

[54] **APPARATUS FOR AUTOMATICALLY
ENCIPHERING AND/OR DECIPHERING
A TEST CONSISTING OF MULTIDIGIT
DUAL CODED CHARACTERS**

[72] Inventor: Sture Nyberg, Zug, Switzerland
[73] Assignee: Anstalt Europäische Handel-
sgesellschaft, Vaduz, Liechtenstein
[22] Filed: Nov. 19, 1970
[21] Appl. No.: 90,981

Related U.S. Application Data

[63] Continuation-in-part of Ser. No. 748,350, July
29, 1968, abandoned.
[52] U.S. Cl. 35/4
[51] Int. Cl. G09c 1/10
[58] Field of Search 35/2, 3, 4; 340/345

[56] **References Cited**

UNITED STATES PATENTS

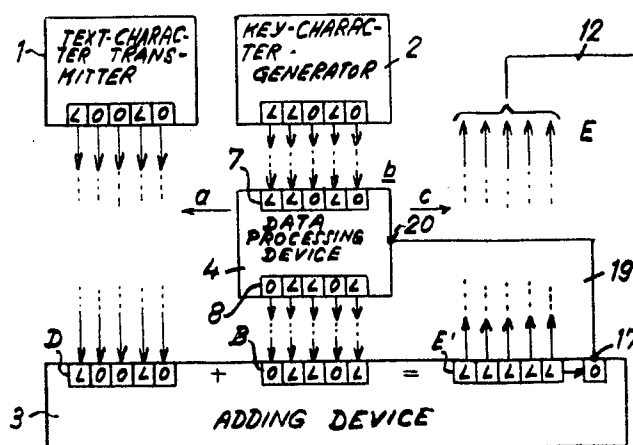
2,750,586 6/1956 Daniels 35/4 X
3,309,694 3/1967 Fierston et al. 35/4 X

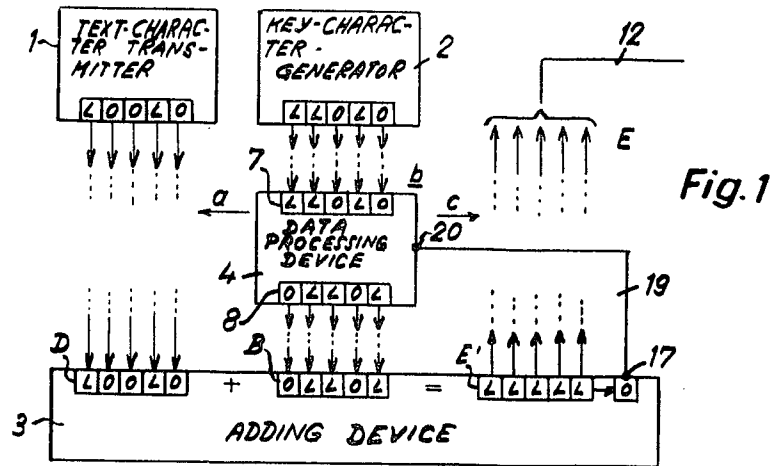
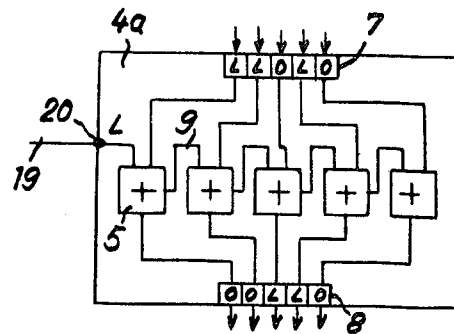
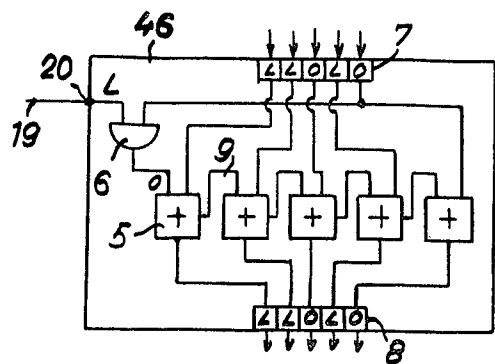
Primary Examiner—Wm. H. Grieb
Attorney—Richard P. Alberti

