RÉPUBLIQUE FRANÇAISE.

OFFICE NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE.

BREVET D'INVENTION.

XVIII. — Articles de bureau, enseignement, vulgarisation. **N° 461.217**

2. — APPAREILS À COPIER, ÉCRIRE ET REPRODUIRE, RELIURE.

Transpositeur à permutations secrètes pour correspondances cryptographiques.

M GEORGES LUGAGNE résidant en France (Bouches-du-Rhône).

Demandé le 23 octobre 1912.

Délivré le 24 octobre 1913. — Publié le 23 décembre 1913.

[Brevet d'invention dont la délivrance a été ajournée en exécution de l'art. 11 § 7 de la loi du 5 juillet 1884 modifiée par la loi du 7 avril 1902.]

La présente invention a pour objet un appareil portatif, pouvant être aisément porté dans la poche, destiné à transformer tout message écrit en langage clair en un message cryptographique et inversement. Le système qui va être décrit assure le secret absolu des correspondances échangées par lettres ou par télégrammes (télégrammes ordinaires ou radiotélégrammes).

Le dessin annexé montre, à titre d'exemple, une forme d'exécution de l'appareil :

La figure 1 en est une vue de face, les réglettes étant dans la position qu'elles occupent lorsque l'appareil n'est pas utilisé;

La figure 2 montre l'appareil avec les réglettes disposées pour une transposition cryptographique;

La figure 3 est une vue par bout.

Comme on le voit sur ces dessins, l'appareil est essentiellement constitué par une planchette-support 1 dans laquelle sont creusées des glissières de forme appropriée; sur le dessin (figure 3), ces glissières ont une section en queue d'aronde, mais elles pourraient évidemment affecter toute autre section convenable. Dans ces glissières se déplacent librement des réglettes 2. Le nombre des rainures (et, par conséquent, celui des réglettes) peut évidemment varier; dans l'exemple représenté, on a prévu dix rainures destinées à recevoir dix réglettes mobiles supérieures et dix réglettes mobiles inférieures. On a choisi ce nombre parce que le télégraphe compte pour un seul mot l'assemblage de dix lettres n'ayant pas de sens apparent mais pouvant être prononcé. Il va sans dire que, si cela présente un intérêt quelconque, on pourra modifier le nombre des réglettes de l'appareil sans s'écarter de l'esprit de l'invention.

Ces réglettes, indépendantes les unes des autres, sont rigoureusement identiques dans leurs dimensions de manière à être parfaitement interchangeables; elles peuvent être introduites indifféremment les unes à la place des autres et dans n'importe quel ordre dans les glissières de la planchette où elles peuvent coulisser à frottement doux.

Les réglettes du jeu supérieur sont numérotées de zéro à neuf; celles du jeu inférieur sont numérotées de la même manière. Sur chaque réglette sont inscrites, les unes au-dessous des autres, mais dans un ordre différent pour chaque réglette, toutes les lettres de l'alphabet.

On remarquera que, lorsque toutes les réglettes sont en place, les numéros inscrits sur chacune d'elles forment un nombre de dix chiffres caractéristique de la position occupée par les réglettes les unes par rapport aux autres. Pour la commodité de la description, on donnera à ces nombres le nom de « MATRICULES ». A chaque disposition des réglettes du jeu supérieur, correspond un matricule supérieur (par exemple, pour la position de la figure 2, 6.978.152.430), de même qu'à chaque position des réglettes inférieures correspond un matricule inférieur (1.407.963.825 pour la figure 2)

Les réglettes de chacun des jeux supérieur et inférieur peuvent être placées, les unes par rapport aux autres, suivant un nombre considérable de dispositions : en effet, le nombre de ces dispositions, obtenues en faisant varier la position des réglettes les unes par rapport aux autres, est donné par la formule connue des permutations dont l'application au cas actuel donne :

$$P_{10} = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 3.628.800$$

Il y a donc 3.628.800 matricules supérieurs et 3.628.800 matricules inférieurs différents.

