Oct. 4, 1927. 1,644,239

A. G. DAMM

APPARATUS FOR PRODUCING SERIES OF SIGNS

Filed Sept. 25, 1924

Fig. 1.

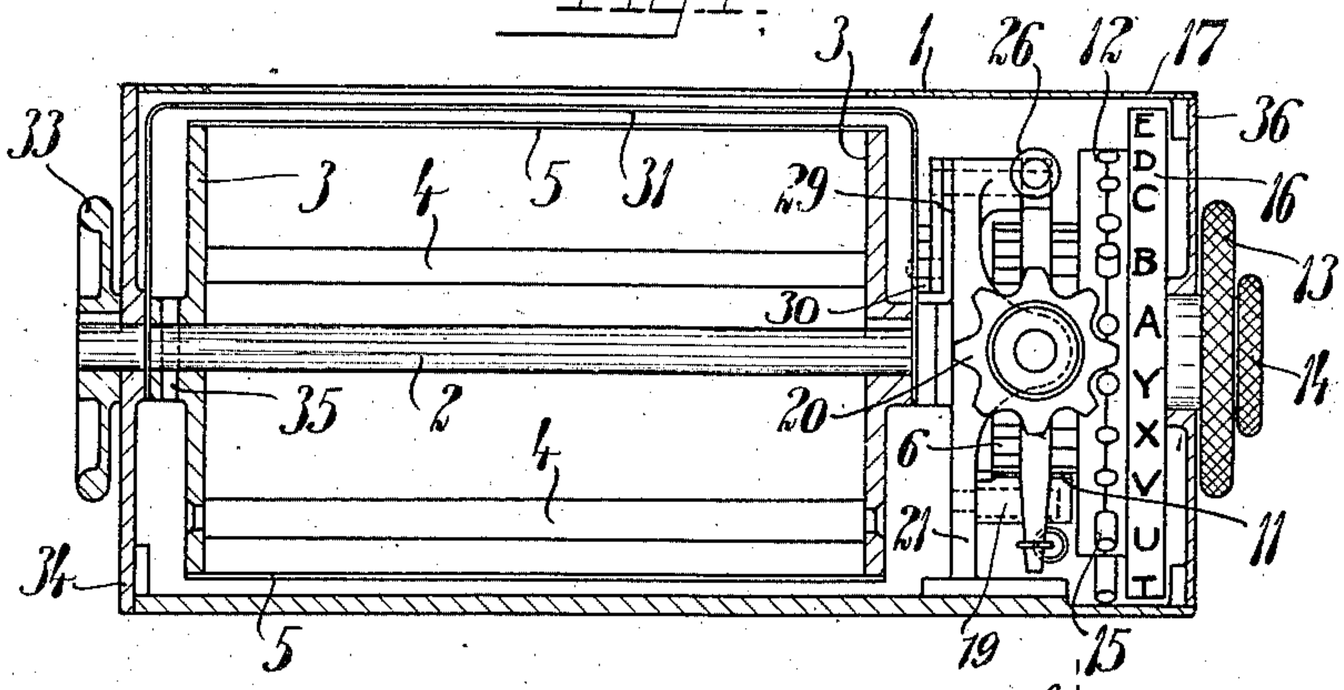


Fig. 2.

