United States Patent

[11] 3,557,307

[72] Inventors **Bengt Florin**
Hagersten;
Kalevi Loimaranta, Mattby, Finland

[21] Appl. No. **805,624**
[22] Filed **Mar. 10, 1969**
[45] Patented **Jan. 19, 1971**
[73] Assignee **AB Transvertex**
Varby, Sweden
a Swedish Joint Stock Company

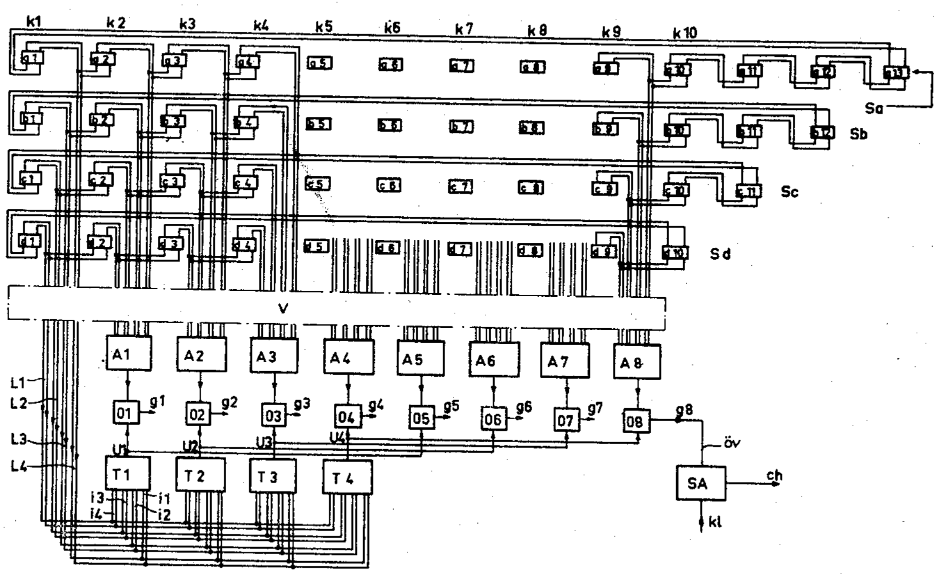
[54] **CIPHERING MACHINE**
4 Claims, 4 Drawing Figs.

[52] **U.S. Cl.** **178/22**
[51] **Int. Cl.** **H04l 9/00**
[50] **Field of Search** 178/22

[56] **References Cited**
UNITED STATES PATENTS
3,038,028 6/1902 Henze 178/22

Primary Examiner—Rodney D. Bennett, Jr.
Assistant Examiner—Malcolm F. Hubler
Attorney—Sommers & Young

ABSTRACT: This invention relates to a ciphering machine for ciphering text in clear produced in binary form by superimposing every text in clear character signal with a variable ciphering signal. Such a machine comprises a number of electric devices stepped in parallel with cyclic operations, for example shift registers, the cycles being mutually different, said devices being formed, for example, by chains or rows of mutually different numbers of bistable flip-flops. The initial states of said flip-flops so were set according to a scheme of preferably random choice that the states of flip-flops stepped in parallel in every column in the different shift registers together define a ciphering character. These column characters, thus, automatically change their nature as soon as a shift register has completed a cycle.