D'autre part, on peut combiner deux à deux ces matricules; le nombre de ces combinaisons est de :

$$3.628.800^2 = 13.168.189.440.000.$$

Chaque jeu de réglettes est barré transversalement par une plaquette 3, 3' dans laquelle est percée une fenêtre servant, comme il sera expliqué plus loin, pour la formation et la lecture des cryptogrammes. Ces plaquettes 3, 3' sont fixées de toute manière appropriée, sur les bords de la planchette-support 1. Pour la commodité de la description, on donnera à ces plaquettes percées d'une fenêtre le nom de « LECTEUR ».

L'appareil est utilisé de la manière suivante :

Les deux correspondants conviennent de deux matricules, l'un inférieur, l'autre supérieur; par exemple, comme l'indique la figure 2, on adoptera comme matricule supérieur 6.978.152.430 et comme matricule inférieur 1.407.963.825.

Lorsque l'un des correspondants veut adresser à l'autre un message secret, il dispose les réglettes de son appareil comme l'indique la figure 2, c'est-à-dire de manière à former les deux matricules convenus; puis, en faisant coulisser les réglettes dans leurs glissières, il fait apparaître, dans la fenêtre du lecteur supérieur 3, le mot à transmettre, soit, par exemple, le mot « INVIOLABLE », comme sur le dessin.

Les réglettes du jeu inférieur étant en contact avec celles du jeu supérieur, comme sur la figure, l'expéditeur lit, dans la fenêtre du lecteur inférieur 3', le cryptogramme à transmettre, soit « ISLYUCEQZI ». Le destinataire, recevant le message ainsi chiffré, n'a, pour le traduire, qu'à disposer les réglettes de son appareil de la même manière que l'expéditeur (c'est-à-dire de manière à réaliser les deux matricules convenus), puis qu'à faire apparaître, dans la fenêtre du lecteur inférieur 3', les mots donnés par son télégramme; il lira instantanément, en langage clair, dans la fenêtre du lecteur supérieur 3, le message de son correspondant.

On remarquera qu'il suffit de changer le matricule inférieur pour modifier complètement le cryptogramme. Ainsi, dans l'exemple proposé, si, au lieu du matricule inférieur convenu (1.407.963.825), on avait disposé les réglettes inférieures pour former, par exemple, le matricule 5.823.960.174, le cryptogramme du mot « INVIOLABLE » deviendrait « EWFOUCYLVU ».

L'inviolabilité du secret des correspondances ainsi transmises est pratiquement absolu. A moins d'une indiscrétion faisant connaître les matricules convenus, il est hors de doute qu'il sera totalement impossible de déchiffrer une dépêche secrète transmise au moyen de cet appareil, étant donné le nombre considérable de matricules que l'on peut obtenir par les permutations; tous autres matricules que ceux convenus entre deux correspondants donnent des transcriptions inintelligibles.

D'autre part, le système cryptographique résultant de l'application de cet appareil donne lieu à des difficultés de déchiffrage insurmontables tenant, entre autres causes, à ce fait que la même lettre est souvent remplacée, dans les cryptogrammes, par des lettres différentes ou, inversement, que la même lettre, A par exemple, dans le cryptogramme, correspond tantôt à un E, tantôt à un I, tantôt à un U, etc., du message clair.

RÉSUMÉ.

L'invention a pour objet un appareil pour la transformation de tout message écrit en langage clair en un message cryptographique et réciproquement, cet appareil assurant, d'une manière pratiquement absolue, le secret des correspondances échangées. Il est essentiellement caractérisé par ce fait que, dans une planchette-support, sont disposés deux jeux de réglettes, chaque réglette portant toutes les lettres de l'alphabet mais disposées dans un ordre différent d'une réglette à l'autre, le déplacement d'une réglette d'un des jeux provoquant ou permettant le déplacement de la réglette correspondante de l'autre jeu, ce qui permet d'établir la traduction en clair du télégramme chiffré.

D'autre part, toutes ces réglettes sont interchangeables, ce qui permet d'assurer un nombre pratiquement infini de combinaisons cryptographiques.

Enfin, elles peuvent être, une fois la dépêche inscrite ou traduite, ramenées à la position de repos et interchangées, ce qui assure la destruction absolue de toute trace de l'opération faite.

GEORGES LUGAGNE.

Par procuration :

DOM. CASALONGA.