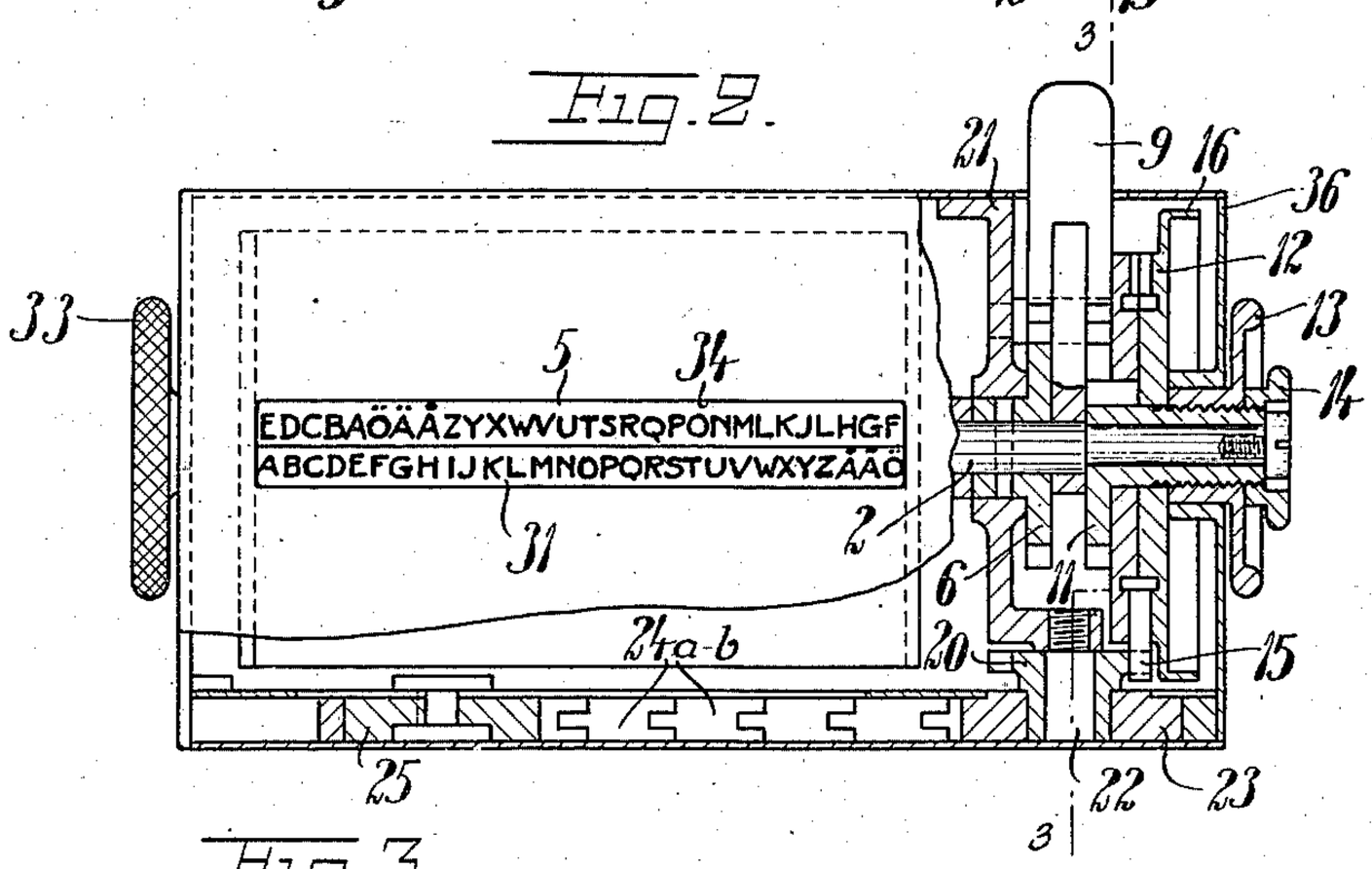


Fig. 3.