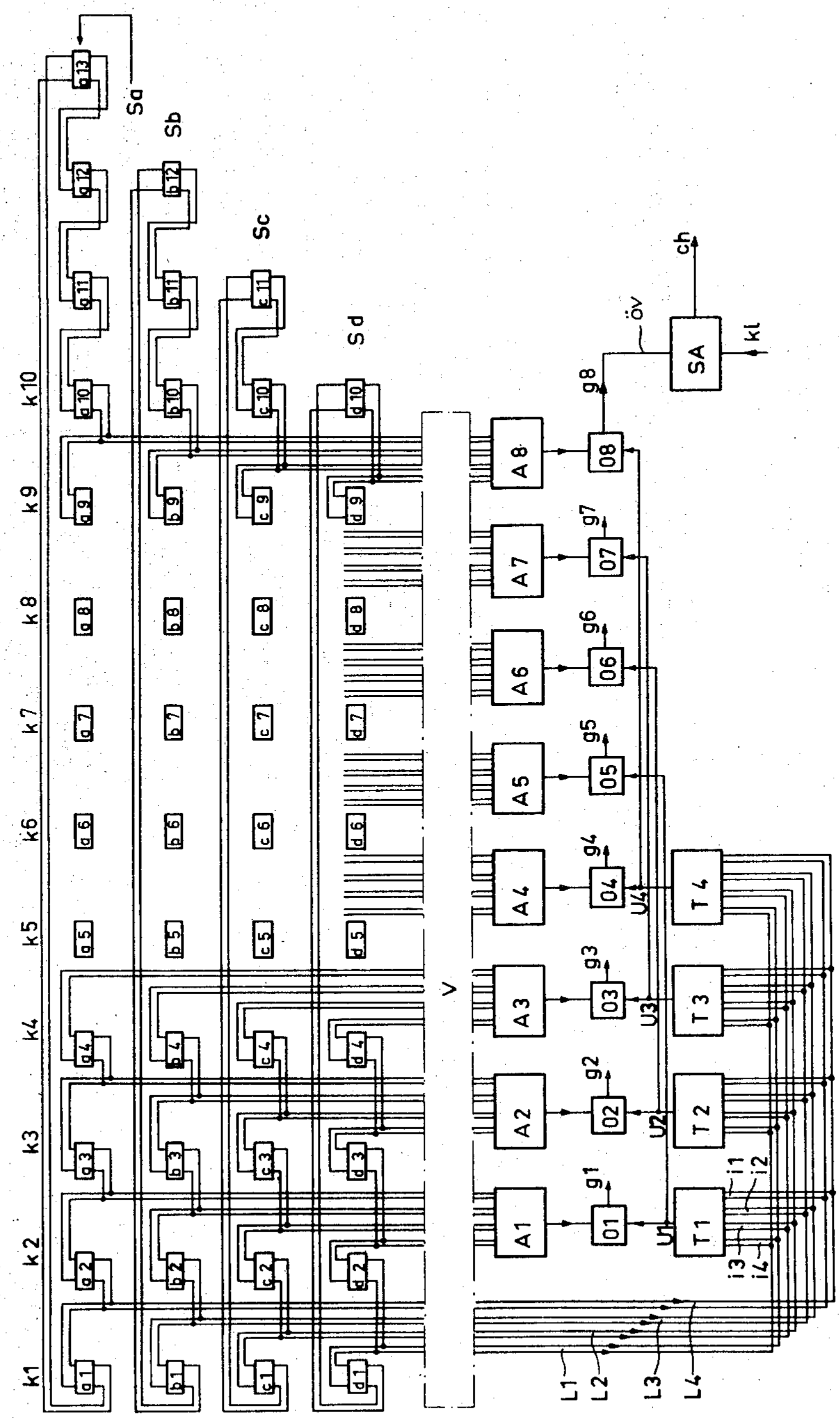


FIG.1

FIG.2

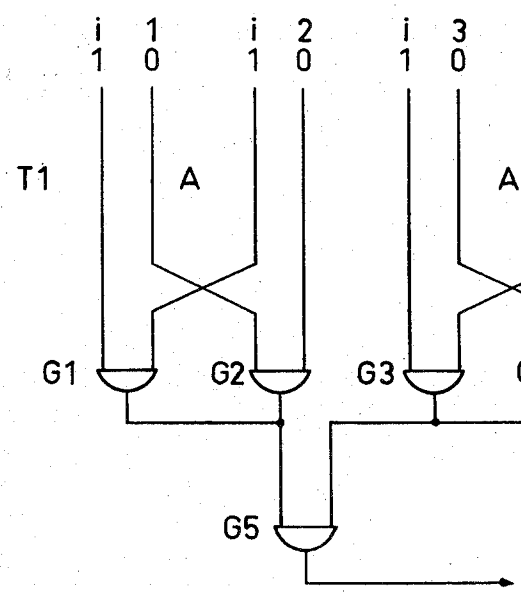

i 1 i 2 i 3 i 4
1 0 1 0 1 0 1 0
T1
A
A
G1
G2
G3
G4
G5

FIG.3

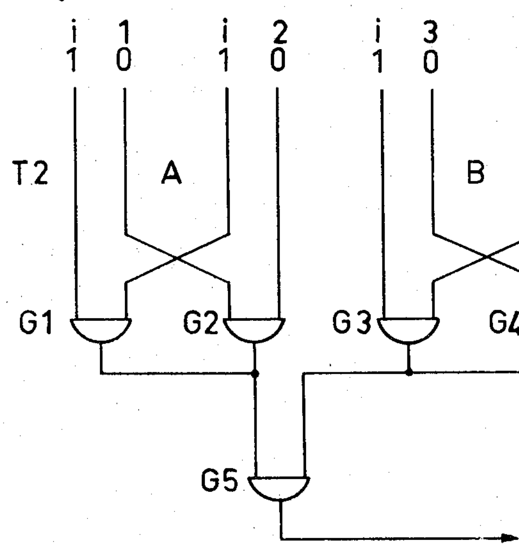
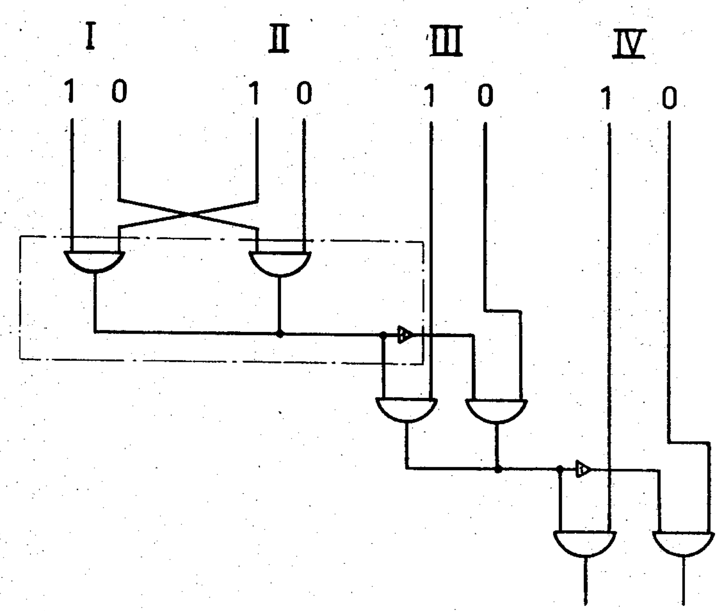

i 1 i 2 i 3 i 4
1 0 1 0 1 0 1 0
T2
A
B
G1
G2
G3
G4
G5

FIG. 4



CIPHERING MACHINE

It is previously known to produce these ciphering signals changed constantly for every character by means of a set of toothed wheels with a different number of teeth (preferably a prime number) which are mounted on the same shaft and are in driving connection with respective separately movable toothed wheels having the same number of teeth. At this second set of toothed wheels every tooth represent a binary bit, and the aligning teeth in the entire set of toothed wheels define a character formed by corresponding binary bits. Said second set of toothed wheels, thus, defines an many characters as there are teeth along the wheel circumference. At the beginning, the bits forming said characters are chosen at random. If the toothed wheels of the first set (having a different number of teeth) are stepped simultaneously one tooth at a time, it is obvious that, when the driving toothed wheel with the lowest number of teeth has been stepped through one entire revolution, the teeth then aligning in the driven set of toothed wheels will represent combinations of binary bits, i.e. characters, other than the original ones. The combinations are changed additionally when the drive wheel with the next to lowest number of teeth has completed its cycle, a.s.o. If, for example, the numbers of teeth of the drive wheels are prime numbers, it is understood that the same combinations (characters) as the original ones will not be obtained unless the set of drive wheels has been stepped a number of steps which is equal to the product of the respective number of teeth on the wheels comprised in the set.