Pour la vente des fascicules, s'adresser à l'IMPRIMERIE NATIONALE, 87, rue Vieille-du-Temple. Paris (3e)

FIG_3_

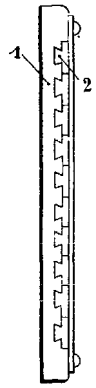


FIG_1_

FIG_2_

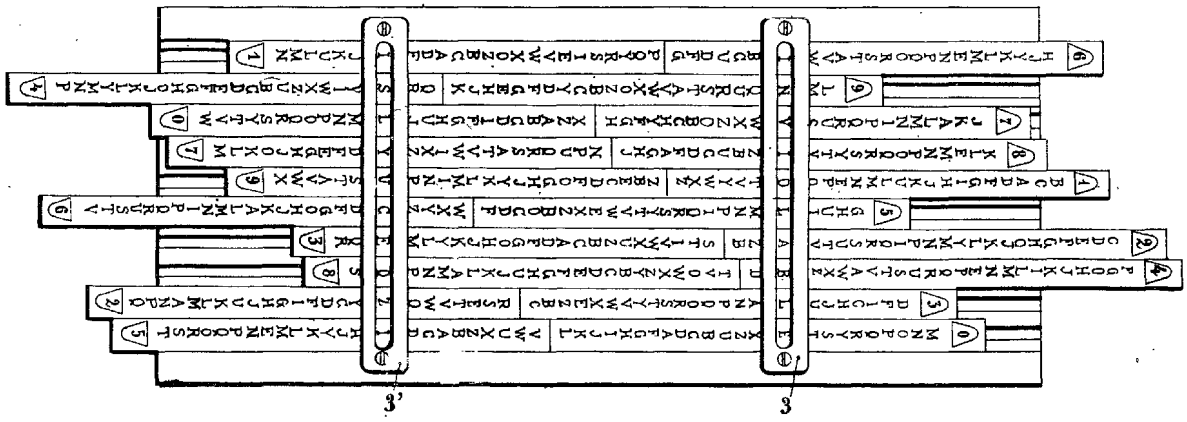


FIG_3_

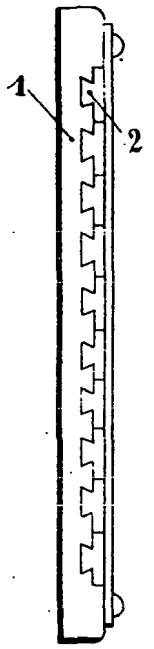


FIG_1_

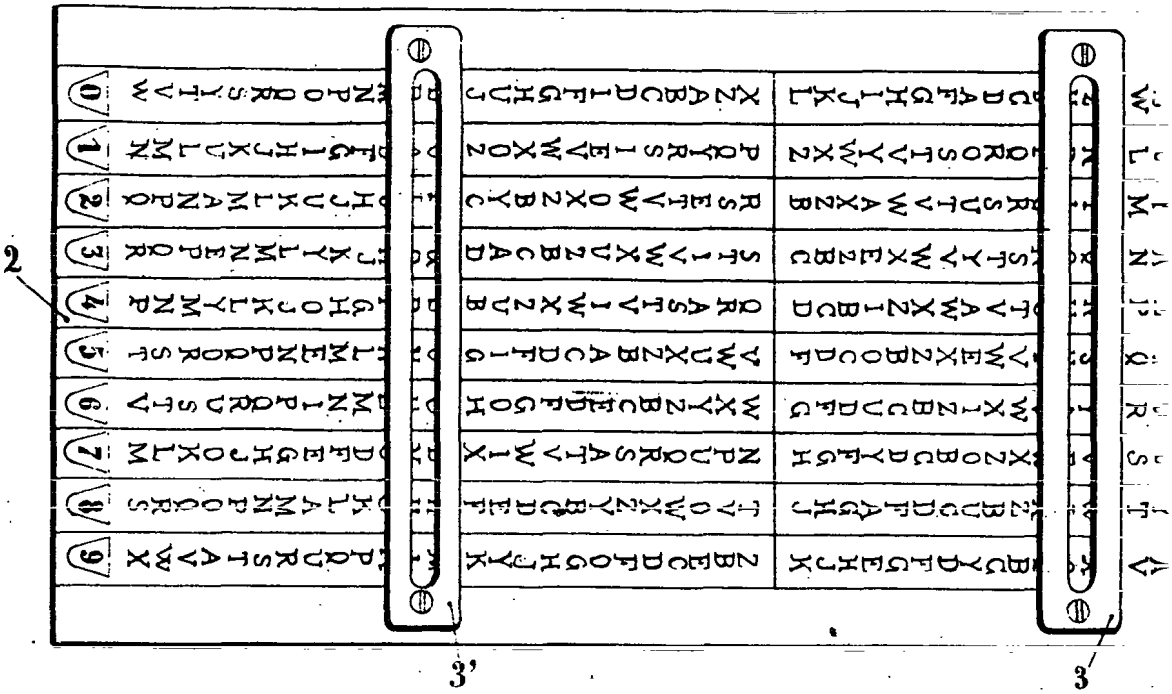
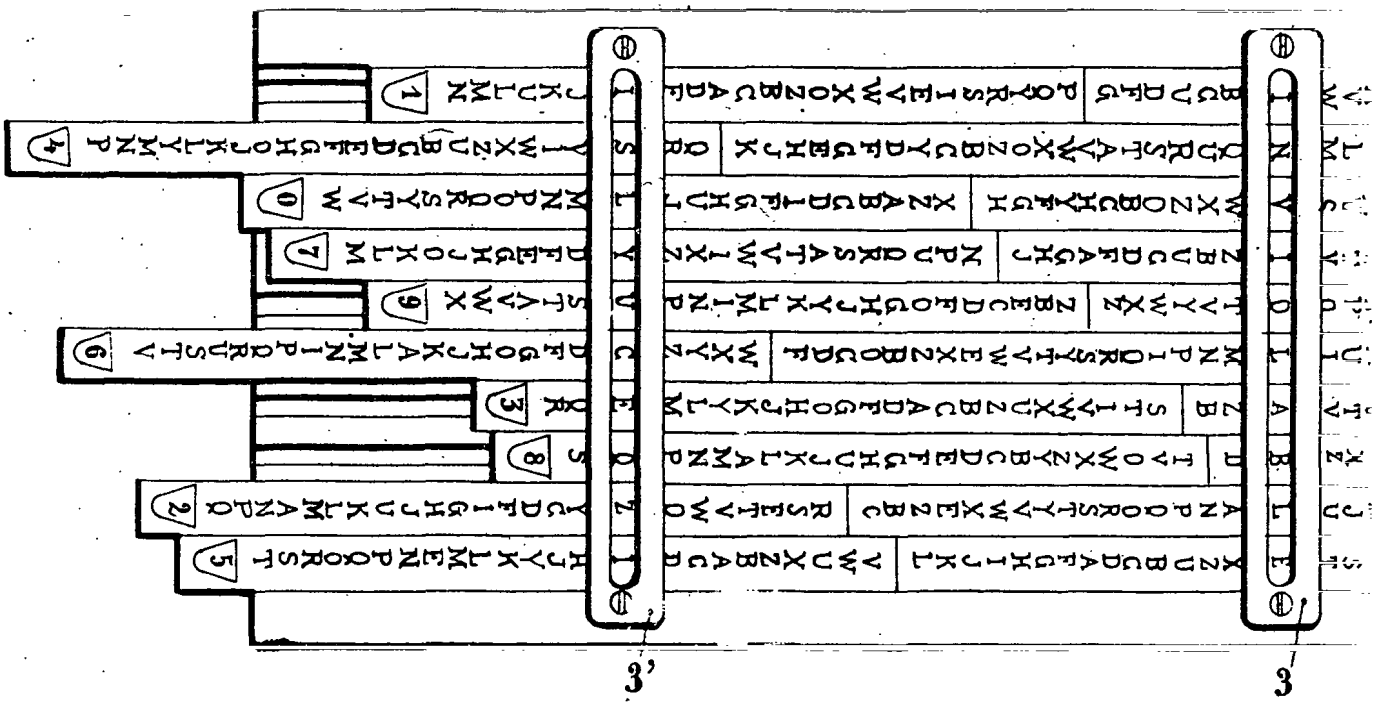


FIG_2_



Pl. unique