[57] **ABSTRACT**

An apparatus for automatic enciphering and/or deciphering a text consisting of multidigit dual coded key characters supplied by a key character generator, comprising an adding device for dual addition of text characters and key characters. The adding device includes first inputs for introducing text characters, second inputs connected to the key character generator for introducing key characters, outputs for result characters obtained at each adding operation, and a transfer or carry output for transmission of a transfer signal when upon addition of the characters a transfer is obtained at the last digit. There is also provided a data processing device for digital signal sequences which is connected to the transfer or carry output, said data processing device being connected to said adding device ahead of said first or said second inputs, or following said outputs thereof, in order to modify the characters introduced into the data processing device in a definite manner, in accordance with a transfer or carry signal.

4 Claims, 6 Drawing Figures





INVENTOR.
STURE NYBERG
BY
Richard P. Allen

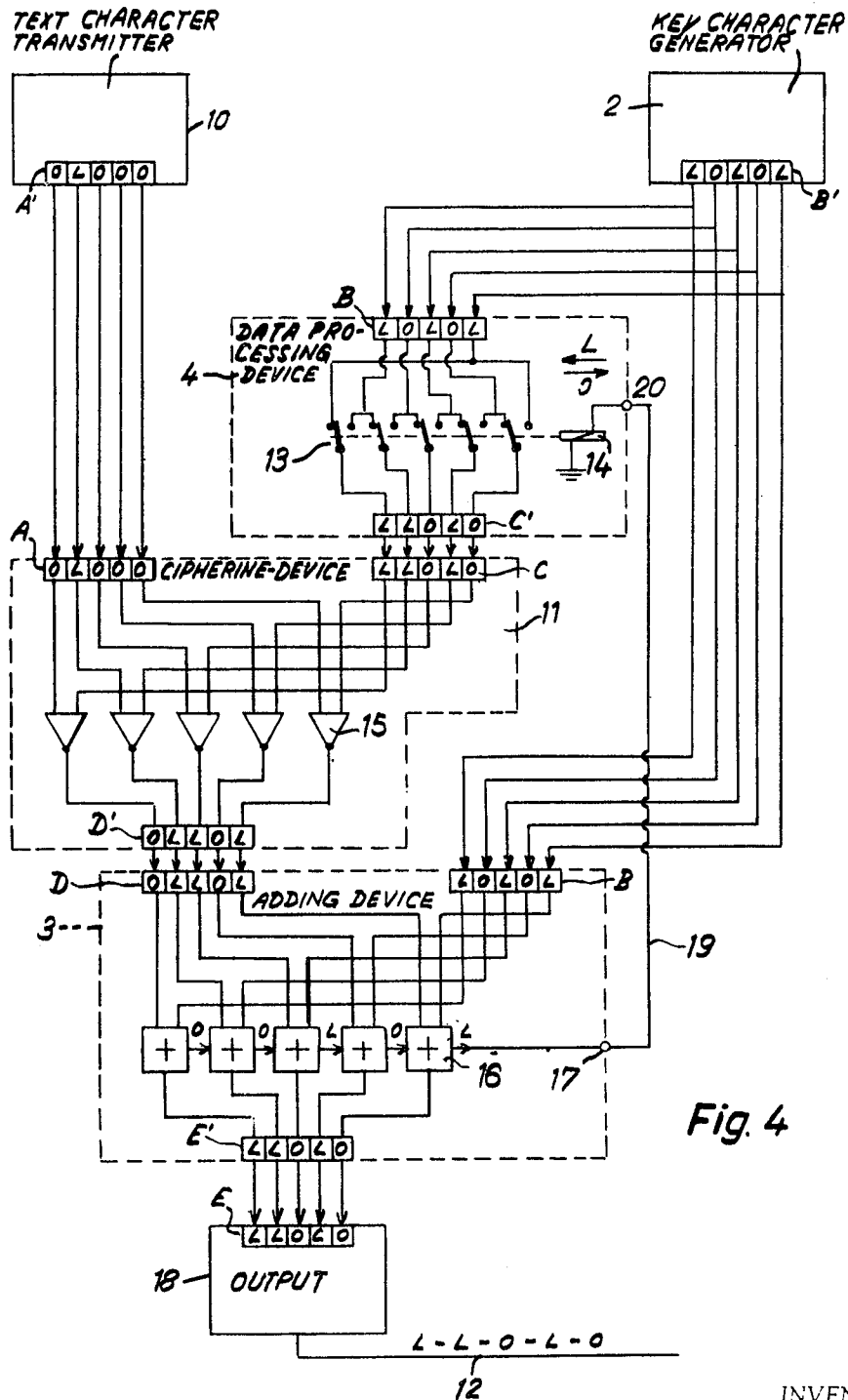


Fig. 4

INVENTOR
STURE NYBERG
BY
Richard P. Allen

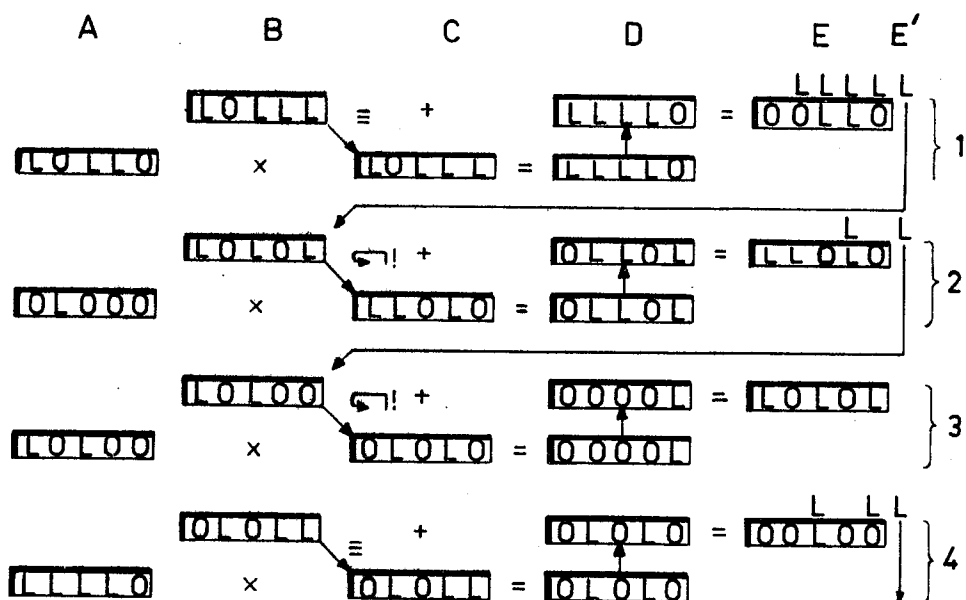


Fig. 5

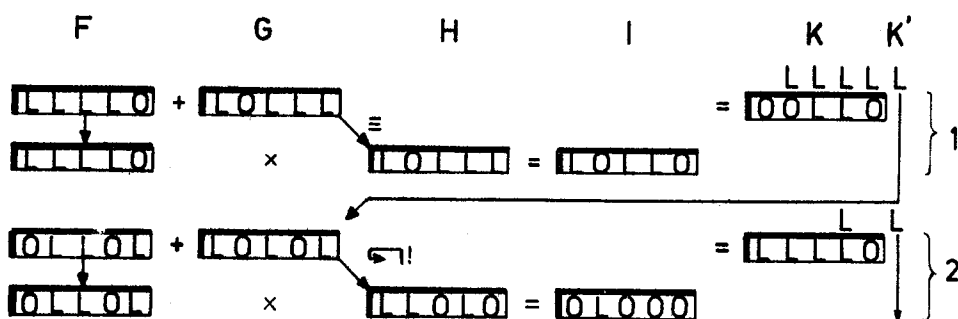


Fig. 6

INVENTOR.
STURE NYBERG
BY
Richard P. Allen

APPARATUS FOR AUTOMATICALLY ENCIPHERING AND/OR DECIPHERING A TEXT CONSISTING OF MULTIDIGIT DUAL CODED CHARACTERS

The instant application is a continuation-in-part application of my commonly assigned, copending U.S. application, Ser. No. 748,350, filed July 29, 1968 now abandoned, and entitled "METHOD AND APPARATUS FOR CIPHERING AND DECIPHERING A SECRET TEXT".

