Aug. 6, 1957 B. C. W. HAGELIN 2,802,047

ELECTRIC SWITCHING DEVICE FOR CIPHERING APPARATUS

Filed Oct. 16, 1953 2 Sheets-Sheet 1

FIG. 1.

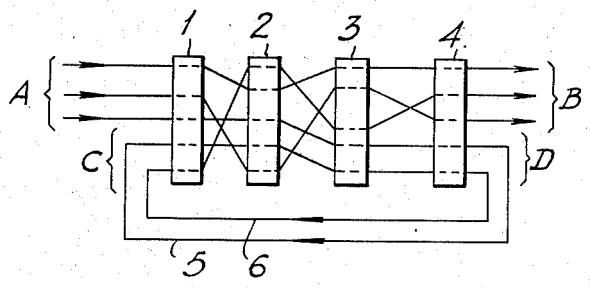


FIG. 2.

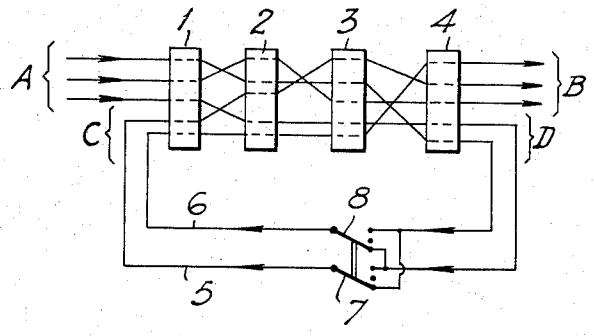
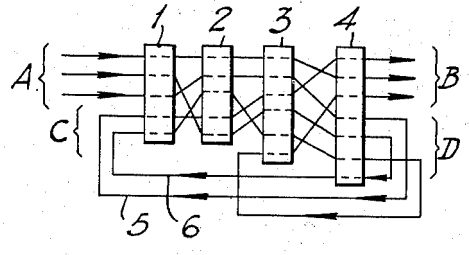


FIG. 3.



INVENTOR:
B. C. W. HAGELIN
By: Mann & Hall
ATTORNEYS.

Aug. 6, 1957 B. C. W. HAGELIN 2,802,047

ELECTRIC SWITCHING DEVICE FOR CIPHERING APPARATUS

Filed Oct. 16, 1953 2 Sheets-Sheet 2

FIG. 4.

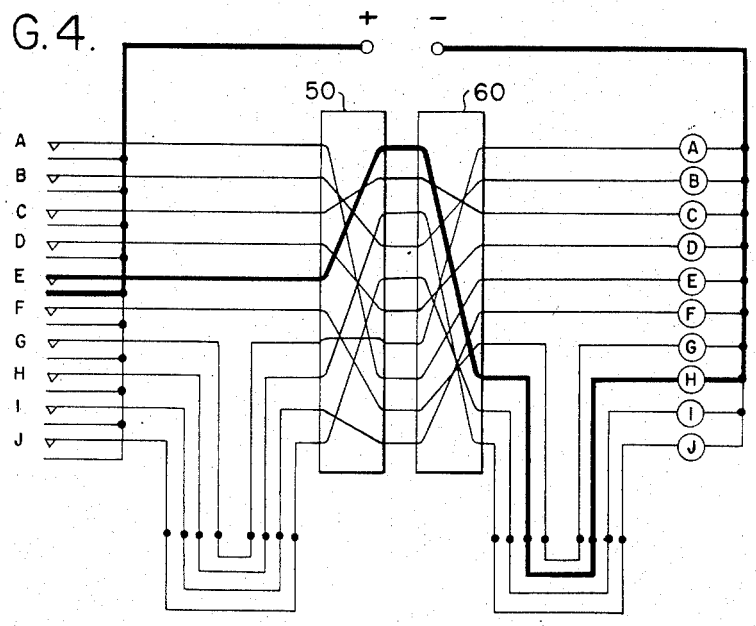


FIG. 5.

