July 18, 1961 F. NEGRI 2,993,089

ENCIPHERING AND DECIPHERING APPARATUS FOR SECRET TELEGRAPH SYSTEMS

Filed Dec. 1, 1958 2 Sheets-Sheet 1

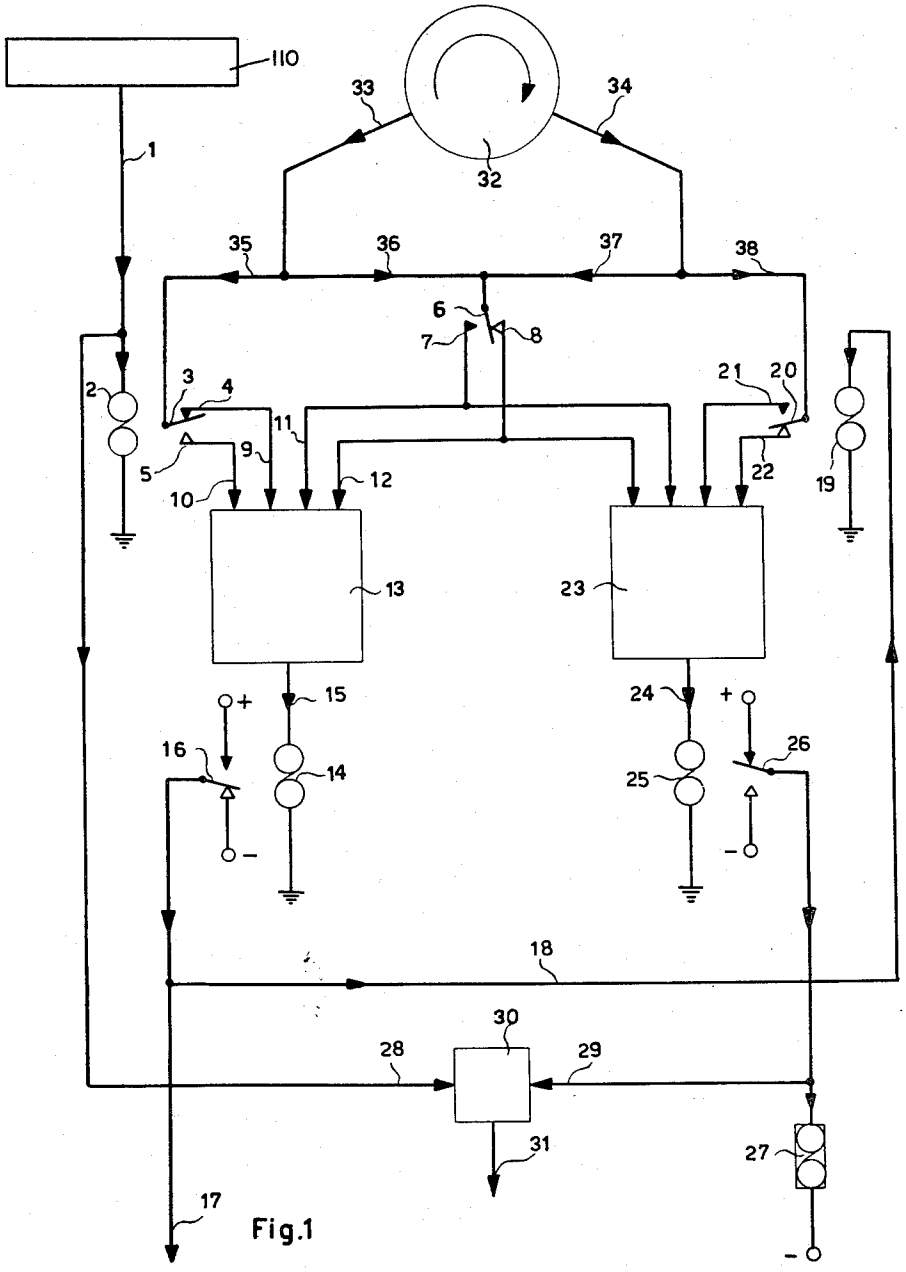



Fig.1

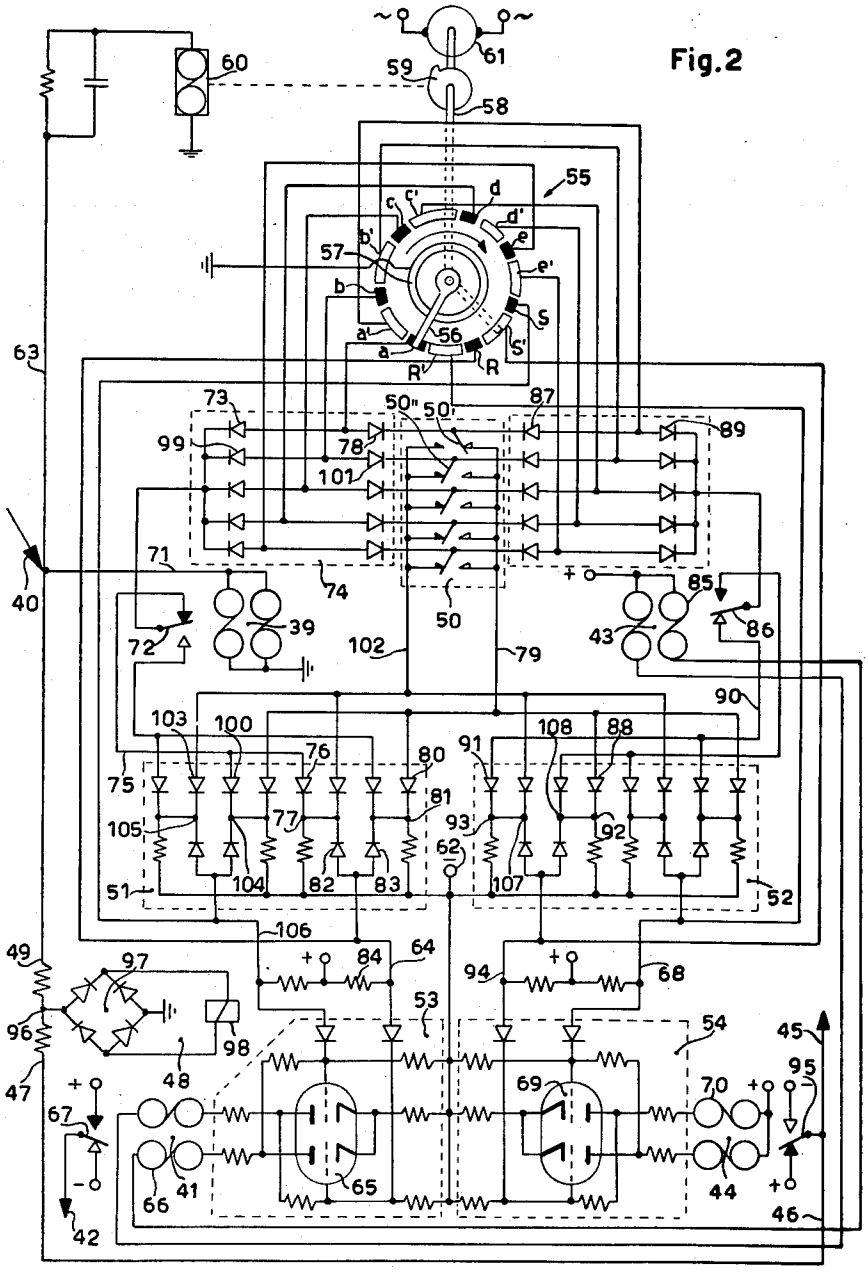
INVENTOR.
Franco Negri
BY Kenyon and Kenyon

July 18, 1961 F. NEGRI 2,993,089

ENCIPHERING AND DECIPHERING APPARATUS FOR SECRET TELEGRAPH SYSTEMS

Filed Dec. 1, 1958 2 Sheets-Sheet 2

Fig.2




INVENTOR.
Franco Negri
BY Kenyon and Kenyon

United States Patent Office 2,993,089 Patented July 18, 1961



2,993,089

# ENCIPHERING AND DECIPHERING APPARATUS FOR SECRET TELEGRAPH SYSTEMS

Franco Negri, Ivrea, Italy, assignor to Ing. C. Olivetti & C., S.p.A., Ivrea, Italy, a corporation of Italy

Filed Dec. 1, 1958, Ser. No. 777,309
Claims priority, application Italy Nov. 30, 1957
3 Claims. (Cl. 178—22)

This invention relates to secret telegraph systems and more particularly to an enciphering and deciphering apparatus of the kind adapted for use in connection with a teletypewriter of the start-stop type.