BACKGROUND OF THE INVENTION

The present invention relates to improved apparatus for the automatic enciphering and/or deciphering of a text consisting of multidigit dual coded characters by means of multidigit dual coded key characters which are supplied by a key character generator.

Automatically operating enciphering and deciphering apparatus generally use digital signal sequences in which a number of dual signal values, generally five, are allocated to the plain or secret text characters, as well as to the respective key characters. Enciphering is generally effected in one of the following two manners: Either logical operations in an Exclusive OR combination are effected with dual informations corresponding to each other as to the number of digits (prefix multiplication), or the dual values modulo -2^n are added together, n representing the number of dual values of the characters (usually, as mentioned, $n = 5$, thus $2^n = 32$).

An example for the first mentioned manner of enciphering: (Exclusive OR logical operation, prefix multiplication) Notation:

O is represented by -1

L is represented by $+1$

Logical operation table:

$+1 \times +1 = +1$	$L \times L = L$
$+1 \times -1 = -1$	$L \times O = O$
$-1 \times +1 = -1$	$O \times L = O$
$-1 \times -1 = +1$	$O \times O = L$

It will be seen that in the left hand table only the prefixes need to be multiplied.

For example, for the enciphering there results therefrom:

Text characters	O L O L L
Key characters	L O O L O
Result	O O L L O

An example for the second mentioned manner of enciphering, binary addition which is here effected from left to right:

Text characters	O L O L L
Key characters	L O O L O
Result	L L O O O (L)

As a rule, the transfer or carry (in brackets) to a further, next higher position drops out for want of a corresponding channel.

The key information is continuously derived from a key character generator, the latter being an independently operating generator or, for example, a punched tape reader or the like. It is obvious that for automatic deciphering, an analogous synchronization of the key

character generator used is necessary. The key character generator produces a chain of key characters which is exclusively subjected to the laws of the used key character generator. At least two such generators accordingly must operate in exactly the same manner. In a telecommunication network a larger number of generators will be used, such a generator being associated with each station, since all stations shall communicate with one another. However, in practical operation, it is impossible to prevent a sequence of characters supplied to a station by its associated key character generator from being used once also by another station. There will result so-called "texts of like keys", which can be decrypted by a linguistic comparison method.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide apparatus for automatic enciphering and/or deciphering of a text consisting of multidigit dual coded characters by means of a key character generator, in which apparatus the occurrence of texts of like keys are prevented.

According to the invention this apparatus for automatically enciphering and/or deciphering with the aid of a key character generator, comprises an adding device for dual addition of text characters and key characters, said adding device including first inputs for introducing text characters, second inputs connected to said key character generator for introducing key characters, outputs for result characters obtained during each adding operation, and a transfer (carry) output for transmitting a transfer signal when, upon the addition of the characters a transfer is obtained at the last digit, and a data processing device for digital signal sequences connected to said transfer output, said data processing device being connected to said adding device ahead of said first or said second inputs or following said outputs thereof, in order to modify in a definite manner, according to a transfer signal, the characters introduced into said data processing device.

With a text of considerable length, on an average about 50 percent of the different additions will result in a transfer, so that for an enciphering operation about one-half of the characters (plain text characters or key characters or secret text characters) will be modified and the other half of the characters is taken over without modification.

In this manner it is obtained that in every text undergoing enciphering or deciphering (plain text or secret text) the key characters furnished by the key character generator are automatically and individually modified. Each communication thus obtains its own individual key.

It will be appreciated that in the case of a key character modification, the keys of two communications will differ also then when the key character chains furnished primarily by the key character generators (at the input B) first show identical characteristics. For linguistic deciphering of two communications, however, it would be obligatory that in both cases the key characters added thereto completely agree with each other.

In this manner, it is obtained that such communications have no longer the same code and therefore may not be deciphered even though originally during enciphering the same key characters had been used.