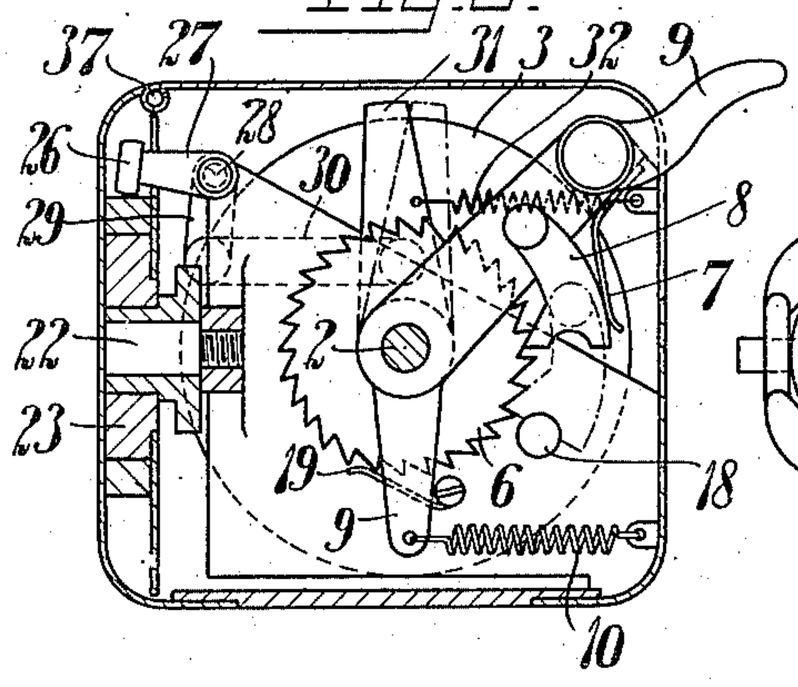
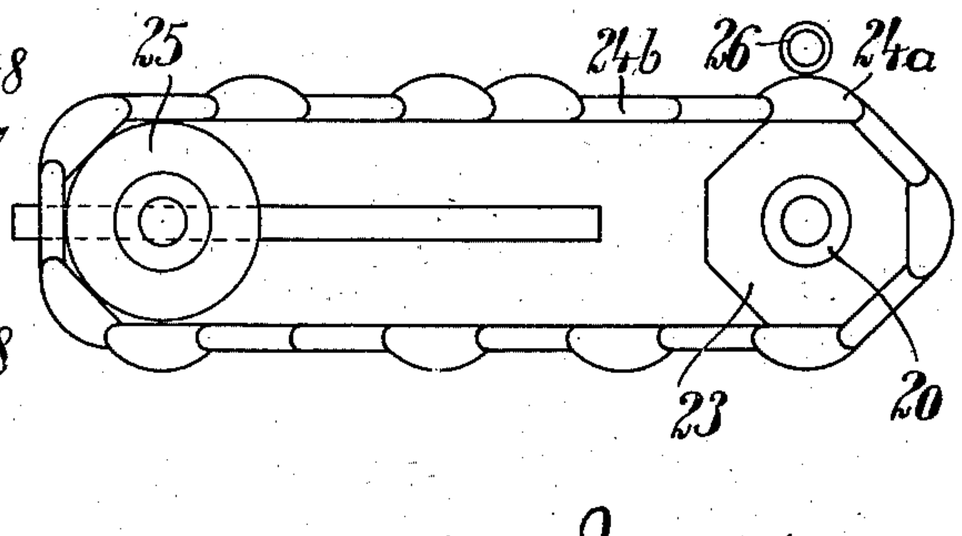


Fig. 4.



Inventor
David G. Damm,
By Mason Orth & Co
Atty

Patented Oct. 4, 1927. 1,644,239

UNITED STATES PATENT OFFICE.

ARVID GERHARD DAMM, OF HUDDINGE, SWEDEN.

APPARATUS FOR PRODUCING SERIES OF SIGNS.

Application filed September 25, 1924, Serial No. 739,890, and in Sweden September 28, 1923.

The present invention relates to a ciphering apparatus, which on account of its construction is especially suitable for use as a portable machine and, in comparison with hitherto constructed portable devices of a similar kind, is characterized by simplicity of mechanical details and therefrom smallness of dimensions, which simultaneously facilitate its manipulation and the production of ciphers of a more complicated nature and with a longer mutation period than hitherto attainable by similar devices.

The extension as far as practically possible of the length of the series of different positions of the ciphering members in relation to one another, which series determines the successive possibilities of sign substitutions during the ciphering process, and which series must become periodical, as in every mechanical ciphering device, is of the utmost importance for the security of the cipher, said security, as is well known, depending partly upon the proportion between the length of period of the mutation series and the length of the cipher, respectively of the text to be enciphered.

Here and in the following, "mutation series" means the number series whose terms successively indicate the distances in a certain standard series alphabet between signs successively corresponding to each other in clear text and cipher.

Apart from said proportion the security of the cipher also depends upon the regularity of the mutation series, which mutation is more or less conspicuous depending upon the characteristics of the cipher.

Because only n different terms can be contained in the mutation series, when a standard series of n signs is used, a greater or smaller number of these terms must be repeated a certain number of times in a series having for instance a length of period of x. n terms, it evidently may occur and, indeed, must occur sooner or later within a continued ciphering process, that repetitions of sign combinations in the text coincide with repetitions of combinations of terms in the mutation series. Such repetitions can, according to known cryptological laws, give indication for conclusions of probability as to the mathematical construction of the mutation series, which conclusions in their turn can facilitate an unauthorized deciphering of the cipher.

Apart from the extenson of the length of period it is consequently desirable on the one hand to construct every mechanical ciphering device so as to prevent as far as possible the formation of identical intervals of repetition and a uniform distribution of the same within the mutation period, and on the other hand to obtain prime number intervals and such intervals, the prime factors of which are not the same as those of the periods of movement of the mechanical members of the apparatus or those defining the arrangement of the key members.

