, that the invention here disclosed is equally applicable to transmission through any known medium and is, therefore, suitable for either wire or wireless transmission.

The forms of the invention here shown are illustrative only, as it will be obvious that various modifications may be made without departing from the spirit of the invention or the scope of the appended claims.

What is claimed is:

1. The method of enciphering signals where the characters are represented by a number of periods of different current values which consists in altering the normal code impulses of a character to be transmitted in accordance with a rule represented by some other character in a like code.

2. The method of transmitting messages where the characters are represented by a number of periods of different current values, which consists in altering the normal code impulses of a character in accordance with a rule represented by some other character in a like code, and restoring the transmitted impulses so produced to their normal code form at the receiving end by altering the received impulses in accordance with a rule represented by the same character.

3. The method of transmitting messages where the characters are represented by a number of periods of different current values, which consists in altering the normal code impulses of a character in accordance with a rule represented by some other character in a like code, restoring the transmitted impulses so produced to their normal code form at the receiving end by alter-

ing the received impulses in accordance with a rule represented by the same character, and correspondingly changing the rule of alteration and restoration at both ends of the line at frequent intervals.

4. The method of enciphering signals which consist in combining the effect of electrical conditions representing the message character, with the effect of those representing a ciphering character, to produce electrical impulses representing some other character.

5. The method of enciphering signals which consists in combining the effect of electrical conditions representing the message character, with the effect of those representing a ciphering character, to produce electrical impulses representing some other character, and changing the ciphering character from time to time.

6. The method of deciphering a secret message, which consists in combining the electrical effect of the received impulses with the effect of the electrical conditions representing a deciphering character to produce electrical impulses representing the message character.

7. The method of deciphering a secret message, which consists in combining the electrical effect of the received impulses with the effect of the electrical conditions representing a deciphering character to produce electrical impulses representing the message character, and changing the deciphering character at intervals, to correspond with the ciphering character used in transmitting the message.

8. The method of transmitting signals, which consists in producing a set of electrical conditions appropriate for transmitting a character of the message according to an accepted code, producing a second set of arbitrarily chosen electrical conditions, combining the electrical effects of the two sets of conditions to produce a third set of electrical conditions, and transmitting impulses corresponding to said third set of conditions.

9. The method of transmitting messages, which consists in producing a set of electrical conditions appropriate for transmitting a character of the message according to an accepted code, producing a second set of arbitrarily chosen electrical conditions, combining the electrical effects of the two sets of conditions to produce a third set of electrical conditions, transmitting impulses corresponding to said third set of conditions and changing the second set of electrical conditions from time to time during the transmission of the messages.

10. The method of transmitting messages which consists in producing a set of electrical conditions appropriate for transmitting a character of the message according to an accepted code, producing a second set of

arbitrarily chosen electrical conditions, combining the effects of the two sets of conditions to produce a third set of electrical conditions, transmitting impulses corresponding to said third set of conditions, producing at the receiving station a deciphering set of electrical conditions corresponding to said second set and combining the electrical effects of these conditions with the electrical effect of the transmitted impulses, to produce a set of impulses representing the message character.

11. The method of transmitting messages which consists in producing a set of electrical conditions appropriate for transmitting a character of the message according to an accepted code, producing a set of arbitrarily chosen electrical conditions of like kind for enciphering the character, combining the effects of the two sets of conditions to produce a third set of electrical conditions, transmitting impulses corresponding to said third set of conditions, producing at the receiving station a deciphering set of electrical conditions corresponding to said second set, combining the electrical effects of these conditions with the electrical effect of the transmitted impulses, to produce a set of impulses representing the message character and correspondingly changing the enciphering and deciphering sets of conditions at intervals.

12. The method of transmitting messages, which consists in producing electrical conditions suitable for representing a character of the message, altering the effect of these conditions by and in accordance with the electrical conditions representing some other character, transmitting impulses according to said altered effect and reproducing at the receiving end the original electrical conditions by altering the effect of the transmitted impulses by and in accordance with electrical conditions representing the same character as the conditions used to effect the alteration at the transmitting end of the line.

