March 2, 1943. G. GARNIER 2,313,012

ENCIPHERING APPARATUS

Filed Dec. 27, 1938 3 Sheets-Sheet 1

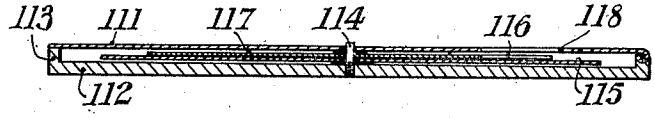


Fig.1

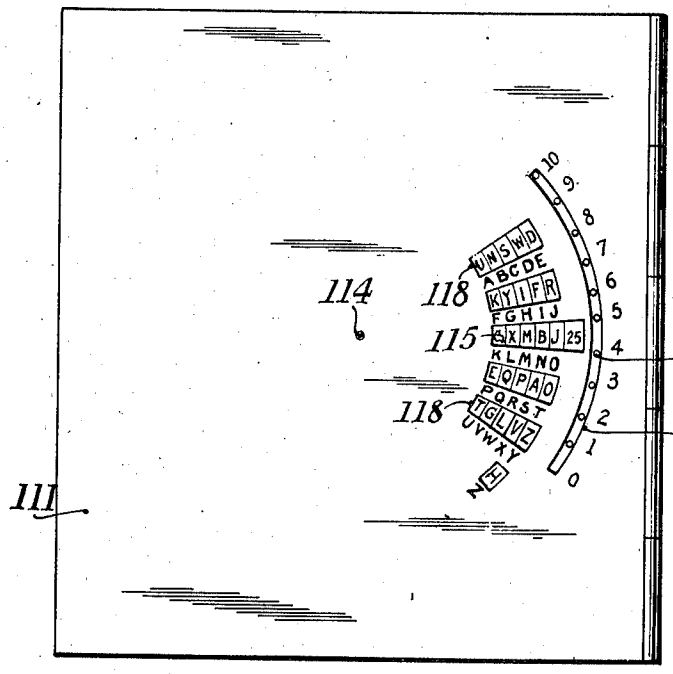


Fig.2

Fig.3

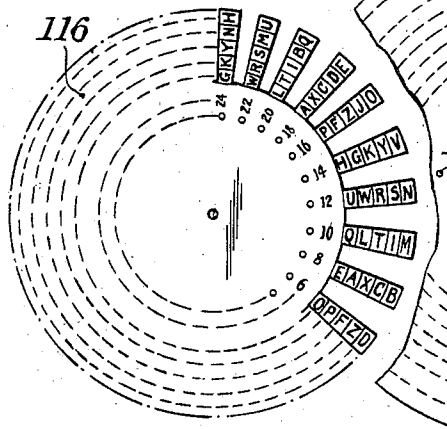
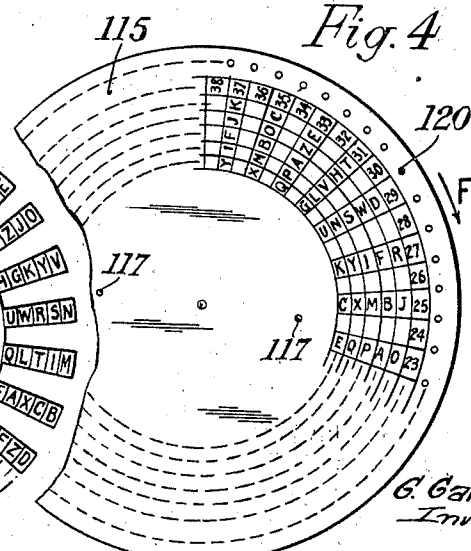


Fig.4



G. Garnier
Inventor

By: Mascock Downing & Seebold
Attys.