The data processing device can be so designed that in response to an input signal it transfers the momentarily introduced characters to the outlet after cyclic permutation thereof by one digit. Data processing devices of such type are known and are assembled, for example, from logical circuit elements.

The data processing device may also be designed in such manner that the transfer or carry over signal modulo 2^n is added to at least one of the momentarily introduced characters. Such a circuit which is also known per se is of particularly simple construction. In this case a still more effective enciphering can be obtained by providing suitable circuits arranged to have the data processing device effecting the said addition only when a determined logical signal, preferably an "L" signal, appears at the last digit of the inputs of the data processing device.

BRIEF DESCRIPTION OF THE DRAWING

The invention will be better understood and objects other than those set forth above, will become apparent when consideration is given to the following detailed description thereof. Such description makes reference to the annexed drawing wherein:

FIG. 1 schematically illustrates the principal construction of inventive apparatus for automatically enciphering and/or deciphering;

FIG. 2 schematically illustrates an embodiment of an adding data processing device of the apparatus of FIG. 1;

FIG. 3 schematically illustrates a data processing device which only then carries out an adding operation with "L", when at the last digit of its inputs there likewise appears an "L"-signal;

FIG. 4 schematically illustrates a preferred embodiment of the inventive apparatus with a key character device and a further embodiment of data processing device;

FIG. 5 diagrammatically illustrates the various operations performed during enciphering with the apparatus depicted in FIG. 4; and

FIG. 6 illustrates the various operations performed when the apparatus of FIG. 4 is used for deciphering.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Describing now the drawings, the apparatus depicted in FIG. 1 will be seen to embody an adding device 3 possessing inputs B for the feed of key characters, inputs D for the input of prepared text characters, outputs E' for the result characters obtained after each character addition, and a transfer (carry) output 17 at which there appears an output signal representing a logical "L" or a logical "O", depending upon whether, during addition of the introduced characters, there does or does not occur a transfer.

Additionally, the apparatus embodies a text character-transmitter device 1 which, in this principle circuit diagram, delivers prepared, i.e. text characters which have been processed in a ciphering device and delivered, for instance, in five unit binary code as is usual in teleprinting. Furthermore, there is provided a key character generator 2 which, in this embodiment, prepares a key character chain likewise in five unit binary code, and a data processing device 4 having a control input 20 coupled by a conductor or line 19 with the

transfer or carry output 17 of the adding device 3. The outputs E' of the adding device 3 should be connected via a non-illustrated outlet or output mechanism, for instance, with a teleprinter network or line 12. The data processing device 4 is, as will be described much more clearly hereinafter, constructed in such manner that in the presence of an "O"-signal at its control input 20 the characters appearing at its inputs 7 are delivered without change to its outputs 8 and the introduced characters after having been processed in accordance with a basic principle are delivered to the outputs 8 as soon as an "L"-signal has been delivered to the control input 20. The data processing device 4 is either connected ahead of the key character inputs B of the adding device 3, as such has been indicated in FIG. 1 and designated by the position reference character *b*, or such data processing device 4 can be connected ahead of the text character inputs D of the adding device 3, which has been shown in FIG. 1 by an arrow indicated by the position reference character *a*. Furthermore, the data processing device 4 can be, however, also connected after the result character-outputs E' of the adding device 3, as such has been schematically represented in FIG. 1 by the arrow *c*.

When, for example, the data processing device 4 is connected ahead of the inputs B for the key characters, that is, between the key character generator 2 and the adding device 3, and when the addition in the adding device 3 results in a carry or transfer signal L at the transfer output 17, then the next following key character introduced by the key character generator 2 to the data processing device 4 is modified owing to the transfer signal and introduced as a modified key character into the adding device 3.

When the data processing device 4 is connected ahead of the inputs D for the next characters, then any text character introduced into the data processing device 4, after occurrence of a transfer signal at the transfer output of the adding device 3, is transferred in modified condition to the adding device 3 and there added to the corresponding key character.

When the data processing device 4 is connected to the outputs E' of the adding device 3, it will deliver a result character, for instance a secret text character, in modified condition for instance to a teleprinter network or line 12, if during the preceding operation the addition of text characters and key characters resulted in a transfer or carry.

