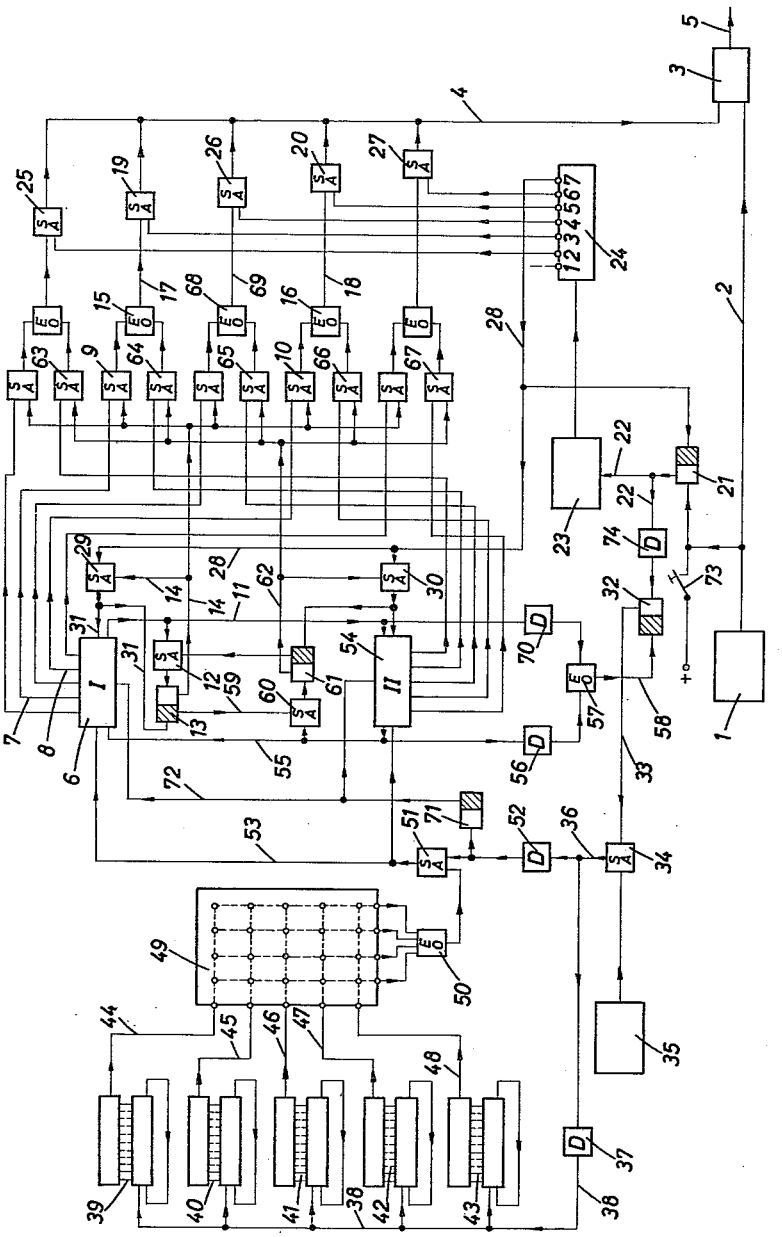
Aug. 28, 1962 R. HELL ET AL 3,051,783

APPARATUS FOR ENCIPHERING-DECIPHERING TELEPRINTER COMMUNICATIONS

Filed June 17, 1959



United States Patent Office 3,051,783 Patented Aug. 28, 1962

3,051,783

APPARATUS FOR ENCIPHERING-DECIPHERING TELEPRINTER COMMUNICATIONS

Rudolf Hell, Kiel, and Roman Koll, Kiel-Wellingdorf, Germany, assignors to Dr.-Ing. Rudolf Hell Kommanditgesellschaft, Kiel, Germany, a company of Germany

Filed June 17, 1959, Ser. No. 821,342
Claims priority, application Germany June 21, 1958
2 Claims. (Cl. 178—22)

This invention is concerned with apparatus for enciphering-deciphering teleprinter communications and may be considered in the nature of an improvement on the disclosures contained in copending applications Serial Nos. 543,549, filed October 28, 1955; and 798,293, filed March 9, 1959.