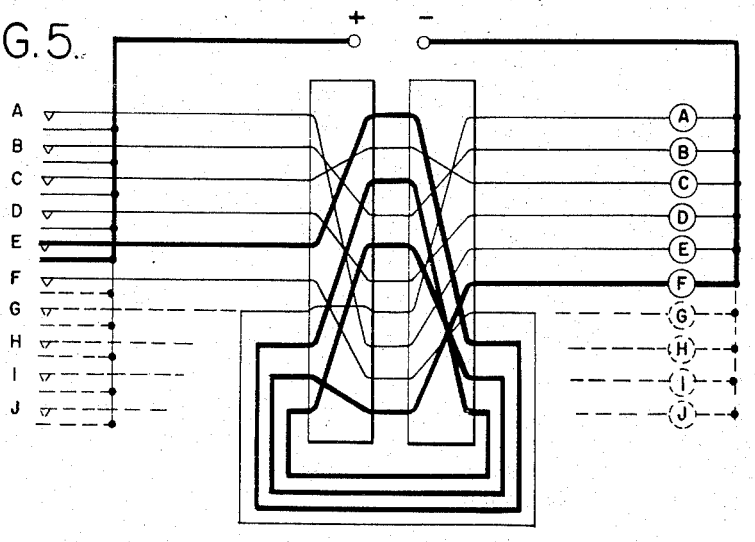
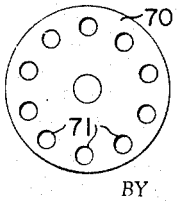


FIG. 6.



INVENTOR
B.C. W. HAGELIN

BY Moore & Hall

ATTORNEYS

United States Patent Office 2,802,047
Patented Aug. 6, 1957

2,802,047

ELECTRIC SWITCHING DEVICE FOR CIPHERING APPARATUS

Boris Caesar Wilhelm Hagelin, Zug, Switzerland

Application October 16, 1953, Serial No. 386,569
Claims priority, application Switzerland January 16, 1953
7 Claims. (Cl. 178—22)

This invention relates to an electric switching device including a set of ciphering cylinders for use in connection with ciphering apparatus.

In ciphering apparatus for the production of a normal code message in printed form usually only the 26 letters of the international telegraph alphabet are reproduced. In telegraphic ciphering in telewriter connections, however, a system has hitherto mainly been used which requires the ciphering of all 32 character combinations of the telewriter alphabet but has nevertheless dominated because of its simplicity (inversion). This system has, however, certain disadvantages.

In the first place the code message cannot be shown in printed form on the telewriter as the series of letters of the telewriter includes only 26 characters. Moreover, the ciphering of regularly repeated signals, as for example for controlling the carriage in sheet writers is a weakness in the ciphering art. It is therefore desirable to cipher only such characters as are part of the text, which, however, should also include intervals and character changing signals (such as "Zi," "Bu") since if such signals remain unciphered they could be quite dangerous.

A further desideratum in telewriter ciphering is that at least in certain cases the code message should be shown in printed form. It is, for example, conceivable that a case may occur where due to interruption of the telewriting connection information must be transmitted in another way. Reproduction of the secret signals which otherwise passed over the line in the form of printed characters would permit this, since the receiver can again decipher this text on his apparatus. In such cases the code message should, however, only include the 26 letters (or as many symbols as the telewriter can reproduce in the alphabet position).

The above mentioned requirement, that is, only to cipher text symbols or to produce a code message with one and the same ciphering mechanism which from case to case has a different number of symbols, can be satisfied by using what may be termed ciphering cylinders known per se, but a new form of connection must be provided. It is to be remembered that in using such cipher cylinders where a separate circuit is provided for each sign of the secret alphabet in teleciphering, precautions must be taken which in sending effect a translation into the telegraph impulse system and on receiving effect a re-translation of the telegraph alphabet into the multicircuit system.

The present invention is characterized by this that for effecting the ciphering cipher cylinders are used which are provided for as many circuits as correspond to the maximum number of the characters to be ciphered.