In order to more fully understand the embodiment especially shown in FIG. 4, the following remarks shall be made: A dual (binary) addition modulo 32 is provided for the five digit code generally used today in teleprinting, which, however, is not directly used for enciphering. The addition, of course, is not limited to this 5 digit character representation which is mentioned here solely by way of example. An addition carry which may possibly occur during this addition (and which, as mentioned above, would usually be dropped) is interrogated and used for modification of especially the following key character which is allocated to the next following text character, whereby initially the actual enciphering operation, i.e., the logical operation effected with the text character and the key character for the present explanation not being considered.

The expression "text", when effecting an enciphering operation, means a plain sequence of dual coded character groups and during deciphering means a ciphered sequence of dual coded character groups.

Modification of the characters introduced into the data processing device 4 can be performed in random manner. In one simple situation, the data processing device 4 can be an adding device which adds the transfer symbol "L" modulo 2^n to the momentarily introduced characters. FIG. 2 shows an exemplary embodiment of such data processing device 4a. Each of the inputs 7 is coupled by an addition element 5 with the corresponding output 8. The transfer output 9 of the first addition element 5 is connected with the second input of the second addition element, the transfer output of the second addition element with the second input of the third addition element, and so forth. At the second input of the first addition element 5 there is connected the control input 20 and via such the transfer output 17 of the adding device 3. The inputs 7 and outputs 8 of the data processing device 4a can be, for example, buffer stores. If a logical "O"-signal appears at the control output 20, then in accordance with a corresponding timing cycle the characters from the input buffer 7 are delivered unchanged to the output buffer 8, but, on the other hand, if a logical "L"-signal appears at the control input 20, then in accordance with the timing cycle there is added "L" modulo 2^n to the characters in the input buffer 7.

This circuitry of the data processing device 4a can be easily modified such that the addition only then is carried out if, for instance, at the last digit of the input buffer 7 there appears a logical L. Thus, as best illustrated for instance in FIG. 3, to this end it is only necessary to connect an AND-element 6 between the input of the first addition element 5 and the control input 20, the control input 20 being located at the one input of this AND-element 6, and the second input of which is connected with the last stage of the input buffer 7, and its output forms the one input for the first addition element 5. Since during logical AND-operations there is always only then obtained a L-signal when both inputs have applied thereto a respective L-signal, the required addition is carried out by the data processing device 4b if there is received from the adding device 3 as a transfer symbol an L and at the same time from the last digit of the input buffer 7, likewise an L.

The data processing device 4 is preferably constructed in such a manner that upon the appearance of an L-signal at the control input 20 it cyclically permutes through one digit or place the introduced characters. In order to elucidate this operation, the schematically illustrated data processing device 4 of FIG. 4 embodies a switching arrangement 13, 14 by means of which, upon the appearance an O-signal at the control input 20, the individual inputs B are connected in the correct sequence with the individual outputs C'. Upon the presence of an L-signal at the control input 20, the switching device 13, 14 is switched in such manner that the last input is coupled with the first output, the first input with the second output, and so forth. Naturally, it would also be possible to utilize other suitably designed data processing devices.

The apparatus depicted schematically in FIG. 4 embodies ciphering device 11 which carries out an Exclu-

sive-OR logical operation of dual signals and, for instance, contains appropriate logical circuit components 15, by means of which the inputs A for the text characters from a text character generator 10 and the inputs C for the modified key characters which are coupled via the data processing device 4 with a key character generator 2, are connected with the outputs D' of the ciphering device. The outputs D' of the ciphering device 11 are coupled with the text character inputs D of the adding device 3. The key character inputs B of the adding device 3 are connected with the outputs of the key character generator 2. The adding device 3 contains a chain adding element 16, whereby the transfer output of the last addition element 16 of the chain represents the transfer output 17 of the adding device 3 which is connected via a line or conductor 19 with the control input 20 of the data processing device 4.

The outputs E' of the adding device 3 are connected with the inputs E of an output mechanism 18, which simultaneously delivers the occurring characters in sequence to a teleprinter network 12.