The first noted copending application Serial No. 543,549 relates to a method of and apparatus for producing extended perforated coding tapes of a very long period with the use of relatively short aperiodic punched coding tapes and using the principle of cross-scanning or reading. The apparatus for performing the method operates electromechanically or magnetomechanically, that is, uses mechanically moved parts and particularly rotating disks for magnetically storing information.

A somewhat modified method has been proposed, for producing extended perforated coding tapes, which provides, as compared with the first noted copending application, a considerable simplification of the apparatus, the aperiodic short punched coding tapes themselves being used for the periodic cross-scanning or reading, instead of their content first being stored magnetically on rotating discs. This apparatus nevertheless still operates electromechanically.

The second noted copending application, Serial No. 798,293 relates to an electronic method and electronic apparatus for producing extended pulse combination sequences punched in a perforated tape, the content of the short aperiodic perforated coding tapes being electronically stored and the transverse scanning or reading being effected electronically without mechanical means.

The advantages of the purely electronic production of the key pulses of the code extender are that mechanically moved parts are completely avoided and the average speed of production of the key pulses, which occur irregularly of course, can be increased considerably. This is of importance in the enciphering and deciphering of information to be transmitted by teleprinter when instead of extended perforated code tapes extended sequences of pulse combinations are to be produced which are to be used for enciphering or deciphering directly, that is to say without first punching them in a paper tape for the purpose of long-duration storage, practically simultaneously with their production.

There is, therefore, pre-supposed a code pulse generator according to the copending applications, in which the key pulses are produced at irregular intervals of time but with an average speed such that a complete key pulse combination is with certainty always available before the transmission of a teleprinter symbol to be enciphered. However, owing to the non-constant speed of production of the key pulses, a short-duration storage of the key pulses cannot be avoided.

The present invention provides for an application of the methods and apparatus of the copending applications in the enciphering and deciphering of information to be transmitted by teleprinter.

According to the invention, the enciphering method comprises storing in one or two storers the pulses of a key symbol delivered by a key pulse generator, thereupon releasing these pulses from the filled storer by the starting pulse of the teleprinter symbol in time with the pulses of

the teleprinter symbol, mixing the teleprinter symbol pulses in generally known manner with the associated key symbol pulses, placing the key pulse generator into operation by the starting pulse of the teleprinter symbol, filling the empty storer with the pulses of a key symbol during the transmission or reception of the teleprinter symbol, and finally again disconnecting the key pulse generator by the storage of the last pulse of this key symbol.

The apparatus for performing the method according to the invention comprises a teleprinter machine, a mixer connected ahead of or respectively in back of the teleprinter machine, for enciphering and deciphering purposes respectively, two storers each for the alternate storage of the pulses of a key symbol, a control device consisting essentially of switches and gates connected to the storer inputs and outputs, a timing generator which is put into operation by the starting pulse of a teleprinter symbol and the operation of which is discontinued again by the stop pulse, a counter for the periodic counting of the timing pulses, by means of which counter the release of the stored pulses of a key symbol is synchronized with the transmission or reception of the associated pulses of a teleprinter symbol, a key pulse generator which in each case fills one of the two storers with the pulses of a key symbol, and control means which cause the code pulse generator to be put into operation by the starting pulse of the teleprinter symbol, the empty storer to be filled with the pulses of a new key symbol during the transmission or reception of the teleprinter symbol, and the operation of the code pulse generator to be discontinued again by the storage of the last pulse of this key symbol.

An embodiment of the invention is by way of example illustrated in block diagram circuit form in the accompanying drawing.

The equipment comprises five main parts, namely, a teleprinter machine, a key pulse generator, a mixer, two storers and a control device for the filling and emptying of the storers and for placing the key pulse generator in operation and discontinuing the operation thereof, respectively.

From the teleprinter machine 1 the communication symbols to be transmitted pass as pulse combinations in the binary five-element code through the line 2 to the mixer 3, in which they are mixed with the key pulses supplied from the line 4 and are passed to the transmission line 5. However, in the case of start-stop operation, a pulse series of the five-element code consists of seven individual pulses, of which the first is the start pulse, the second to sixth contain the information in the five-element code, and the seventh is the stop pulse. Since the teleprinter timing has been internationally fixed at 50 pulses per second (50 baud), 50:7=7.15 teleprinter symbols per second can be transmitted.