It is the object of the present invention to realize these intentions as far as possible.

Further it has for its object to facilitate a quick and easy exchange of the members influencing the whole procedure of ciphering and an easy adjustment of said members relatively to each other.

The accompanying drawing illustrates one embodiment of my invention. Fig. 1 shows a longitudinal section and Fig. 2 a view of the apparatus from above, partly in section. Fig. 3 shows a cross-section on the line 3—3 of Fig. 2 and Fig. 4 the arrangement of the chain, a member representing an arbitrary series of figures.

In a casing of substantially square shaped cross-section a shaft 2 is rotatably mounted, on which are fixed two circular disks 3, rigidly connected to each other by means of rods 4. On the circumferences of said disks 3 axially extending rectangular bars 5 are detachably mounted, each bar carrying a normal series of signs, an alphabet, on its outside. The ciphering member or drum constituted by said disks 3 and bars 5 is herebelow referred to as the "cylinder".

Further, on the shaft 2 is fixed a ratchet wheel 6, in which engages a pawl 8, actuated by a spring 7. Said pawl 8 is journalled on the one arm of a double-armed lever 9, pivotally journalled on the shaft 2. The other arm of the lever 9 is actuated by a spring 10 fixed to the casing and tending to keep the lever 9 in the position shown in Fig. 3. The ratchet wheel 6 has the same number of teeth as the number of bars 5 of the "cylinder".

Further, a ratchet wheel 11 is rotatably journalled on the shaft 2. To the hub of said wheel 11 is secured a pin-wheel 12, kept in position by a milled nut 13 and a locking nut 14. On the circumference the pin-wheel 12, which may be composed of two disks as is shown in the drawing, is formed with radial holes arranged at equal distances from

one another, in which holes pins 15 can be placed. The pin-wheel 12 is provided with a cylindrical flange 16, carrying signs, corresponding to each pin-hole of the pin-wheel 12, the chance position of which can, by means of said signs, be read off through a small aperture 17 (Fig. 1) in the casing 1. The ratchet wheel 11, which is actuated by the pawl 8, actuating also the ratchet wheel 6 has the same number of teeth as the number of pin-holes of the pin-wheel 12, said number being smaller than the number of teeth of ratchet wheel 6. Said two numbers of teeth are so chosen in relation to each other and to the movements of the lever 9, that said lever, when its upper arm is pressed down fully from the position shown in Fig. 3, turns the ratchet-wheel 6 through an angle corresponding to two teeth, but the ratchet wheel 11 through an angle corresponding to one tooth only. The downward movement of the lever 9 is limited by the pawl 8 stopping against a pin 18 (see the position of said pawl shown by dotted lines in Fig. 3). The two ratchet wheels 6 and 11 are kept in their positions by a spring 19 bearing against them, as is shown in Fig. 3.

The pins 15 of the pin-wheel 12 actuate a driving wheel 20 rotatably journalled on a pin 22 secured to a bearing 21. To the hub of said driving wheel is fixed an octagonal prism 23, which serves to transmit the movement of the driving wheel 20 to a chain, composed of links 24^a and 24^b of different height and arranged according to an arbitrarily chosen series of figures. This chain moves round an adjustable guide-roller 25. Every time a pin 15 actuates the driving wheel 20, this is turned one eighth of a revolution, whereby the chain is moved forward a distance corresponding to the length of one chain link. Against said chain and opposite the prism 23 a roller 26 is pressing, which is journalled on a pivot at the end of an arm 27, fixed on the one end of a rocking shaft 28, which is journalled in a projection of the bearing 21. At the other end of said rocking shaft 28 and at 90° angle to the arm 27 an arm 29 is fixed. which by means of a link 30 is connected to a U-shaped member 31, journalled on the shaft 2. A spring 32 actuates said member 31 in such manner that the roller 26 is kept pressed against the chain 24^a, 24^b.

When the roller 26 engages a low link 24^b, the member 31 occupies the position shown by full lines in Fig. 3, while it is forced to occupy the position indicated by dash and dot lines in Fig. 3, when the roller 26 engages a high link 24^a. In the upper side of the casing 1 a rectangular aperture 34 is provided, the dimensions of which correspond to the surface of two adjacent bars 5 of the "cylinder". The member 31 is so arranged relatively to said aperture 34 as to cover alternately the one or the other of the two bars below the aperture 34, depending upon its chance position. The member 31 carries an alphabet on its outer side (see Fig. 2).