Now, in order to explain the mode of operation reference is made to FIG. 5 where there have been illustrated the successive operational steps. The individual operational steps are controlled by a non-illustrated timing device of FIG. 4. During enciphering of a clear or plain text during a first operational cycle I, a text character is introduced into the ciphering device 11 and from the key character generator 2 a key character is introduced into the data processing device 4 and into the adding device 3. During the second operating cycle II the key character introduced into the data processing device 4 — which key character would have been modified upon the appearance of a L-signal from the preceding work cycle at the control input 20, the otherwise is unmodified upon the presence of an O-signal at the control input 20 — appears at its output and is introduced via such output to the key character input C of the ciphering device 11. During the third operational cycle III there occurs the Exclusive-OR-logic operation of the characters introduced into the ciphering device 11 and the delivery of a result character via the output D' of the ciphering device 11 into the result character input D of the adding device 3, the key character input B of which has been furnished with a key character from the first operational cycle. During the operational cycle IV there occurs the addition of both input characters at the adding device 3, the output of the resulting character in the output device 18 and, depending upon whether during the addition there has resulted a transfer L or no transfer O, the adjustment of the data processing device 4 via its control input 20 for the next successive operating cycle. During the operational cycle V the characters from the output device 18 are introduced into the teleprinter line or network 12 and the input buffer and output buffer, insofar as such are present, at the data processing device 4, at the ciphering device 11, and at the adding device 3, are reset.

In FIGS. 5 and 6 the adding device 3 is represented by a "+" symbol. The inputs for introducing the key characters, these inputs being connected with the key character generator, are represented by the frames in column B, the inputs for prepared text characters by

the frames in column D, the outputs for the result characters are represented by the frames in column E, and the transfer or carry output is represented by reference character M. This transfer output is represented in FIG. 5 by an L at the right-hand corner of the frame of the column E.

The ciphering device 11 known per se, and which effects a logical Exclusive Or operation, is symbolized in FIGS. 5 and 6 by the sign "x". Its inputs for introducing text characters are represented by the frames in column A, and its inputs for introducing key characters are represented by the frames in column C. The outputs of the ciphering device are, as mentioned, connected both with an outlet unit as well as also with the input for the prepared text characters of the adding device, this being represented in FIG. 5 by the frames provided with an arrow in column D. The data processing device 4 provided for the apparatus is symbolized in FIG. 5 only by the function symbol ($\square \neg !$). This data processing device 4, upon a control signal, effects a cyclic permutation of the introduced characters by one step. The control input 20 of the data processing device is connected with the transfer or carry over output 17 of the adding device 3, this connection being represented by an arrow leading from the transfer symbol "L" in column M to the mentioned function symbol.

In the represented apparatus the following operations are performed automatically:

A logical operation is effected, according to the principle of prefix multiplication, with the text signal sequence, designated in the following as text letter, and the associated key signal sequence, designated in the following as key letter, this key letter, under certain circumstances as mentioned above, previously undergoing cyclic permutation through one digit.

The rules of the logical operations shall again be recapitulated:

(Exclusive-OR logical operation)

$$L \times O = O, O \times L = O, L \times L = L, O \times O = L$$

For producing a modification signal which shall act on the next following key letter, an addition is performed, the following basic principle again being recalled: $O + O = O, O + L = L, L + O = L, L + L = O$ ($+L$) $O + O + L = L, O + L + L = O$ ($+L$), $L + O + L = O$ ($+L$), $L + L + L = L$ ($\times L$)

FIG. 5 shows a tabular representation of five successive cipher stages. In column A, plain text letters are shown which are represented in five unit binary code style, as is usual in teleprinting. In column B, the key letters are shown as they are fed from the key character generator. Column C contains the modified keys as they were produced by cyclic permutation after a modification signal of the preceding stage was encountered. In column D, the results of the calculation "text $\times$ modified key" are to be seen, and finally, in column E the results for producing the signal which are obtained by the calculation "(original) key plus secret letter".

It will be apparent that in line 1 as the first operation, the secret letter of column D is therefore produced by multiplication of the text letter in column A by the key letter in column C.