Of the peripherally moving characters one character is selected for every ciphering operation, which character corresponds to a row of aligning teeth, either along one and the same reference line or with a systematic shifting between different lines in order to render unauthorized deciphering still more difficult.

The ciphering character obtained (in form of a signal) is superimposed to the simultaneously stepped character in clear so as to form the ciphered character.

The arrangement described above, however, involves several disadvantages.

From a purely ciphering point of view it shows the restriction that the aforesaid systematic change of characters in the peripheral series of characters for purely practical reasons hardly can be carried out for characters (tooth rows) other than such located relatively closely. Consequently, the possibilities of changing existing in reality between the total of characters located along all of the wheel circumference is utilized only to a small fraction.

These shortcomings are overcome by the ciphering machine according to the invention which is characterized in that it comprises an arrangement adapted at every ciphering moment automatically to select one or some of a number of selectable flip-flop columns in the flip-flop array and to transfer the signals corresponding to the flip-flop state in question to an adding device for forming the ciphering signal to be superimposed to the text in clear signal.

One embodiment of the invention is described below with reference to the accompanying drawings wherein:

FIG. 1 shows a basic diagram for a ciphering machine according to the invention;

FIGS. 2 and 3 show wiring diagrams for two examples, respectively, of character selectors comprised in the machine; and

FIG. 4 shows the wiring diagram for a type for adding circuits also comprised in the machine.

FIG. 1 shows in this embodiment four shift registers S_a, S_b, S_c and S_d, each of which comprises a chain of bistable flip-flops, which here are shown merely schematically as clocked.

The number of flip-flops varies from one chain to another. The shift register S_a, for example, which is represented in the FIG. by the uppermost row of flip-flops, comprises 13 flip-flops *a*1 —*a* 13. The shift register S_b representing the second row comprises 12 flip-flops *b*1 —*b*12, and in an analogous manner the shift registers S_c and S_d, respectively, formed by the third and fourth row of flip-flops comprise 11 and 10 flip-flops *c*1 —*c*11 and *d*1—*d*10, respectively.

In every chain the outlet of one flip-flop is connected in a usual way to the inlet of the next following flip-flop in such a manner, that upon stepping the register one the information in ever flip-flop in said chain is shifted forward one step. In the FIG. also is shown the last flip-flop in every chain connected to the first flip-flop in the same chain in order to form a closed step cycle.

From the beginning, all of the flip-flops are given, for example by punched cards, conditions preferably chosen at random. For the sake of clearness, however, the arrangement for this feed of information has not been included in the FIG. nor are the usual drive circuits for the shiftings shown.

The registers are intended to be stepped in parallel, i.e. the information bits in the first column *k*1 of flip-flops *a*1, *b*1, *c*1 and *d*1 are transferred to the flip-flops *a*2—*d*2 of the second column *k*2, and the contents of the latter is transferred to the flip-flops *a*3—*d*3 of the third column, and so forth. Every flip-flop column defines a character, which in this case comprises four bits. Owing to the difference in length of the cycles of the shift registers the bits fed in from the beginning into, for example, the first column *k*1 will be stepped unchanged to the "last" flip-flop *d*10 of the register S_d, corresponding to column *k*10. At a further parallel stepping the shift register S_d starts a new cycle with the beginning in *k*1 where the original bit in the flip-flop *d*1 returns, but the remaining bits in *k*1 are replaced by the bits in the flip-flops *a*13, *b*12, and *c*11, respectively, said bits being originally present in flip-flop *a*4, *b*3, and *c*2 of the registers S_a—S_c. At the next stepping the register S_c starts a new cycle with the beginning in *k*1, which now in addition to the original bit in the flip-flop *c*1 includes the new bits from *a*13, *b*12 and *d*10. This cycle is repeated in an analogous manner for the remaining registers S_b and S_a. It is understood that the original bit combinations do not appear again unless a number of steps equal to the product of the step number of the four shift registers have been stepped.

In the following the arrangement is described which is used for selecting the character i.e. the bit combination in a column, to be utilized for ciphering a character in clear in the form of a pulse fed simultaneously with the stepping of the shift registers.