The mixing of the teleprinter pulses with the key pulses is effected according to a commutative multiplication pattern, for example according to the algebraic sign rules of multiplication: $+\cdot+=+$, $+\cdot-=-$, $-\cdot+=-$, $-\cdot-=+$. Sign + here means a positive pulse or the presence of a pulse and the sign — a negative pulse or the absence of a pulse. The expression "commutative multiplication" or "commutative mixing" means that when K is the sign of the plain-text pulse, S the sign of the key pulse and G the sign of the enciphered pulse, $K\cdot S=S\cdot K=G$. To obtain the plain-text pulse K from the enciphered pulse G, the sign of G would have to be divided by the sign of S. Since, however, the division of the signs is governed by the same rules as their multiplication, the plain-text is likewise clearly obtained by commutative multiplication of the sign of the encoded pulse by that of the key pulse: $K=G\cdot S=S\cdot G$. The deciphering key is thus equal to the enciphering key,

which has the advantage that the same device can be used for enciphering and deciphering.

Transmission of the Enciphered Symbols

Let is be assumed that a preceding functional process to be discussed later has resulted in the storage in a first storer **6** (I) of the pulses of a key symbol, for example − + − + −, and in consequence positive voltage appears at the lines **7** and **8**. The And gates **9** and **10** are thus prepared for switching through. After the filling of the storer **6** there is also voltage at line **11**. The switch **13** is thus changed over by way of the SA And gate **12** and voltage is applied to the line **14**. This voltage creates the second switching-through condition for the SA And gates **9** and **10** and therefore passes through the Or gates **15** and **16** to the lines **17** and **18**, so that the SA And gates **19** and **20** are also prepared for switching through.

The starting pulse of a pulse combination to be transmitted by the teleprinter **1** is differentiated. From the leading flank of the starting pulse a pulse is thus obtained which brings the switch **21** into the "On" position. Voltage thus passes to the line **22**, so that the multivibrator **23** is put into operation, which operates at a time speed of 5 pulses per second. The pulses are fed to the counter **24** which advances by one counting step responsive to each multivibrator pulse. The first counting step is not utilized. During the counting steps 2–6 there appear at the corresponding outputs of the counter in succession voltages or changes of potential which are fed to the SA And switches **25**, **19**, **26**, **20**, **27**. According to the example assumed, the gates **19** and **20** are prepared for switching through, so that the third and fifth counting step, that is to say the second and fourth code step, connects voltage to the line **4**. The sequence of the individual pulses of the information combination in time corresponds with the sequence of the multivibrator cycles in time so that associated pulses of the key symbol and of the information symbol are adapted to one another per unit of time and are mixed in the mixer **3**. The symbol leaving the mixer is correspondingly enciphered.

Upon further operation the multivibrator **23** switches on the seventh stage of the counter **24**. The output of this stage is connected by way of line **28** to the SA And gates **29** and **30** and to the switch **21**. The latter is switched back into its initial position, renders the line **22** devoid of voltage and switches off the multivibrator **23**. By way of the gate **29** and the line **31** the storer **6** is erased and the voltage at the lines **17** and **18** accordingly disappears. The erasing pulse by way of line **31** also switches the switch **13** back into the normal position and cancels out the pass condition for the SA And gates **9** and **10** associated with the storer **6**.

