

Dec. 15, 1959

B. C. W. HAGELIN

2,917,579

CIPHERING MACHINES

Filed Aug. 1, 1955

FIG. 1.

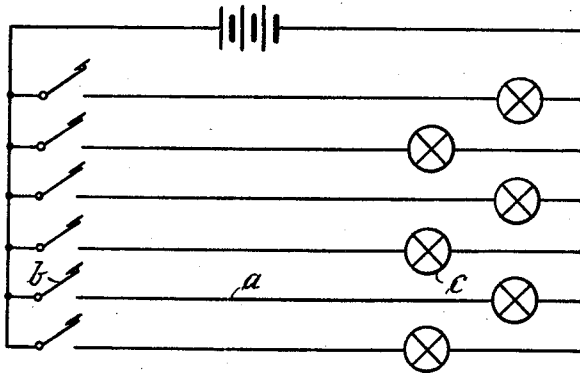


FIG. 2.

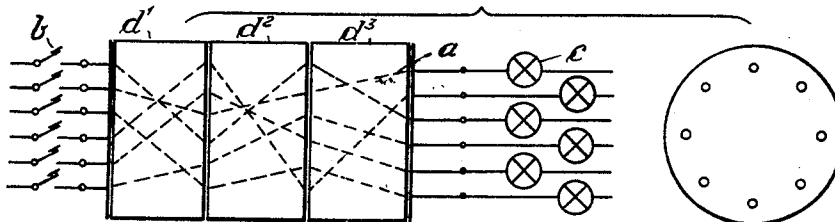
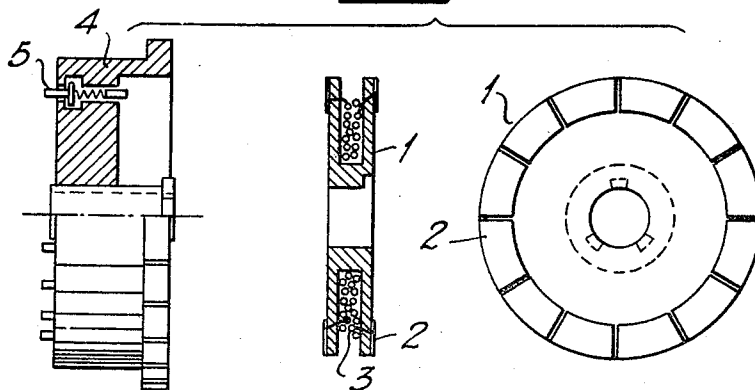


FIG. 3.



INVENTOR:
BORIS C.W. HAGELIN
BY: *Moore & Hall*
ATTORNEYS.

1

2,917,579

CIPHERING MACHINES

Boris Caesar Wilhelm Hagelin, Zug, Switzerland

Application August 1, 1955, Serial No. 525,702

Claims priority, application Switzerland October 14, 1954

5 Claims. (Cl. 178—22)

The present invention relates to cipher cylinders for ciphering machines and more particularly to ciphering machines of the type known under the trademark of "Enigma." The object of the invention is to provide an improved cipher cylinder for use in connection with such machines.

The principle of the Enigma machine is based on the fact that the individual characters of an alphabet are represented by individual channels of a set of connecting channels which are electrically conducting while isolated from each other. In Fig. 1 of the accompanying drawing such a set of connecting channels is illustrated in a diagrammatic manner. In this figure the inlets of the channels *a* are provided with contacts *b* operable by keys and the outlets of the channels are provided with electrical indicators *c*, as for instance glow lamps, the arrangement being such that the depression of a key will cause the indicator belonging to the respective channel to operate.

In order to allow a ciphering operation, the set of channels is not constructed as a cable but comprises a plurality of cylinders each of which may be considered as a section of a cable with its channels arranged in a circular row around a central axis. In Fig. 2 of the drawing three such cylinders are shown where they are indicated by the reference characters d^1 , d^2 , d^3 . Inside said cylinders the channels are connected crosswisely according to a given scheme. The result will be a shifting of the relations between the key operated contacts and the indicators. In case of an unsymmetrical arrangement of the channels of the various cylinders it is possible by rotating the cylinders one or more steps (channel divisions) with relation to each other, to obtain continually shifting relations between the key bank and the indicator bank, as may be clearly understood by an inspection of Fig. 2.

Provided the arrangement of the channels of the cylinders and the program for the stepwise rotation thereof are known, it will be possible to start a cipher communication between two machines provided with the device above described. For enciphering purposes it is only necessary to interchange the key operated contacts and the indicators.

In practice, the cipher cylinders are provided at least at one of their flat surfaces with sliding contacts in order to secure a good transmission of current to the adjacent cylinder or cylinders. In order to obtain a maximum number of variations it has been suggested to make the arrangement of the channels of the individual cylinders variable. According to a known structure the cylinders are formed with rigidly mounted inlet and outlet contacts the interconnections of which may be changed by resoldering. In another construction rigid inlet contacts are used, while the outlet contacts are connected by soldering to flexible connecting channels and shaped as plugs the positioning of which in the cylinder may be varied.

2

All known constructions of the Enigma machine, however, are very big so that they do not permit a speedy operation as required, for instance, in automatic ciphering operations in telewriter systems. (In such systems each individual character requires the rotation of at least one cylinder at least one step. The telewriter operates at full load with 400 signs a minute.)