In the now common telewriter alphabet there are 29 symbols which under all circumstances must be ciphered, viz. 26 letters and, in addition, a symbol for word intervals and two signs for change signals. The cipher cylinders according to the invention should therefore be arranged for 29 connecting channels. In cases where it is

desired to produce a secret code which has only 26 written characters (which presumes that the printed matter includes only 26 of the 32 sign combinations of the telewriter) only 26 conductors will lead to and from the transit wheels. Now, the cipher cylinders have 29 inlet and exit points or contacts of which only a few can be left open if a free flow of current for all circuits and with all imaginable possibilities of connection of the cipher cylinders is to be ensured. For the solution of this apparently insoluble problem in accordance with the invention the three disengaged inlet contacts present in the above example are connected in any arbitrary manner with the three disengaged exit contacts. The system thus becomes capable of use for the ciphering of 26 symbols

In the present invention, concerning the technique of ciphering machines, the term "cipher cylinders" is employed to denote a flat disc-shaped machine element equipped on its sides with a circular group of contacts or channels which are in an irregular way connected to each other in pairs. Two or more of these cylinders are usually mounted parallel to each other and can be set in various relative positions by the means of a shifting device in order to sense, code or decode, the individual characters in the message.

In the drawings:

Figure 1 is a schematic showing of an assembly of cipher cylinders according to the invention.

Figure 2 is a modification of Figure 1.

Figure 3 is a further modification embodying the invention.

Figure 4 is a schematic circuit diagram showing the invention applied to two cipher cylinders.

Figure 5 is a modification of Figure 4.

Figure 6 is an elevation of one form of cipher cylinder.

In the accompanying drawings each of Figs. 1 to 3 illustrates an embodiment of the invention.

In Fig. 1 of the drawing the above explained principle of connection is illustrated. In Fig. 1 the reference numerals 1, 2, and 4 indicate four cipher cylinders each of which is provided five through-extending connecting wires, hereinafter referred to as "channels," of which in the example only three are used for ciphering purpose. Allotted to each such wire or "channel" are an inlet contact and an exit contact. In the example shown there are thus two disengaged inlet contacts and also two disengaged exit contacts. The three inlet conductors are indicated by A and the three exit conductors by B. The disengaged inlet contacts are indicated by C and the two disengaged exit contacts by D. In this example the first and the second inlet conductors reckoned from above are connected with the first and third exit contacts B solely by way of the channels of the wheels. The two disengaged inlet contacts are connected on the one hand with the disengaged exit contacts D through bye pass conductors 5 and 6 extending outside of the cipher cylinder system. Moreover, the first inlet contact C is connected with the second exit contact D in such manner through channels of the cylinders that the two bye pass conductors 5, 6 are connected in series. The second inlet contact C, however, is connected through channels of the wheels with the second exit conductor B, while the first exit contact D is connected with the third inlet conductor A. There is thus a connection between the third inlet conductor A and the second exit conductor B by way of the two disengaged contacts C and D connected in series, so that all the channels of the wheels are utilized for making the connections between the three conductors A and the three conductors B.

It may occur that certain circuits provide multiple channels according to the connections necessitated by the position of the cipher cylinders. In particular cases the

circuit of a single symbol may flow four times through the cipher cylinders.

The connections can thus be switched in or out or reversed by means of switches, as shown in Fig. 2, where the reference numerals 7 and 8 indicate switches associated with the conductors 5 and 6.

It is further possible to select a number of circuits in connection with the cipher cylinders which is higher than is absolutely necessary for the ciphering of the symbols in question. Such a construction would result in certain technical ciphering complications.

An additional advantage of the above described connections consists in this that one and the same ciphering mechanism can be used both for the normal telewriter and for printing ciphering machines which having regard to the increasing mechanisation of the ciphering services both for military and for diplomatic purposes allows an extensive standardising of the constructions.

Variations are possible where in a group of cipher cylinders the individual wheels present different numbers of channels and the circuits not traversed can be selectively connected together, a connection being effected from beginning to end of the group or only in part tappings thereof. An example of such an arrangement is shown in Fig. 3 of the drawing. In this example the cylinders 1 and 2 like those in Figs. 1 and 2, each has five channels while the cylinder 3 has six and the wheel 4 has seven. The first inlet conductor A is connected with an exit conductor B only through the channels of the cylinders, while the connections between the two remaining inlet conductors A and the two remaining exit conductors B contain also bye pass conductors which all claim disengaged channels.

The alternative arrangement of rotating and stationary cipher cylinders provides another special case, the latter having an excess number of channels which are separately connectible.