13. In an electrical signaling system, a set of contacts arranged to be closed in accordance with a pre-determined code for representing characters; a similar set of contacts arranged to be closed in like manner; a third set of contacts, means for closing any or all of said third set of contacts to correspond with the relative positions of corresponding contacts in said first and second mentioned sets, and means for transmitting impulses to the line in accordance with the arrangement of said third set of contacts.

14. In an electrical signaling system, a set of relays for controlling the impulses transmitted to the line, means for connecting either end of any relay winding of said set to either pole of a current source, and means for transmitting impulses to the line in accordance with the circuit conditions

produced by said relays under the varying connections for their windings thus produced.

15 15. In an electrical signaling system, a set of relays for controlling the impulses transmitted to the line, two sets of winding terminals for said relays, means for applying differing electrical potentials to the terminals in either set to make the sets correspond with predetermined code signals one of which represents the message characters and means for transmitting impulses to the line in accordance with the circuit conditions established by the relays.

15 16. In a signal transmitting system, two sets of contacts, any one of which may be connected to either pole of a current source, whereby either set may represent any character of a code depending on the arrangement of its contacts, relays having windings connected between corresponding contacts in the two sets and means for sending current impulses through the contacts controlled by said relays.

25 17. In a device for automatically enciphering messages, the combination of switching mechanism for making sets of electrical connections to current sources of differing potential thereby representing the successive characters of the message, other switching mechanism for making other sets of electrical connections, circuits connecting the corresponding contacts in the two sets of connections and means controlled by the current in said circuits for governing the combination of impulses transmitted to the line.

18. In a device for automatically deciphering messages, a combination of switching mechanism for making sets of electrical connections corresponding to the connections used in ciphering the message, means responsive to the received impulses for altering the condition of a local circuit, and means for combining the effect of the electrical condition of the local circuit under successive line impulses with the effect of the conditions produced in said switching mechanism, whereby a set of impulses is created corresponding to the message character.

19. In a signal receiving instrument, switching mechanism for determining the code impulses to be recorded, a line relay responsive to the received impulses, a set of terminals whose electrical condition relative to each other may be varied to represent ciphering symbols, and means under the combined influence of said relay and said set of terminals for controlling said switching mechanism.

20. In a signal receiving instrument, a plurality of circuits for controlling the re-

65 cording of characters, a relay for controlling each of said circuits, a deciphering device arranged to connect one terminal of each of said relays to either pole of a source of current, a distributor for connecting the opposite terminal of each of said relays successively to a single circuit, and a line relay responsive to receive impulses for connecting said single circuit to either pole of a source of current, according to the character of the impulse received.

21. In a signaling system, a main circuit, a plurality of branch circuits, a distributor for connecting the main circuit with said branch circuits successively, switching mechanism in said branch circuits for determining the character of the impulse transmitted over the main circuit when connected to the respective branch circuits, two controlling devices either one of which may transmit impulses representing code characters, and connections between said controlling devices and said switching mechanism whereby the switching mechanism may be operated by said controlling devices separately or in accordance with their combined effect.

22. In a signal transmitting system, means for transmitting normal code impulses over the line, ciphering and deciphering devices at opposite ends of the line for automatically altering the impulses to transform them into a different character and restoring them at the receiving end of the line, and means for throwing said devices into and out of operation by the transmission of predetermined signals over the line.

23. In a signaling system, a main line, mechanism at each end of said line for sending and receiving messages, ciphering and deciphering devices at opposite ends of said line and associated with said mechanism for automatically ciphering the message at the transmitting end and for deciphering it at the receiving end, and means for throwing the ciphering and deciphering devices into or out of operation in response to the transmission of a predetermined signal over the line.

24. In a signal transmitting system, a sending and receiving mechanism comprising a set of relays controlling the impulses imposed upon the line, another set of relays for controlling the impulses sent to the recording mechanism, a ciphering and deciphering device connected to both sets of relays whereby the message to be sent is enciphered for transmission and received messages are deciphered by the same device.

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

GILBERT S. VERNAM.