March 2, 1943. G. GARNIER 2,313,012

ENCIPHERING APPARATUS

Filed Dec. 27, 1938 3 Sheets-Sheet 2

Fig. 5

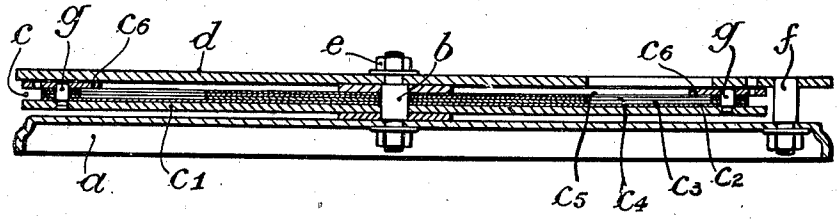
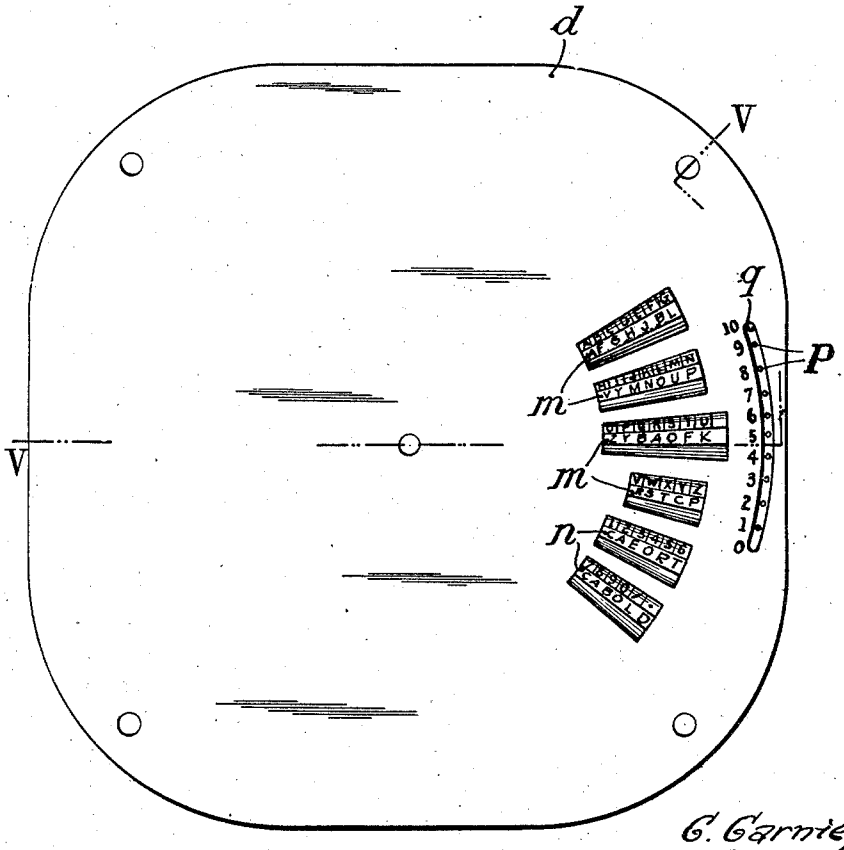


Fig. 6



G. Garnier
Inventor

By: Glascock Downing & Seebold
Attys.