According to a known practice the code combinations representing characters of a clear message are altered in polarity and order of sequence by means of mechanical or electromechanical cipher elements, such as cipher disks, whereby the electric signals generated by the transmitter represent the enciphered code combinations to be sent over the telegraph line. To decipher the message at a distant receiver, the enciphered code combinations are altered by similar cipher elements controlling the conventional selector of the printer in order to be deciphered and thus restored to their original form according to the clear message. Of course, the signals generated by the transmitter may also be sent to a local receiver to print a deciphered control message affording control both of the original clear message and of the correctness of the enciphering operation.

To increase the secrecy of the system there have been proposed enciphering apparatus wherein the code combinations representing characters of a clear message are mixed or scrambled with arbitrary code combinations representing characters of a key message, the resulting enciphered code combinations being transmitted to the telegraph line. To decipher the message at the distant receiver, the message is mixed with a similar key message, whereby the resultant code combinations are restored to their original form according to the clear message.

In the enciphering apparatus of this type the signals of the clear message are generally generated at the transmitting station by the transmitter of a teletypewriter or by a main tape transmitter, whereas the signals of the key message are generated by an auxiliary transmitter fed by a tape punched according to the key message and operated in synchronism with the teletypewriter or the main tape transmitter. The signals of the clear message and of the key message are then pulsewise mixed according to a predetermined law by an electric mixing circuit adapted to drive the usual telegraph relay controlling the telegraph line. At the local receiver the clear message is generally recorded by directly detecting the signals generated by the transmitter of the teletypewriter or by the main tape transmitter, whereby no control is made for the correctness of the enciphering operation. If any damage occurs to the mixing circuit of the enciphering apparatus the enciphering operation may be faulty, however, without preventing the resulting code combinations from being further transmitted to the line. In this case the operator at the transmitting station will not detect the faulty transmission and the message received at the receiving station will be unintelligible.

The primary object of the present invention is to provide an improved enciphering and deciphering apparatus operating in a pure electrical way.

A more specific object of the invention is to provide an enciphering apparatus of the kind referred to wherein the correctness of the enciphering operation may be easily controlled at the transmitting station.

Still another object of the invention is to provide an enciphering apparatus wherein the transmission may be discontinued as soon as the enciphering operation proves to be incorrect.



According to the invention, in a secret telegraph system of the start-stop type including a transmitting station I now provide an enciphering and deciphering apparatus in said station comprising means for generating electric pulses according to clear code combinations, means for generating electric pulses according to key code combinations, a first electric circuit for pulsewise mixing a clear code combination with a key code combination to generate a resulting enciphered code combination, a second electric circuit for pulsewise mixing said enciphered code combination with said key code combination to generate a resulting deciphered code combination, and means for locally controlling the operation of the enciphering apparatus by detecting the resulting deciphered code combination.

It will be understood that the enciphering and deciphering apparatus according to the present invention is adapted to encipher the clear message and to transmit the enciphered message to the line, and simultaneously to decipher the enciphered message and to print the deciphered message at the local receiver as a control clear message, one and a single key tape being used in the transmitting station both for enciphering the clear message and for deciphering the enciphered message.

Other objects, features and advantages of the invention will become apparent from the following description, taken in conjunction with the accompanying drawings wherein:

FIG. 1 is a diagrammatic representation in block form of an enciphering and deciphering apparatus embodying the object of the invention;

FIG. 2 illustrates the detailed electric circuits of the apparatus of FIG. 1.