Production of a Key Symbol

At the instant of the beginning of the transmission of the information symbol and of the changeover of the switch **21**, the switch **32** is also switched over by way of the line **22** and the differentiating member **74**. Voltage thus passes to the line **33**, and the SA And gate **34** is opened. Pulses produced by the square wave generator **35** pass through the gate **34** to the line **36** and are fed by way of the differentiating member **37** to the common line **38** disposed at the input of the electronic counters **39–43**. These counters consist of self-containing ring counters which are advanced by one step by each pulse and after each full cycle begin again with the first step without interruption. As described in detail in the previously mentioned copending application Serial No. 798,293, the step numbers of the individual counters are so chosen that no two of them have a common divisor. By means of the programs associated with the counters each counting step of each counter is allotted a determined positive or negative validity so that the outputs **44–48** of the counters **39–43** have varying potentials according to these programs. The electronic scanning of the programs in this way leads to varying five-element pulse combinations at the lines **44–48**. These pulse combinations are compared in the electronic cross-scanner or transverse scanner **49** with a plurality of determined pulse combinations previously agreed upon between the communicating teleprinter parties. If the scanned combination agrees with any of the determined combinations (a hit) a pulse is obtained which is fed through the EO Or gate **50** to the SA And gate **51** and the latter is prepared for the passage for the duration of the current generator period. In the middle of the generator period, reversal of the polarity of every other square phase of the generator **35** by way of the differentiating member **52** produces a pulse which passes through the gate **51** and is taken through the line **53** to the storers **6** (I) and **54** (II). These two storers are connected to form a ring by way of the lines **11** and **55** and form a ten-stage electronic shift register. The mode of operation of this register is described in detail in the previously second mentioned application with reference to FIG. 2 thereof. Pulses at the common control line **53** common to the two storers successively switch the five switch stages of the first storer **6** (I), and then those of the second storer **54** (II), and then again those of the storer **6** (I), and so forth. At the moment of the present consideration, the storer **6** (I) is still in operation since the extraction of the pulses of the key symbol stored in it is of course just starting. The first pulse occurring at the line **53** will thus occupy the first position of the storer **54** (II). Further pulses originating from the cross-scanner **49** occupy the second to fifth positions. With the occupation of the fifth position voltage passes to the line **55**. By differentiation in the differentiating member **56** a pulse passes through the EO Or gate **57** and through the line **58** to the switch **32** and switches the latter back into its normal position. The gate **34** is thus closed and the further supply of pulses from the generator **35** to the counters **39–43** is interrupted.

The generator **35** must have a very high frequency in relation to the transmission frequency of the teleprinter symbol pulses in order that in the time of 140 ms. required for the transmission of an information symbol there may be dependably formed a new key pulse combination, the pulses of which are of course produced very irregularly as to time. With a cross-scanning number of four, for example, on the average each eighth period of the generator would lead to a cross-scanning hit, that is to say 625 hits per second or 87.5 hits in 140 ms. Five hits, however, fill a storer and form a new code symbol. With an assumed generator frequency of 5,000 c.p.s. the production of a key pulse would on the average require a time of 8 ms.

At the moment when the storer **54** is filled and the line **55** receives the voltage, the storer **6** is therefore generally not yet erased. The switch **13** is therefore still situated in the working position, the line **59** is devoid of voltage, and the SA And gate **60** is blocked. It remains blocked until the storer **6**, as already described, is erased and the switch **13** is switched back after completion of the transmission of the teleprinter symbol by the seventh step of the counter **24**. Voltage thus passes to the line **59** and the SA And gate **60** permits the passage of voltage to the line **55**. The switch **61** switches over and in turn applies voltage through the line **62** to the SA And gates **63–67**, which are associated with the storer **54** and are thus prepared for switching-through. The second pass condition of these gates is established by the positive pulses of the key pulse combination stored in the storer **54**. Let it be assumed that the code symbol − − + + − is stored in the storer **54**. The SA And gates **65** and **66** then open, so that voltage passes to the lines **69** and **18** through the EO Or gates **68** and **16**. The SA And gates **26** and **20** are thus also prepared for switching through. This condition remains until the key

symbol stored in 54 has been read out and the storer 54 erased after a new symbol transmission. The voltage at the line 62 has in fact also prepared the SA And switch 30. After the key symbol in the storer 54 has been read out and used, the switch 30 is opened by the seventh counting position of the counter 24 and thus erases the storer 54.

With the starting pulse of the second information symbol to be transmitted, which has used up the key symbol stored in the storer 54, the changeover of the switch 32 initiated a new filling of the storer 6 and hence preparation of the third key symbol. The filling of the storer 6 also proceeds much more rapidly than the consumption of the key symbol stored in the storer 54. Thus upon completion of the new filling of the storer 6 voltage appeared on the line 11 and by way of the differentiating member 70 and the EO Or switch 57 and the lines 58 switched back the switch 32 and thus stopped the key pulse generation by the blocking of the switch 32. With the filling of the storer 6 and the preparation of the key symbol in this storer the starting point of the present consideration of a cycle has been reached again. The process, which has been described in two sections, is repeated upon the enciphering of each further symbol transmitted by the teleprinter.