Figures 4 and 5 represent schematic designs of a cipher device set up with lamps to be lighted, A through J, in respective circles, and two ciphering cylinders, 50 and 60, to demonstrate the application of ten channels arranged in a circle circumferentially. The channel arrangement is shown in Figure 6 wherein cylinder 70 is provided with a plurality of suitable channels 71.

These cipher cylinders are usually employed to capacity, and in this case it would mean that they are intended for a ten-character alphabet, each channel providing a path for a current relating a character. The connection between an incoming contact, such as E, and an outgoing contact, such as H, is indicated in the drawing of Figure 4 by heavy lines, from an inspection of which it will be noted that the application of a potential at E will cause the lamp H to glow. This is, of course, a purely demonstrative circuit, and the lamp H may be replaced by a relay or any other piece of equipment of suitable character.

Figure 5 illustrates the use of the same ciphering cylinders as in Figure 4, but this time wired to operate on a six-character alphabet requiring six circuits. This arrangement leaves four channels free and requires a special type of cross-connected shifting device. Here again the channels employed in a signal from E input to, in this case, the F output, are marked in red.

It will be understood that the number of characters in any encoded message must not, with the present construction, exceed this number of channels, and we are here primarily concerned with a device which adapts a machine having cipher cylinders of M channels to a ciphered text containing a lesser number N unique characters, and therefore a lesser number of channels. This shifting device increases greatly the flexibility of a given ciphering machine and permits the cipher mechanism to be used in ciphering operation and still meet the revised requirements. Ciphering operation as the phrase is here employed is intended to cover both enciphering and deciphering.

It should be clear that the present invention requires no fixed numbered ratio, which occurs in some other arrangement, such as 1:2, 1:3 or 1:4.

The arrangement for the ciphering of an alphabet of suitable number of characters can be used for the above described and any other embodiment of the invention, a limit being set only by this that not more symbols should be present than there are channels.

I claim:

1. In a combination in a shifting device for a cipher machine employing a varied number of characters in a ciphered text wherein the number of channels available is in excess of the number of channels required, comprising a plurality of ciphering cylinders having switch contact means for connecting the channels of one cylinder to those of another in the many relative positions said cylinders may have and circuit means connecting said excess channels of one cylinder to the excess channels of another cylinder whereby on relative displacement of the cylinders to successive positions the required channels are maintained conducting for all operating positions of the cylinders.

2. The combination set forth in claim 1, each said circuit means connecting said excess channels having a switching means forming a part thereof.

3. In combination a cipher device comprising a set of relatively movable cipher cylinders having through-extending electrically conducting channels and connections between the channels of the various cylinders to form paths for transmitting signs through the set of cipher cylinders, said cipher cylinders being subject to a ciphering operation, characterized in that said connections are so arranged that when a set of cipher cylinders having a given number M of through-extending conducting channels is used for transmitting a given number N of signs, N being a number smaller than M, the inlets of the *M* minus *N* unoccupied channels of the first cipher cylinder are each connected with an individual one of the exits of the *M* minus *N* unoccupied channels of the last cipher cylinder of the set of cylinders.

4. The combination set forth in claim 3, switch means for said channels.

5. The combination set forth in claim 3, said connections between the inlets and outlets of those of said channels which are unoccupied comprising at least in part by-pass conductors external of the set of cipher cylinders.

6. The combination set forth in claim 5, said external by-pass conductors having switches inserted therein.

7. In combination, a cipher device comprising a set of relatively movable cipher cylinders each having information conveying means carried thereby, transfer means between said means of the various cylinders to transmit information through the set of cipher cylinders, characterized in that said conveying means are so constructed and arranged that when a set of cipher cylinders having a given number M of said conveying means is used for transmitting a given number N of unique items of information, N being a smaller number than M, the information receiving portions of the *M* minus *N* unoccupied conveying means of the first cipher cylinder are each connected with an individual one of the delivery portions of the *M* minus *N* unoccupied conveying means of the last cipher cylinder of the set of cylinders.

References Cited in the file of this patent

UNITED STATES PATENTS

1,683,072	Hebern	Sept. 4, 1928
2,402,182	Rosen	June 18, 1946

FOREIGN PATENTS

248,973	Switzerland	Mar. 16, 1948