For this purpose a number of character selectors are provided, in this case four in number, viz. T1, T2, T3 and T4. Every character selector has four pairs of inlets *i*1—*i*4, which are connected in parallel with the corresponding inlets of the other character selectors and adapted to be connected to four pairs of flip-flop outlets of an arbitrary column via a switch (system selector) V not described in detail. In the following argumentation the selectors are assumed, as indicated in the Figure, to be connected to the flip-flops *a*1—*d*1, respectively, of the column *kl* via conductor pairs L1—L4.

The outlets U1—U4, respectively, of every character selector T1, T2, T3 and T4 are connected to the one inlet of—in this case two—AND-gates **01** and **05**, and **02**, **06**; **03**, **07**; and **04**, **08**, respectively. The other inlet of every gate **01**—**08** is connected to the outlet of an adding circuit A1—A8, which like the character selector has four pairs of inlets, each pair being connected to the respective four flip-flop outlet pairs of its column via the switch V. In the embodiment shown the switch is assumed so be set that the adding circuits A1—A8 are connected to the flip-flop columns *k*2—*k*9 straight above them in the FIG. The outlets *g*1—*g*8, respectively, of the gates **0l**—**08** are all connected (but for the sake of clarity shown only for the outlet *g*8) to a first öv on a final adding circuit SA, to the other inlet *k*1 of which a binary coded signal in clear is fed in a way not described in detail synchronously with the stepping of the shift registers S1—S4. From the outlet *ch* of the adding circuit SA then the signal is taken out which is superimposed with the character content of the column in question, i.e. the ciphered signal.

Before describing the mode of operation of the above arrangement, it briefly shall be dealt with the construction of the character selectors T1—T4 and adding circuits A1—A8, with reference to FIGS. 2—4 showing embodiments of the construction of these arrangements. As appears from FIGS. 2 and 3 the character selectors T1 and T2 are built up of the same components, i.e. AND-gates G1—G5, but the internal connections are made different in order to give every character selector its own special nature. In FIG. 2, thus, the gate pairs G1, G2 and G3, G4 are shown connected in like manner with respect to the respective inlet pairs *i*1, *i*2, *i*3, *i*4, in that in both of the gate pairs G1, G2; G3, G4 the O-conductor in the left-hand inlet pair *i*1 and *i*3, respectively, extends to the 1-inlet on the right-hand gate G2 and G4, respectively, in the pair, and the 1-conductor in the right-hand inlet pair *i*2 and *i*4 respectively, extends to the O-inlet on the left-hand gate G1 and G3, respectively, in the pair. In FIG. 3 the relation is the same as regards the left-hand gate pair G1, G2 while at the right-hand gate pair G3, G4 the O-conductor in the left-hand inlet pair *i*3 extends to the O-inlet on the right-hand gate G4, and the O-conductor in the right-hand inlet pair *i*4 extends to the O-inlet on the left-hand gate G3.

By these two basic type connections represented by the left-hand and right-hand gate pair, which may be designated by A and B, the connections of the two remaining character selectors T3 and T4 are obtained in that T3 is built up of a left-hand par part of B-type and a right-hand part of A-type, and T4 is built up of a left-hand part B and a right-hand part also of B-type.

A Table of the buildup of the four character selectors T1—T4 and the bit combinations deductible from FIGS. 2 and 3) at the inlets in *i*1—*i*4 causing outsignal from the character selector in question, is shown below.

	Construction	Bit combinations			
Character selector:					
T1	A+A	1111	1100	0011	0000
T2	A+B	1110	1101	0010	0001
T3	B+A	0111	0100	1000	1011
T4	B+B	0101	0110	1001	1010

FIG. 4 shows the buildup of the adding circuits A1—A8 which are of mutually entirely equal nature and built up in a conventional way with unit circuits connected to each other of the type as framed in FIG. 4. A more detailed description appears not necessary.

A simple example may illustrate the mode of operation of the ciphering machine described above.