With reference to FIG. 1, the numeral **1** indicates an electric conductor by means of which the signals of the code combinations of the clear message, generated in form of electric pulses at the transmitting station by the transmitter **110** of a teletypewriter or by a punched tape transmitter operating according to the start-stop system, are fed to a telegraphic relay **2**, which upon receiving a positive pulse will bring its tongue **3** on the marking contact **4**, and upon receiving a negative pulse will move its tongue **3** to the spacing contact **5**.

The numeral **6** indicates a means for generating electric pulses according to code combinations of the key message, said means being formed of the tongue of the telegraph relay of an auxiliary transmitter fed by a key tape punched according to arbitrary code combinations. The tongue **6** is moved to the marking contact **7** by the positive pulses and is moved to the spacing contact **8** by the negative pulses of the code combinations of the key message.

The numeral **13** indicates a first electric mixing circuit or mixer, the inputs **9**, **10**, **11**, **12** of which are connected to the contacts **4**, **5**, **7** and **8**, respectively to receive the clear message and the key message. This mixer is of a known type and is adapted to mix the two messages according to a predetermined law and to correspondingly control a telegraph relay **14** through its output **15**. According to said law two pulses having like polarity generate a pulse having a certain polarity, for instance, a positive one, and two pulses having unlike polarity generate a pulse having the opposite polarity, namely a negative one.

The enciphered message leaving the mixer **13** through the output **15** is transmitted by the tongue **16** of relay **14** over a telegraph line **17**.

The tongue **16** is further connected to a telegraph relay **19** by means of a conductor **18**. The pulses sent over the line **17** by relay **14** are thus simultaneously repeated

by the relay 19. The tongue 20 of the latter, upon receiving a positive pulse will contact the marking contact 21, and upon receiving a negative pulse will contact the spacing contact 22.

According to the main feature of the invention a second electric mixing circuit or mixer 23, identical to the mixer 13, is adapted to receive the enciphered message through contacts 21 and 22 and the key message through the contacts 7 and 8. In said mixer 23 the enciphered message and the key message are again mixed according to the same predetermined law; the resulting deciphered message leaving the output 24 should be in accordance with the clear message fed through the conductor 1, and may be used to control operation of the apparatus.

A telegraph relay 25, operable through the output 24, energizes by means of its tongue 26 a selector magnet 27 conditioned to drive for instance, the receiving apparatus of the local telegraph station, where the control message leaving the mixer 23 will be typed as a clear message, thus allowing the operator to control the deciphered message during the transmission of the ciphered message over the line 17.

According to a further feature of the invention, the deciphered control message and the clear message may be automatically compared to detect any discrepancy therebetween. To this purpose, there is provided a comparator 30 adapted to receive on its input 29 the deciphered control message and on its input 28 the clear message. The comparator 30, which may be of any known kind, is conditioned to generate an alarm signal when the two pulses of a pair of pulses arriving on the two inputs are of opposite polarity. This alarm signal may operate, through the output 31, a means adapted to discontinue the operation of the enciphering apparatus and to switch on a signalling means, for example an electric lamp.

The numeral 32 designates a timing means, such as a distributor, adapted to alternately operate the mixers 13 and 23, so that each pulse of a code combination of the clear message is first enciphered by the mixer 13 and immediately deciphered by the mixer 23. Said distributor may be of the conventional rotatable kind or of an electronic kind and is adapted to alternately energize the outputs 33 and 34 in order to generate two sequential pulses concurrently with each pulse of a code combination of the clear message.

A pulse generated on the output 33 is conveyed to the tongue 3 through the conductor 35 and to the tongue 6 through the conductor 36. By means of these tongues the pulse is thus simultaneously applied to a selected pair of inputs of the mixer 13.

Similarly, a pulse generated on the output 34 is conveyed to the tongue 6 through the conductor 37 and to the tongue 20 through the conductor 38. By means of these tongues the pulse is thus simultaneously applied to a selected pair of inputs of the mixer 23.