When the apparatus described above is to be used for enciphering, the "cylinder" 3, 5 is turned into an initial position previously agreed upon by means of a disk 33 fixed on the shaft 2 outside the casing 1.

According to agreement between the correspondents, the operator before or after depression of lever 9 one or more times, locates that letter in the alphabet on the member 31, which corresponds to the first letter of the clear text. The letter on the cylinder alphabet, which is simultaneously visible through the aperture 34 opposite said letter on the member 31, is then noted as the first sign of the cipher. Thereafter the lever 9 is again pressed down fully and that letter of the alphabet of the member 31 which corresponds to the second letter of the clear text is located, whereupon the letter of the cylinder alphabet then visible through the aperture 34 below or above the said letter on the member 31 is noted as the second sign of the cipher. Identical manipulations are then repeated for each following sign of the clear text.

That a deciphering of the cipher thus obtained can be effected by the same apparatus is obvious from the fact that the different alphabets during deciphering will successively occupy the same relative positions as during the enciphering process.

Whether the signs of the alphabet of the member 31 and of the cylinder alphabets are arranged in reversed order or are arbitrarily reciprocal two and two, according to any of the types:

I. abcdefghijklmnopqrstuvwxyz
zyxwvutsrqponmlkjihgfedcba
II. edcbazyxwvutsrqponmlkjihgf
jihgfedcbazyxwvutsrqponmlk
and so forth

or:

I. abcdefghijklmnopqrstuvwxyz
II. jmkxygfplacibvzhswqutnrdeo
psjwihlfecmgkxuatvbqordnzy
and so forth

where I indicates the alphabet of the member 31 and II the cylinder alphabets, the sign substitutions can be effected in quite the same way in deciphering as in enciphering.

If, however, the alphabet of the member 31 and the cylinder alphabets are irregular relatively to one another, it is necessary, if sign-substitutions in the enciphering process have been made from the alphabet of the member 31 to the cylinder alphabets, to make the corresponding substitution from the cylinder alphabets to the alphabet of

the member 31 when deciphering, and vice versa.

In order to explain the function of the apparatus, as regards the mutation series on which the enciphering is founded, and to simplify the description, it is in the following supposed that all cylinder alphabets have their signs arranged in inverse order to that of the alphabet of the member 31 and are displaced in relation to one another correspondingly to their order around the cylinder in opposite direction to the direction of movement of the cylinder.

In the apparatus described above, the drum, of course may be provided with any desired number of alphabet bars. Certain of said bars may be dispensed with at arbitrary places or they may have no alphabet. In such case, it will in certain positions of the drum happen that apart from the alphabet of the member 31 no alphabet will appear in the aperture of the casing, in which case the lever 9 must be pressed down two or more subsequent times, before any sign substitution can be made.

It may for instance be supposed that the cylinder carries 29 bars and that the alphabets number 7 and 12 are dispensed with, so that at stillstand of the member 31 and a stepwise driving of the cylinder two steps at a time, the cylinder alphabets counting from 1 will appear successively in the aperture 31 in the following sequence:
1, 3, 5, 9, 11, 13, 15, 17, 19, 21, 23, 27, 29, 2, 4, 6, 8, 10, 14, 16, 18, 20, 22, 24, 26, 28, 1, 3, 5, 9 . . .
and under said suppositions result in a mutation series identical to said series of numbers.

If, however, the member 31, which is supposed at the beginning of the operation to have occupied the position shown by full lines in Fig. 2, changes its position for instance at the first cylinder movement, the cylinder alphabet number 4 will appear in the aperture 31 and not the alphabet number 3. If the member 31 is not moved at the next manipulation, the alphabet number 6 will appear, while, if the member had changed its position, alphabet number 5 would instead have appeared. Thus the movement of the member 31 normally serves to produce quite the same effect regarding the relative displacements between the alphabet of the member 31 and the cylinder alphabets as if the cylinder were turned alternately 2, 3, or 1 steps. But since empty spaces on the circumference of the cylinder can necessitate one or several extra manipulations and the effect of such spaces will be dependent upon the chance position of the member 31, i. e. of the composition and chance position of the chain 24^a, 24^b, which position in its turn depends upon the arrangement and chance position of the pin-wheel 12, it is consequently clear that, by utilizing said conditions, an enormously complicated series of alphabet changes can be attained, the character of which cannot be expressed by any generally applicable and analytically useful formula, because one and the same effect can have several different causes.