It is assumed that in a certain moment during the continued stepping of the field of columns *k*1—*k*9 in column *k*1 the bits O 1 0 O are found in the respective flip-flops *a*1—*d*1. This character signal is fed via respective conductor pairs L1—L4 to the inlets *i*1—*i*4 of all character selectors T1—T4. Hereby only the character selector T3 (according to the Table above) gives an outsignal to associated AND-gates 03 and 07. At the second inlets of these gates—as at the second inlets of all remaining gates—a signal is available by assistance of the adding circuit A3 (A7, respectively) which represents the total of the character bits in column *k*4 (and column *k*7). These bits are, for example, assumed to be 1 1 0 1 (and O 0 1 1). The total *b*1 then is 1 (O, respectively). As the outsignal of the character selector opens gate 03 (07, respectively), this 1-signal (O-signal, respectively) passes through to the inlet on the final adding circuit SA in order there to be superimposed to the text in clear impulse arriving at the same time. (The O-signal possibly can be used as a second superimposing pulse).

At the next stepping of the shift registers a character selector determined by the new bit combination in the flip-flop column *k*1 will open the passage for a new signal from a corresponding column, aso. For every new stepping, thus, a "-jump" forward or back of the practically always entirely available field of all informations in the flip-flop chains of the different shift registers is obtained. This renders possible a many times greater utilization of the total character variations in the information field than it is possible at the mechanic designs of ciphering machines.

The fact that in the example shown only four character selectors are required together with the four flip-flops in every column, has its reason in the circumstance that both the character itself and its pole switching are allowed to act upon the character selectors in their design shown.

In like manner as at the known ciphering arrangements operating with binary code, the deciphering is carried out simply by superimposing the ciphered signal pulses with the same series of pulses as used at the ciphering operation. Owing to the special nature of the binary system, the text in clear is restored.

The invention is not restricted to the embodiment described above, but various modifications thereof can be imagined, particularly with respect to the number of shift registers and the relation between their cycles.

The invention in principle is not bound to the use of shift registers, but also other electric arrangements with cyclic operations can be imagined, such as binary counters with associated logic circuits.

The application field of the machine, furthermore, can be widened to a large extent by making the cycles of the electric arrangements in question adjustable.

We claim:

1. In ciphering machine for ciphering text in clear produced in binary form, by superposing every text-in-clear character signal with a variable ciphering signal, comprising a plurality of electric devices stepped in parallel, said devices each having a different and repetitive operative cycle and forming an array of parallel rows of a different number of bistable flip-flops, the initial states of which are set according to an arbitrary scheme so that the states of flip-flops stepped in parallel define together, in every flip-flop column of said array, a ciphering character, whereby said column characters automatically change their bit composition every time a row of flip-flops has completed a cycle and starts a new one; the improvement comprising means, responsive to the present contents of a flip-flop column in a preselected reference position, to select, at each ciphering moment or step, at least one of the remaining flip-flop columns in the flip-flop array, as determined by said contents, and to transfer the signals corresponding to the states of the selected flip-flops to an adding device for producing said ciphering signal which is to be superposed on the text-in-clear signal.

2. A machine according to claim 1, where the means for selecting at least one certain flip-flop column comprises a plurality f of character selectors individually associated with a different one of said remaining flip-flop columns, and each of said character selectors having a plurality of inputs of the same number as that of the flip-flop rows, the inputs of all of said character selectors being connected in parallel to the corresponding outputs of the flip-flops in the column of said reference position, and each of said character selectors having its output connected to one input of an AND-gate, the second input of which is connected to the output of an adding circuit, said adding circuits having their respective inputs connected with the outputs of the flip-flops in the associated columns such, that for a certain character in said reference position column only one character selector is activated to supply an output signal to its AND-gate, at the second input of which the output signal from its adding circuit is always present, for effecting an output signal from said AND-gate, representing said ciphering signal.

3. A machine according to claim 2, wherein each of the character selectors comprises a system of AND-gates having its respective input connected to the output of the flip-flop of said reference position column in such a manner that an output signal from the gate system is obtained only in response to certain definite characters in said reference column.

4. A machine according to claim 2, wherein a switch is placed between the outputs of the flip-flop columns and the associated adding circuits for enabling shifting of the connections between said flip-flop columns and the character selectors.