More particularly, if a pulse of a code combination of the clear message is positive and the corresponding pulse of the corresponding code combination in the key message is negative, the tongues 3 and 6 will occupy the position shown in FIG. 1. Consequently, the pulse generated on the output 33 of the distributor 32 is conveyed to the mixer 13 through the two inputs 9 and 12, and a negative signal will appear on the output 15 of the mixer 13 according to the above recited law. This operation causes the relay 14 to move its tongue 16 to the spacing contact and to send a negative pulse over the line 17, said pulse forming an element of the enciphered code combination. At the same time, this negative pulse is conveyed to the relay 19, causing the same to move its tongue 20 to the spacing contact 22. The pulse generated on the output 34 of the distributor 32 is conveyed to the mixer 23 through a pair of inputs corresponding to a pair of negative pulses of the key message and of the enciphered message. According to the recited law, a positive pulse will appear on the output 24 of the mixer 23, causing the relay 25 to send a positive pulse to the comparator 30 and to the selector magnet 27, said pulse forming an element of the deciphered code combination.

It will be readily apparent that the hereinabove disclosed apparatus allows an immediate and easy control of the enciphering operation, a discrepancy between corresponding elements of said enciphered and deciphered code combinations indicating that a failure or damage has occurred in the apparatus.

FIGURE 2 shows the detailed electric circuits of an enciphering and deciphering apparatus operating according to the block representation of FIG. 1 and embodied in a transmitting station of a telegraph system of the start-stop type.

Standard components, such as inserting devices, batteries, jacks, condensers, resistors, etc., necessary for the correct operation of the circuit, have been left out.

The numeral 39 indicates a telegraph relay controlled by the clear message entering from 40; the numeral 41 indicates a telegraph relay for transmitting the enciphered message to the line 42; the numeral 43 designates a telegraph relay repeating the signals received from relay 41 and the numeral 44 indicates the local receiving relay fed with the deciphered message. The relay 44 through the conductor 45 is connected to the local printer of the station and is further connected through the conductor 46 to the input 47 of a comparator 48 formed of a bridge of diodes 97 driving a relay 98. A second input 49 of the comparator 48 conveys thereto the clear message. The relays 39, 41, 43, 44 are of the polarized type having one pair of windings.

The numeral 50 designates the conventional set of five code contacts of an auxilliary transmitter fed with a tape punched according to the key message.

In the present embodiment the two mixers operate electronically and comprise a diode binary adding circuits 51 and 52, respectively, and flip-flops 53 and 54, respectively. The flip-flops are of the Eccles-Jordan type and are adapted to staticise the pulses generated by the respective adding circuits, in order to send properly rectangular shaped pulses to the relays 41, respectively 44.

The numeral 55 designates a timing means, such as a rotary distributor comprising a rotating brush 56, a grounded ring 57, a first set of sequential elements, such as contact segments R, *a*, *b*, *c*, *d*, *e*, S corresponding in the order to the start element, five code elements and stop element of the five-unit start-stop code, and a second set of sequential elements, such as contact segments R', *a'*, *b'*, *c'*, *d'*, *e'*, S' interspersed with the segments of the first set and having a similar significance. By inspecting FIG. 2 it will be clear that each set of segments is connected to the transmitter 50, each segment of each set corresponding to an element of a code combination.

The brush 56 is carried by a shaft 58 which may be connected for one revolution to the electric motor 61 through a one revolution clutch 59 controlled by a start relay 60. Since the brush 56 is grounded through the ring 57, the adding circuits 51 and 52 and the flip-flops 53 and 54 are negatively polarized through the terminal 62, so that positive pulses will be sent by the contact segments during a revolution of said shaft 58.

The apparatus operates as follows:

The start pulse of a code combination of the clear message generated by a main transmitter of the transmitting station and arriving at 40 throughout the conductor 63, will energize the start relay 60, thus disengaging the clutch 59 and starting a cycle of the distributor 55, which will thus be operated synchronously with the main transmitter. The brush 56, which at rest contacted the stop segment S' (position shown in dotted lines in FIG. 2) contacts now the segment R, thus generating a positive pulse on the input 64 of the flip-flop 53. This pulse energizes the lower section of the double triode 65 and thus the lower winding 66 of the relay 41, which will

move its tongue 67 to the spacing position, thus sending a nonenciphered negative start pulse over the line 42.