Upon the filling up of the storers and the preparation of the key symbols a positive or negative polarity is allocated to the individual positions of the five-element combinations of the key symbols, as already described previously. This allocation is effected by means of the switch 71. The pulses passing through the differentiating member 52 switch over the switch 71 into a position varying with each following pulse and a voltage varying periodically between + and — appears on line 72. In accordance with this allocation, even numbered pulses are positive and odd numbered pulses negative at the line 36. Since, however, the cross-scanning hits occur at irregular intervals of time and prefer neither even nor odd numbered pulses, positive and negative key pulses, regarded over a relatively long transmission period, are statistically uniformly distributed.

It had been assumed that at the beginning of the message transmission a key pulse combination was already stored in the storer 6 (I). In order that this may in actual fact always be the case, the first filling of the storer 6 must be initiated automatically when the apparatus is switched on, that is to say before the beginning of the teleprinter transmission. This is effected by the contact 73, which is coupled to the On-Off switch of the apparatus. By means of this contact a short pulse is passed to the switch 21, which effects the initiation of a storage sequence and hence the preparation of the first key pulse combination.

The arrangement illustrated in the single figure of drawing is concerned primarily with the transmitting station. Identical apparatus is provided at the receiving station but the connection of the apparatus to the transmission line 5 and to the teleprinter 1 is effected in the reverse sequence. At the receiver station, line 2 is the transmission line from which the incoming pulses are taken to the switch 21 and to the mixer 3. The line 5 leads from the mixer 3 to the teleprinter 1, which prints in plain-text the enciphered teleprint symbols arriving over the transmission line 2 and deciphered by the mixer 3.

It is understood, of course, that the codes effective at the transmitting and receiving stations for the two enciphering and deciphering devices must be agreed upon beforehand between the communicating parties and must agree.

Changes may be made within the scope and spirit of the appended claims which define what is believed to be new and desired to have protected by Letters Patent.

We claim:

1. In the transmission of messages by teleprinter machines, a device for respectively enciphering and deciphering said messages by mixing the pulses of the teleprinter symbols with key pulses, comprising a key pulse generator, means for alternately separately storing key pulse combinations formed from individual key pulses, from said generator, means operatively connected to said storage means for releasing the pulses of a stored key pulse combination responsive to the start pulse of the teleprinter symbol, means operatively connected to said storage means and said teleprinter machine operative to mix the pulses of the teleprinter symbols with the pulses of the released key pulse combination, means operatively connected to said generator for starting the production of key pulses responsive to said start pulse, to effect storage during the transmission and reception of the teleprinter symbol, of a key pulse combination in place of the released combination, and means operatively connected to said generator for stopping the production of key pulses responsive to the storing of the last pulse of such key pulse combination.

2. In the transmission of messages by teleprinter machines wherein messages are respectively enciphered and deciphered by mixing impulses of the teleprinter symbols with key pulses, apparatus for respectively transmitting and receiving messages and for respectively effecting enciphering and deciphering thereof, comprising a teleprinter machine for respectively transmitting and receiving messages, a mixing device operatively connected to said teleprinter machine for enciphering teleprinter symbols therefrom and for deciphering teleprinter symbols to be fed thereto, two stores for alternately separately storing the impulses of code impulse combinations formed from key pulses, a timing device for producing timing pulses respectively operatively connected under the control of a start impulse of a teleprinter symbol and disconnected under control of the stop impulse, a counter connected with said timing device for periodically counting the timing impulses produced thereby operative to effect the release to said mixing device of stored impulses of a key pulse combination for mixing in synchronization respectively with the transmission and reception of the impulses of a teleprinter symbol, a key pulse generator for supplying impulses of a key pulse combination to the respective storers, a switch connected with the teleprinter machines for operatively connecting said key pulse generator under control of the start impulse of the teleprinter symbol, an And-gate connected with said switch and with said key pulse generator, means for connecting the output of said And-gate with the storer inputs, said And-gate being during the respective transmission and reception of the teleprinter symbol effective to fill a storer from which impulses had been released with impulses of another key pulse combination, and an Or-gate connected with the respective inputs and outputs of said storers, the output of said Or-gate being connected with said switch operative to stop the operation of said key pulse generator responsive to the storing of the last impulse of said other key pulse combination.

References Cited in the file of this patent

UNITED STATES PATENTS

2,785,224	Ehrat	Mar. 12, 1957
2,874,215	Zenner	Feb. 17, 1959
2,899,498	Thompson	Aug. 11, 1959