March 2, 1943. G. GARNIER 2,313,012

ENCIPHERING APPARATUS

Filed Dec. 27, 1938 3 Sheets-Sheet 3

Fig. 7

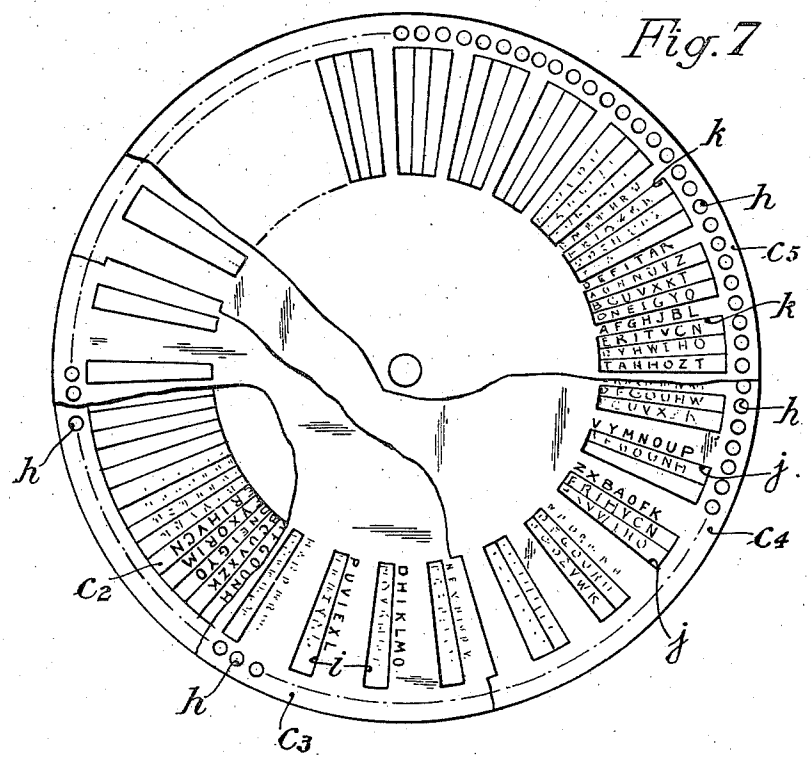
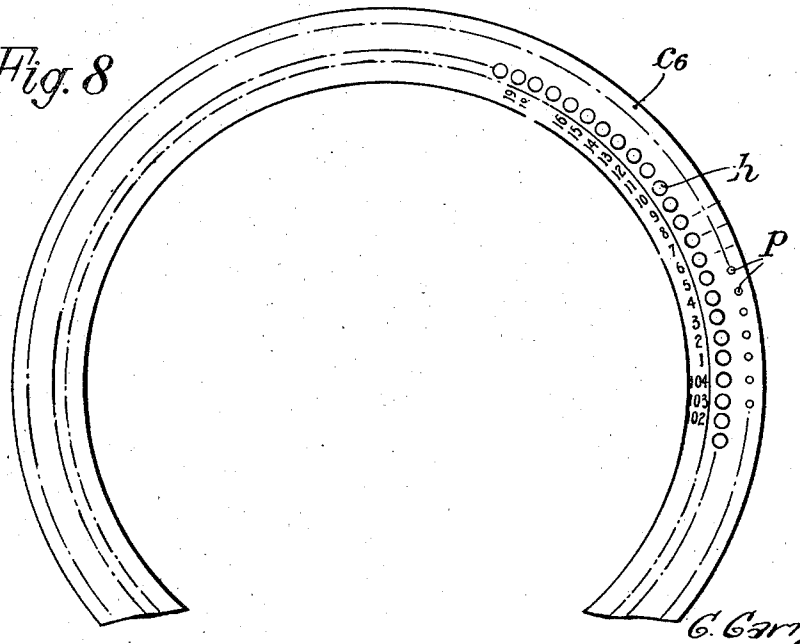


Fig. 8



G. Garnier
Inventor

By: Glascock Downing & Seebold
Attys.

Patented Mar. 2, 1943 2,313,012

UNITED STATES PATENT OFFICE

2,313,012

ENCIPHERING APPARATUS

Gustave Garnier, Paris, France; vested in the Alien Property Custodian

Application December 27, 1938, Serial No. 247,957
In France January 6, 1938

1 Claim. (Cl. 35—2)

The present invention has for object a very simple apparatus allowing to very easily and rapidly translate plain-texts into cipher and, reversely, cryptograms into plain-texts, and this with a number of available combinations so considerable that it is practically impossible for a non-authorized person to decipher them.

This apparatus essentially comprises a disc which is movable about its centre underneath a fixed plate or dial perforated with radial apertures. The letters of the alphabet are inscribed on the edges of said apertures in such an order that it is easy to rapidly find each of them.

On the other hand, the movable disc bears on its entire annular zone capable of appearing at the apertures of the fixed dial, cryptographic characters or signs adapted to be substituted for the letters inscribed on the edge of said apertures, the number of said characters or signs being a multiple of that of the letters of the alphabet, and their positions in said zone being suitably chosen, so that for each position of the disc the characters appearing in the apertures opposite the letters of the alphabet are all different from each other.

Said movable disc is preferably composed of two or more elements which each bear a certain number of the cryptographic characters and the relative positions of which can be changed at will, so that the order according to which all said characters pass in one and the same aperture is variable in view of multiplying the number of available combinations.

The accompanying drawings diagrammatically illustrate and by way of example only, a form of construction of the subject-matter of the invention.

Fig. 1 is a vertical section passing through the centre of the apparatus.

Fig. 2 is a top plan view.

Figs. 3 and 4 illustrate separately the two elements of the movable disc.

Fig. 5 is a section of a modification, made according to line I—I of Fig. 6.

Fig. 6 is a top plan view of this apparatus.

Fig. 7 is a plan view of the movable disc composed of four superposed discs, the three upper discs being partly broken away.

Fig. 8 shows the numbered crown, or ring.

Only a small number of the cryptographic characters have been illustrated in these figures so as not to unnecessarily complicate the drawings.