During its further revolution the brush 56 contacts the segment R', whereby a positive pulse is sent to the input 68 of the flip-flop 54, thus energizing the upper section of the double triode 69 and the upper winding 70 of the relay 44 which will transmit a negative start pulse to the local receiver.

The following pulses of the clear combination will energize the relay 39 through the conductor 71, while the code contacts 50 are in turn positioned by the pulses of the corresponding code combination of the key message. More particularly, FIG. 2 is drawn to the first code pulse, which is assumed to be positive in the clear message and negative in the key message, as referred to in the example of FIG. 1. Consequently, the tongue 72 of the relay 39 will assume the marking position whereas the first tongue 50' of the auxiliary transmitter will assume the spacing position. The brush 56 contacts now the segment *a*.

In this case, the conection 77 of the first adding circuit 51 will be grounded through segment *a*, diode 73 of a matrix of diodes 74, tongue 72, conductor 75 and diode 76; a second connection 81 of the same adding circuit 51 will also be grounded through segment *a*, diode 78 of the matrix 74, tongue 50', conductor 79 and diode 80. The connections 77 and 81, normally energized negatively through the terminals 62, are now simultaneously energized by two positive pulses, whereby a positive pulse will be generated on the input 64 of the flip-flop 53, this input being connected to said connections 77, 81 by a gate formed of the diodes 82 and 83 and the resistor 84.

In response to said positive pulse the relay 41 will send a negative pulse over the telegraph line 42; this pulse is the first enciphered pulse of the clear code combination to be enciphered.

Since the winding 66 of the relay 41 is connected in series with a winding 85 of the relay 43, the latter will be energized together with the relay 41 and the tongue 86 will be moved to the spacing position, as shown in FIG. 2.

The brush 56 of the distributor 55 is now contacting the segment *a'*, whereby a positive pulse is similarly sent to the connection 92 of the second adding circuit 52 through diode 87, tongue 50', conductor 79, diode 88 and to the connection 93 of the adding circuit 52 through diode 89, tongue 86, conductor 90, diode 91. Due to the coincidence of these two positive pulses a positive pulse is generated on the input 94 of the flip-flop 54, thus energizing the lower sections of the double triode 69. Consequently, the lower winding of the relay 44 is energized and its tongue 95 moves to the marking position, thus generating a positive pulse.

This pulse, which has been obtained by mixing the original clear pulse twice with the key pulse, is sent to the local receiver through the conductor 45 and is furthermore compared with the original clear pulse in the comparator 48. As long as the pair of pulses conveyed by the conductors 47 and 49 are of the same polarity, the connection 96 of the comparator 48 receives an alternating voltage which is rectified by the bridge 97, thus energizing the relay 98, which in the present embodiment is a time delayed relay.

If owing to a failure or damage in the apparatus, especially in the mixing circuits, the compared pulses will not be coincident the voltage in the connection 96 drops to zero, thus causing the relay 98 to be deenergized. This interruption may be used to discontinue the operation of the apparatus and to operate an acoustical or optical warning signal.

Assuming now that the second pulse both of the clear code combination and of the key code combination is positive, the segment *b* will send a positive pulse to the connection 104 of the adding circuit 51 through diode 99, tongue 72, conductor 75, diode 100 and to the connection 105 of the adding circuit 51 through diode 101, tongue 50'', conductor 102, diode 103. Since these two pulses are of the same polarity, a positive pulse is generated on the input 106 of the flip-flop 53, thus moving the tongues 67 and 86 to the marking position and sending a positive pulse over the line 42.

As the brush 56 turns from the segment *b* to the segment *b'* a positive pulse is similarly sent to the connections 107 and 108 of the adding circuit 52. The coincidence of the two positive pulses generates a positive pulse on the input 94 of the flip-flop 54, thus maintaining the tongue 95 on the marking position and generating a positive pulse.

This latter pulse is also compared with the original clear pulse directly arriving to the comparator 48.