Thus for instance a subsequent reading off on alphabets numbers 1 and 5 can depend upon any one of below explained suppositions:

(*a*) Rotation of the cylinder from 1 to 3, empty space on 3, and rotation of the cylinder to 5, the chain being unmoved or having two identical links successively in operating position.

(*b*) Rotation of the cylinder from 1 to 3, a high link of the chain being moved into operation position, which results in reading-off position 4, empty space 4, rotation of the cylinder to 5, which becomes reading-off position, because a high link of the chain is again moved into operative position.

(*c*) Rotation of the cylinder from 1 to 3 with reading-off position 2 on account of a high link of the chain being moved into operative position, empty space on 2, rotation of the cylinder to 5, which becomes reading-off position, because a low link of the chain is moved into operative position.

Supposing the cylinder to contain an odd number, 2N–1, of bars 5, the pin-wheel to be arranged for S pins, the number of chain-links to be K and said different numbers to have no factor in common, the length of period will be $P=(2N-1)\ S.\ K$ manipulations; and if a certain number T of empty spaces occur on the cylinder, the period will be $P=(2N-1-T)\ S.\ K$ sign substitutions, as a periodicity, can, of course, occur only when all ciphering members have returned to their initial positions relatively to each other.

Those parts in the above described apparatus, which influence the composition of the cipher, are easily and conveniently accessible for re-arrangement or exchange. For this purpose the end walls 38, 36 of the casing are arranged as removable lids, and that wall of the cover, which is adjacent to the chain 24^a, 24^b, can be opened on hinge 37. When the order of the bars 5 of the cylinder is to be changed, the disk 33 is removed and lid 38 loosened. Then a pin 35 is removed, which locks the cylinder on the shaft 2, whereupon the cylinder can be pulled out. When the pins 15 of the pin-wheel 12 are to be placed in other positions the nuts 14 and 13 are screwed off, whereupon the end 36 is loosened and the pin-wheel 12 pulled out.

Having now described my invention what I claim is:

1. In an apparatus for enciphering and

deciphering messages the combination of, a casing formed in one of its side walls with a reading off aperture, a rocking member provided with a series of signs visible through said aperture in both positions of said rocking member, a stepwise rotatable cylinder having on its circumference a plurality of axially extending series of signs visible according as the said cylinder is rotated through said aperture the one after other at the one or the other side of the alphabet of said rocking member, a stepwise movable member for arbitrarily operating said rocking member, and means for arbitrarily moving said movable member, substantially as and for the purpose set forth.

2. In an apparatus for enciphering and deciphering messages the combination of, a casing formed in one of its side walls with an elongated reading off aperture, a rocking member in said casing having a series of signs visible through said aperture in both positions of said rocking member, a stepwise rotatable cylinder having on its circumference a plurality of axially extending series of figures displaced in relation to one another and visible according as the said cylinder is rotated through said aperture the one after the other at the one or the other side of the alphabet of said rocking member, means for rotating said cylinder, a stepwise rotatable pin-wheel, a toothed wheel operated by said pin-wheel, a prism rigidly connected to said toothed wheel, and a movable endless chain operated by said prism, the said chain being composed of links of two different shapes, and adapted to operate the said rocking member, substantially as and for the purpose set forth.

3. In a ciphering and deciphering apparatus, a casing having a reading-off aperture, a rocking shutter having a normal series of signs thereon visible at all times through said aperture, a stepwise rotated cylinder, a plurality of series of signs arranged in cipher order on said cylinder and longitudinally thereof, said aperture being of sufficient width to simultaneously expose the shutter and an adjacent cipher series and means to shift said shutter at intervals to one side or the other of said aperture for correlation to a cipher series at such aperture.

4. In a ciphering and deciphering apparatus, a casing having a reading-off aperture, a rocking shutter having a series of characters thereon and visible at all times through said aperture, a stepwise rotated cylinder, a plurality of exchangeable cipher series of characters arranged on said cylinder and extending longitudinally of the cylinder, said aperture being of sufficient width to simultaneously expose said series of characters of the rocking shutter and an adjacent cipher series of characters, mechanism operated with said cylinder to irregularly rock said shutter into one or the other of its two positions, said mechanism including means to permit a change of such irregular movement.

In testimony whereof I have hereunto subscribed my name this 10th day of September 1924.

ARVID GERHARD DAMM.