111 designates a dial supported at a short distance above a base 112, for instance by means of supports 113 or of a circular flange, etc. Between this plate and the base is placed the movable disc pivoting about a pin 114. In this example the disc is composed of two superposed elements: a lower disc 115 and an upper disc 116, which are secured to each other by any attaching means 117 allowing to change at will their relative angular position.

The dial 111 is perforated with a certain number of radial apertures 118 on one edge of which are inscribed the letters of the alphabet, that is to say for instance the twenty-six letters of the English alphabet in their natural order from left to right along the successive apertures: in the drawings, five apertures have been illustrated each bearing five letters and a smaller aperture bearing the twenty-sixth letter (Z). The angular widths of these apertures and those of the solid portions separating them are substantially equal to an amount which will be called "angular pitch."

Concentrically with the row of apertures, a slot 119 in the shape of an arc of circle is provided in the dial 111, and the figures 0 to 9 or 0 to 10 are inscribed on one edge of said slot at intervals or angular pitches which are equal to the width of the apertures 118.

On the movable discs 115 and 116 the cryptographic characters are inscribed on the entire annular zone which, by rotating, passes under the apertures 118; these characters are arranged according to radial rows the spacing apart of which corresponds to the angular pitch previously mentioned, and according to concentric circumferences corresponding to the radial spacing apart of the letters of the alphabet along the apertures. It results therefrom that for each position of the double disc 115, 116, twenty-six cryptographic characters appear opposite the twenty-six letters of the alphabet and express the respective translations for this position.

In the example illustrated, the angular pitch is equal to $\frac{1}{52}$ of circumference, and the disc bears $5 \times 52 = 260$ characters, that is to say the value of ten alphabets.

Each character is repeated thereon ten times, that is to say five times on disc 115 and five times on disc 116.

Figs. 3 and 4 show that the upper disc 116 is cut out on its periphery so as to have twenty-six teeth and twenty-six notches, each of said teeth bearing five characters and each notch allowing five characters inscribed on the disc 115 to be seen.

Attaching means 117 are provided so that each

tooth of disc 116 can be moved and held stationary between any two radial rows of characters of disc 115; the setting of one disc relatively to the other is easy owing to the numbering of the rows of characters on said two discs.

One of the apertures 118 is extended up to above the ring of numbers of disc 115 and allows of marking out the position of the latter relatively to the dial 111.

For causing the double disc 115, 116 to rotate, use can be made of a pencil or of any stylus the point of which is engaged in the slot 119 and in one of the fifty-two holes 120 provided in the periphery of disc 115.

It it is desired to rotate the double disc n number of steps, smaller or equal to 10, in the direction of the arrow F, the point is engaged in the hole 120 located opposite the number n inscribed on the edge of the slot 119 and said point is brought up to the end of the slot marked 0.

Thus can be caused to appear in the apertures 118, every time the movable disc is thus rotated, according to code agreed upon, one of the fifty-two combinations of twenty-six characters corresponding to the fifty-two possible positions of the disc.

As these combinations of twenty-six characters can be changed by displacing the disc 116 on disc 115; the operator has, in reality, at his disposal $52\times26=1352$ cryptographic alphabets for translating the plain alphabet. This number is quadrupled if each elementary disc bears characters on both its faces.

On the other hand, the movable disc can itself be replaced by other similar discs but the characters of which are inscribed in different orders, so that the number of cryptographic alphabets at the disposal of the operator is practically illimited.

The graduated slot 119 is particularly adapted to increase in a considerable proportion the number of changes of combinations utilisable during the translation of one and the same text.

For instance, the various elements of disc 115–116 can be designated according to the successive figures of a number agreed upon beforehand, which can be as long as desired (the decimals of the number π amongst others).

The successive designation of the elements of the disc can also be based on a countersign agreed upon; for instance with the word "Vendôme," V will be designated by 22 steps of the rotating disc, E by 5 steps and N by 14 steps etc.

These two methods of designation are indicated only among an infinite number of others the choice of which can always be modified as the correspondents desire.

The direction of rotation of the disc can itself be conventionally changed, for instance that of the arrow F on odd days, the reverse direction on even days, etc.

It is to be noted that the distribution of the characters on each disc, whether the latter is double as illustrated, or triple, or quadruple, etc. or simple, must always be established in such a manner that all the combinations of twenty-six characters which the disc is capable of presenting under the apertures 118 are different from each other, and that each of them never comprises a repetition of one and the same character, which repetition might prevent the easy deciphering of a secret text.