The mode of operation of the apparatus is similar for the following third, fourth and fifth pulse of the code combination considered.

As the brush 56 passes from the segment *e'* to the segment S a positive pulse is directly sent to the input 106 of the flip-flop 53, thus moving the tongues 67 and 86 to the marking position and generating a positive stop pulse on the line 42.

The brush 56 will then be stopped on the segment S', where it generates a positive pulse directly conveyed to the input 94 of the flip-flop 54 and causing the tongue 95 to be moved to the marking position.

It will be apparent that the two sets of segments of the distributor 55 are adapted to alternately operate the first and second mixing circuits, whereby a clear code combination is enciphered and deciphered pulsewise, each pulse of said code combination being first enciphered and then deciphered by the two mixing circuits.

From the foregoing description it will be understood that many changes may be made in the above construction, and different embodiments of the inventions could be made without departing from the scope thereof. It is, therefore, intended that all matter contained in the above description, or shown in the accompanying drawing, shall be interpreted as illustrative, and not in a limiting sense.

What I claim is:

1. In a transmitting station of a secret telegraph system, a clear message transmitter for generating electric pulses according to clear code combinations, a key message transmitter for generating electric pulses according to key code combinations, and an enciphering apparatus responsive to the output of the said transmitters, said clear message transmitter being operable irrespective of the simultaneous operation of said apparatus, said apparatus comprising a first electric circuit concurrently fed by said transmitters for pulsewise mixing a clear code combination with a key code combination to generate a resulting enciphered code combination, a second electric circuit concurrently fed by said first electric circuit and said key message transmitter for pulsewise mixing said enciphered code combination with said key code combination to generate a resulting deciphered code combination, first means connected to said second electric circuit for transmitting said resulting deciphered code combination, second means connected to said clear message transmitter for transmitting said clear code combination, and a comparator connected to said first and second means for pulsewise comparing said deciphered code combination with said clear code combination to control operation of said apparatus.

2. In a transmitting station of a secret telegraph system including a telegraph line, a clear message transmitter for generating electric pulses according to clear code combinations, a key message transmitter for generating electric pulses according to key code combinations, and an enciphering and deciphering apparatus responsive to the output of the said transmitters, said clear message transmitter being operable irrespective of the simultaneous operation of said apparatus, said apparatus comprising a first electric circuit concurrently fed by said transmitters for pulsewise mixing a clear code combination

with a key code combination to generate a resulting enciphered code combination, a first telegraph relay energizable by said first electric circuit for transmitting said resulting pulse over said line, a second electric circuit concurrently fed by said first relay and said key message transmitter for pulsewise mixing said resulting enciphered code combination with said key code combination to generate a resulting deciphered code combination, a second telegraph relay energizable by said second electric circuit for transmitting said resulting deciphered code combination, means connected to said clear message transmitter for transmitting said clear code combination, and a comparator connected to said second telegraph relay and said last-named means for pulsewise comparing said deciphered code combination with said clear code combination to control operation of said apparatus.

3. In a transmitting station of a secret telegraph system, a clear message transmitter for generating electric pulses according to clear code combinations, a key message transmitter for generating electric pulses according to key code combinations, and an enciphering and deciphering apparatus responsive to the output of the said



transmitters, said clear message transmitter being operable irrespective of the simultaneous operation of said apparatus, said apparatus comprising a first electric circuit concurrently fed by said transmitters for pulsewise mixing a clear code combination with a key code combination to generate a resulting enciphered code combination, a second electric circuit concurrently fed by said first electric circuit and said key message transmitter for pulsewise mixing said resulting enciphered code combination with said key code combination to generate a resulting deciphered code combination, and timing means operating in synchronism with said transmitters for alternately operating said first and second mixing circuits to first mix a pair of pulses in said first mixing circuit and then mix a corresponding pair of pulses in said second mixing circuit.

**References Cited** in the file of this patent

UNITED STATES PATENTS

| | | |
|---|---|---|
| 1,310,719 | Vernam | July 22, 1919 |
| 2,458,734 | Reiber | Jan. 11, 1949 |
| 2,537,420 | Potts | Jan. 9, 1951 |