This secret letter, as the result, is made available for further transmission or passing on; however, it is also used, as illustrated by an upward arrow, in order to carry out the calculation: key from column B plus this secret letter = signal result in column E

It is evident that a transfer or carry L is produced in line 1 which is here used as signal for modifying the key letter in line 2 of column B.

In line 2, the key letter of column B is therefore cyclically permuted in counterclockwise direction through one step, its new form is illustrated in column C, the multiplication by the text letter from column A gives the result in column D.

The original secret letter in column B in line 2 is now added to the result of column B just produced and gives in column E an auxiliary signal letter wherein a carry L in column M is again produced, by which the data processing operation performed in line 3 is affected.

In line 3, it is evident that a result is obtained in column E which shows no carry; consequently in line 4, the secret letter in column B is transferred unchanged to column C for mixing.

In summary, the following two operations are to be carried out:

1. Actual Ciphering operation:

Text letter times modified key letter = Result.

2. Auxiliary calculation:

Result plus original key letter = Signal.

The signal (transfer signal) M or N is a L-character which modifies the following key letter if there is a carry.

It is, of course, also possible to carry out an addition modulo -2, or modulo -32, instead of the "EXCLUSIVE-OR" logic for the actual combination enciphering operation, whereby the auxiliary operation is not necessary, the result being used at the same time as the signal. In this case, a further modification may also be provided: the carry signal command or order shall be only effective when the key character for producing the signal letter has an L at any digit (e.g., in the last digit).

Deciphering is carried out in similar manner and is illustrated in FIG. 6. In column F, secret text letters are shown, in column G the key letters, in column H the modified keys, in column I the results of the multiplication (plain text produced by deciphering), finally in column K the signal letters, the transfers or carries of which in column N can release the modification of the key, when they are not zero.

In line 1 the secret letter is shown in column F, as may be seen from FIG. 5, column D, line 1. Its addition to the key in column G (originally for enciphering column B) results in column K in the signal letter which again has a carry or transfer L in column N.

The same secret letter in column F, line 1 is, however, also multiplied by the modified key of column H (in the first character again identical to the original key from the key character generator) and produces in column I the deciphered character as the result letter.

In line 2, the same operations are represented, it being evident that the secret letter in column G is changed by the modification order from the preceding line by cyclic permutation, into a new letter which is shown in column H. The multiplication again produces the original plain text letter of line 2.

It is obvious to the person skilled in the art that instead of affecting the key letter, also the text letter could be influenced. It is also possible to influence the corresponding result letters. The whole operation is, therefore, reduced to an influencing of the actual momentary ciphering process.

The illustrated example in which a cyclic permutation of the binary elements of the key letter is caused by the modification, has only been shown as one of the possibilities which may be carried out. In the case of an enciphering operation by addition, it would also be conceivable, for example, to add the binary element which appears as transfer or carry to the next key character in order to effect its modification.

While there is shown and described present preferred embodiments of the invention, it is to be distinctly understood that the invention is not limited thereto but may be otherwise variously embodied and practiced within the scope of the following claims. Accordingly,

What I claim is:

1. Apparatus for automatic enciphering and/or deciphering of a text consisting of multidigit dual coded key characters supplied by a key character generator, comprising an adding device for dual addition of text characters and key characters, said adding device including first inputs for introducing text characters,

second inputs connected to said key character generator for introducing key characters, outputs for result characters obtained at each adding operation, and a transfer output for transmission of a transfer signal when upon addition of the characters a transfer is obtained at the last digit, and a data processing device for digital signal sequences connected to said transfer output, said data processing device being connected to said adding device in a feedback loop from said transfer output of said adding device to one of said first and second inputs thereof, in order to modify the characters introduced into the data processing device, in accordance with said transfer signal.

2. Apparatus according to claim 1, wherein said data processing device comprises means effective in response to a control signal for cyclic permutation of the introduced characters by one digit.

3. Apparatus according to claim 1, wherein said data processing device is an adding device which adds the transfer character modulo 2^n to the introduced characters.

4. Apparatus according to claim 3, wherein said adding data processing device is controlled by one of its inputs, said data processing device only when performing the addition when said one input carries a logical "L" signal.

* * * * *

30

35

40

45

50

55

60

65