In the example illustrated, the disc is divided into fifty-two sectors or "steps," but it is to be understood that it can, in a general manner, be divided into n A steps, A being the number of the letters of the alphabet (English or other alphabet) and n any whole number whatever.

In the example illustrated the letters are arranged according to five concentric crowns or rings, but it is to be understood that, without departing from the scope of the invention, the number of said concentric crowns or rings can be varied, the angular pitch of the divisions being independent of this number and remaining equal to $360°/nA$.

For facilitating the changing of the discs, the dial can be hingedly mounted on its supports in any suitable and removable manner, and the discs can be simply threaded on the pivot 114.

In Figs. 5 to 8, a designates a base at the centre of which is secured a vertical pin b serving as a pivot for the movable disc c; above the latter a fixed dial or cover d is secured by a nut e on the pin b and held stationary by tenons f freely engaged in holes formed in said dial.

In this example, the movable disc is composed of a rigid disc c_1 serving as support, of four cryptographic discs c_2 c_3 c_4 c_5 of small thickness, for instance made of brass, and of a rigid crown or ring c_6; these elements are freely superposed and their relative positions are maintained by means of tenons g secured to the disc c_1 and freely engaged in holes h formed in the discs c_2 to c_5 and in the crown or ring c_6.

Each of the thin discs is divided into 104 elementary sectors; on the lower disc c_2 (Fig. 7) are inscribed 104 groups of 7 letters, occupying all the sectors; the disc c_3 is perforated with 26 apertures i uniformly spaced apart each having the width of an elementary sector, and bears groups of 7 letters inscribed either on one edge only of each aperture, or on both edges, or moreover, in the intermediary sectors; the disc c_4 is also perforated with 26 apertures j, but the latter each have the width of 2 elementary sectors, and groups of 7 letters are inscribed on one edge or on both edges of each aperture; the disc c_5 is perforated with 26 apertures k having a width of three elementary sectors and bears a group of 7 letters on each of the sectors separating the apertures.

Finally, in the fixed dial d (Fig 6) are cut out apertures m and n, each of which has a width of one elementary sector and is separated from the next one by a solid portion having a triple width. The edges of these apertures are bevelled in order to facilitate the reading of the cryptographic discs.

The four apertures m, adapted to translate texts, have a total length allowing to read at the same time 26 letters on the movable disc and, in addition, one of the 104 numbers carried by the crown or ring c_6 opposite its 104 reference holes h.

The two apertures n, provided for the translation of figures and conventional signs, have a total length allowing to read on the movable disc a number of letters equal to the number of these figures and signs, for instance 12.

The letters, figures and signs to be translated are engraved on one edge of these different apertures, in their normal order.

In the crown or ring c_6 are perforated, in addition to the holes h, 104 holes p, equally spaced apart on a larger circumference, and serving to operate the movable disc by means of a point or stylus which the operator moves through a slot q in the shape of an arc of circle, provided in the dial d and having a length equal, for instance,

to about 10 elementary sectors. Owing to a graduation numbered on the edge of said slot the movable disc can thus be rotated to the extent of one or more divisions, either in one direction or in the other at will.

It is to be remembered that the choice of the letters inscribed on the discs c_2 c_3 c_4 c_5 must be such that, whatever may be the positions of said discs relatively to each other and to the fixed dial, the letters simultaneously appearing in the apertures m are different from each other; the same will then be true for those simultaneously appearing in the apertures n.

I claim:

An enciphering apparatus comprising the combination of a base, a plate pivotally mounted on said base and having registering projections on its upper face, a plurality of discs superposed on said plate and each having a circular series of apertures adapted to engage over said projections, said discs being provided with a series of uniformly spaced radial slots and bearing a plurality of indicia on one edge of each of said slots, said apertures being provided in a number which is a multiple of the number of said slots, a ring-shaped disc placed above the periphery of said discs and having two concentric series of apertures the spacing apart of which corresponds to that of the apertures of said discs, the apertures of the inner series being adapted to engage over said projections, and a non pivoting cover having a plurality of radial slots and bearing on one edge of each of said slots a plurality of letters of the normal alphabet, said cover also having a slot made according to an arc extending above the outer series of apertures of said ring-shaped disc.

GUSTAVE GARNIER.