The present invention relates to a cipher cylinder construction the dimensions of which may be so reduced that the mass relations permit the use of the cylinder in telewriter cipher operation. The exactness of the sliding contacts as required by the small size of the cylinder, however, renders the manufacture uneconomic as compared with the manufacture of the bigger cylinders hitherto used. Especially, it is to be noted that for effecting a shifting of the inner connections of the cylinder a single resoldering operation is required. This operation, however, can be carried out only by persons skilled in the art of fine mechanics. In practice, this fact causes the disadvantage that for each ciphering machine a great number of cylinders must be available which have to be interchanged individually or in groups for shifting the base key. This measure, however, results in still increased costs of manufacturing the device, which is not desirable.

In order to avoid this drawback the cipher cylinder according to the invention is divisible into two main members. One member carrying the precision sliding contacts and the power transmission means, may be considered as neutral from ciphering technical point of view and may remain unchanged. Said member serves as a socket for the other member which comprises a double flat commutator representing the ciphering element proper, see Fig. 3.

Said insertion member comprises a narrow flanged reel on the flat surfaces of which contact laminae 2 are provided. The two rows of contact laminae are electrically connected together according to a given scheme by means of isolated conductors 3. The insertion member may be locked to the socket member 4 by means of a bayonet clutch in a rapid and reliable manner. The socket member 4 is formed with a circular set of axially yielding contacts 5 for effecting connection between the outlets of the respective insertion member and the inlets of an adjacent cylinder.

As the insertion member has no movable elements it may be manufactured in a very economic manner as a mass article. The only manual work required is represented by the internal connections via the conductors which cannot be subject to mechanical work, since said connections must be different for each individual insertion member.

According to the invention a ciphering machine provided with cipher cylinders of the construction described may be delivered with a single set of socket members and, as the case may be, two or more sets of insertion members in order to allow interchangeability of insertion members according to directions.

The means provided in connection with the Enigma machine for stepwise rotation of the cipher cylinders is similar to that of the train of wheels of a counting register. For each character to be ciphered the cylinder numbered 1 should be rotated one step. Following a complete revolution of cylinder d^1 , cylinder d^2 is rotated one step, and so on. It is to be noted that, of course, other arrangements than those above described may be used operating according to a different scheme for the stepwise rotation of the cipher cylinders. Thus, for instance, the scheme for the stepwise rotation of the cipher cylinders may be so arranged as to cause the cylinders to move themselves and the adjacent cylinders by means

of pins via a drum having slide bars as shown in my copending U.S. Patent No. 2,765,364, granted October 2, 1956, showing bars 9—38 and dual position pins 64. Also shown are means to drive the several key wheels 1—5 with pins 64 which can be used to impart driving power to the sockets herein. The program for operating the cipher cylinders obtainable in this way is re-coupled to such a device and presents a very great number of variation possibilities.

When cipher cylinders of the above described design are combined with such an operating device, the pins should accordingly be situated on the neutral socket members, since said members represent movable elements which, however, need not be exchanged individually.

While there have been described above what are presently believed to be the preferred forms of the invention, variations thereof will be obvious to those skilled in the art and all such changes and variations which fall within the spirit of the invention are intended to be covered by the generic terms in the appended claims, which are variably worded to that end.

I claim:

1. A cipher cylinder of low inertia for use in automatic ciphering operations in telewriter systems comprising a body member having a recessed central portion forming a socket, a ciphering member comprising a double flat commutator ciphering member comprising a narrow disc having a set of contacts on each side thereof, connector elements connecting a contact of one set to a contact of the other set according to a preselected ciphering arrangement, said ciphering member being readily insertable into said socket in any one of a plurality of possible cipher positions, and means to hold said ciphering member in said socket in a selected position.

2. The combination set forth in claim 1, said body member having dual-position elements for making circuit completing contact with said contacts of said commutator ciphering member, said dual-position elements being individually movably mounted on said body member for movement to an operative or to an inoperative position.

3. The combination set forth in claim 2, said dual-position elements comprising annularly arranged axially displaceable pins, said cipher element comprising a flanged reel with said connector elements positioned around the periphery thereof between the flanges of the reel, said sets of contacts comprising circular rows of segmental contact laminae on opposite sides of said reel adjacent the periphery thereof.

4. A ciphering cylinder having movable contacts, characterized in that said cylinder is composed of two relatively rotatable members, viz. a socket member and a disc-shaped insertion member, said socket member carrying movable sliding contacts for connecting insertion members and means for coupling the cylinder to a driving device, while said insertion member is provided with circular rows of contact laminae, with the laminae at the different rows interconnected by through extending conductors, said insertion member being insertable in various angular positions into the socket for changing the connections as effected by the cylinder.

5. A ciphering cylinder as claimed in claim 4, in which the socket of the ciphering cylinder carries annularly arranged, axially displaceable pins which may occupy two end positions.

References Cited in the file of this patent

UNITED STATES PATENTS

1,652,708	De Leeuw	Dec. 13, 1927
1,663,624	Damm	Mar. 27, 1928
1,905,593	Korn	Apr. 25, 1933
1,953,829	Morris	Apr. 3, 1934
2,529,487	Cooley	Nov. 14, 1950
2,753,034	Hell	July 3, 1956
2,777,556	Hagelin	Jan. 15, 1957
2,802,047	Hagelin	Aug. 6, 1957

FOREIGN PATENTS

550,796	Germany	May 20, 1932
118,034	Australia	Jan. 17, 1944