RÉPUBLIQUE FRANÇAISE.

MINISTÈRE DU COMMERCE ET DE L'INDUSTRIE.

DIRECTION DE LA PROPRIÉTÉ INDUSTRIELLE.

BREVET D'INVENTION.

Gr. 18. — Cl. 2. **N° 812.481**

Perfectionnements à certains appareils cryptographiques.

M. Albert Antoine Marie GENTET résidant en France (Bouches-du-Rhône).

Demandé le 24 octobre 1936, à 10h 15m, à Marseille.
Délivré le 1er février 1937. — Publié le 11 mai 1937.

On sait qu'actuellement, les appareils cryptographiques à alphabets réellement ou virtuellement mobiles, réalisent d'une façon commode, des substitutions variées de lettres, c'est-à-dire remplaçent toute lettre du texte clair par une autre lettre dite chiffrée, différente de cette lettre claire originale ou pouvant même dans certains cas, lui être identique.

Ces substitutions, employées sans autres précautions, se révèlent inefficaces à protéger contre les indiscrétions, le texte chiffré qu'elles permettent d'établir.

Aussi a-t-on cherché d'interdire tout décryptement intempestif, ou tout au moins de compliquer la tâche des décrypteurs en opérant préalablement à leurs substitution, ou même postérieurement, un brouillage desdites lettres, c'est-à-dire en combinant une transposition des lettres avec leurs substitutions.

Divers moyens ont été réalisés pour obtenir cette transposition, mais au détriment de la rapidité des opérations de chiffrement ou de déchiffrement.

La présente invention concerne un perfectionnement applicable à ces appareils cryptographiques, consistant en une réalisation pratique de cette transposition, utilisable sans complication notable de l'appareil substituteur, apportant un supplément considérable de résistance au décryptement des textes qui en résultent et n'alourdissent relativement pas la durée des opérations.

Ce perfectionnement consiste en :

1° L'adjonction sur l'un ou l'autre des lecteurs qui aident à la compilation des textes clairs ou chiffrés, ou même sur les deux, d'un index mobile pouvant être déplacé sur toute la longueur utile de ce ou de ces lecteurs et pouvant y être immobilisé en certains points ;

2° La création en certains points convenables desdits lecteurs de repères visibles ou autres, au droit desquels pourra être immobilisé l'index mobile ci-dessus.

Fig. 1 montre en plan, un type normal d'appareil substituteur, muni d'un index mobile et de repères-chiffres, sur son lecteur inférieur.

Fig. 2 représente en coupe et perspective, un mode de réalisation de lecteur et d'index mobile.

Fig. 3 représente en perspective, un type d'index.

Dans cette réalisation, l'appareil substituteur normal, est constitué d'un socle 1 (fig. 1) possédant dix jeux de réglettes 2 (fig. 1), dont les divers alphabets qui les ornent, peuvent défiler dans les lumières 3 du lecteur « clair » 4 et du lecteur « chiffrant » 5, par l'action de la rotation des molettes 6 ou 7 qui, par une liaison mécanique quelconque, assurent le déplacement

Prix du fascicule : 6 francs.

des réglettes 2 qui leur correspondent.

Le lecteur chiffrant 5 (fig. 1 et 2) est muni de repères visibles 10 (fig. 1 et 2), qui dans la présente réalisation sont constitués par la suite : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, des chiffres arabes, gravés au droit des intervalles qui séparent l'une de l'autre les réglettes parallèles. En outre, il possède dans les rives de sa lumière centrale 3 (fig. 2) deux rainures 8 dans lesquelles peut coulisser avec un certain frottement, l'index 9 (fig. 1, 2 et 3).

Le fonctionnement de l'index est le suivant :

Après avoir constitué comme à l'ordinaire, une fraction de dix lettres de texte clair dans la fenêtre 3 du lecteur clair 4 (fig. 1) et avant de lire le texte chiffré qui en est résulté dans la fenêtre 3 du lecteur chiffrant 5 (fig. 1), l'opérateur fait occuper à l'index mobile 9 (fig. 1) une certaine position préalablement convenue avec son correspondant, et identifiée par un chiffre, tel par exemple que le chiffre : 4.

Puis il effectue la lecture du texte déjà apparu dans le lecteur chiffrant, non en commençant de l'extrême gauche comme il a déjà été fait pour le texte du lecteur clair, mais par exemple, en débutant à partir de l'index, continuant vers la droite jusqu'à l'extrémité droite du lecteur, et poursuivant ensuite de l'extrémité gauche du lecteur, jusqu'à l'index, c'est-à-dire en lisant de proche en proche et lettre par lettre, le texte chiffré, non dans l'ordre naturel des nombres mais pour l'exemple de la fig. 1 dans l'ordre : 4-5, 5-6, 6-7, 7-8, 8-9, 9-0, 0-1, 1-2, 2-3, et 3-4.

De ce mode de lecture, résulte une discordance convenue, variable et secrète entre l'indice du rang dans le texte clair d'une certaine lettre, et l'indice du rang dans le texte chiffré de la lettre qui lui est conjuguée.

Il est évident, qu'il y a intérêt à faire occuper à cet index mobile, une place différente pour chaque fraction du texte clair en cours de chiffrement.

La loi de déplacement de cet index au cours de l'avance du travail de chiffrement, pourra être aisément établie et retenue dans la mémoire, par l'établissement de toute clé convenable.

Au déchiffrement et pour ce même exemple de réalisation, il suffira de disposer l'index mobile à l'aplomb du chiffre-repère convenu pour la fraction de texte chiffré en cours de traduction, puis de faire apparaître successivement toutes les lettres de cette fraction de texte chiffré, en commençant dès la droite de l'index et poursuivant dans l'ordre défini ci-dessus. Le texte clair se lira dans la fenêtre du lecteur correspondant, de gauche à droite, par fraction entière de texte.

Cette réalisation n'ayant été donnée qu'à titre d'exemple on pourra évidemment recourir au besoin à d'autres modes et à d'autres formes d'exécution, sans changer la nature de cette invention.

On pourra également, selon les circonstances et les applications, varier les détails de construction ou de montage et remplacer divers éléments constitutifs par d'autres jouant le même rôle ou donnant le même résultat.

Il est bien entendu aussi, qu'on pourra utiliser tout procédé, toute matière et tout produit susceptible de servir à la fabrication de ces appareils.

RÉSUMÉ.

Cette invention concerne un perfectionnement aux appareils cryptographiques à alphabets réellement ou virtuellement mobiles, caractérisé par :

Un ou plusieurs index mobiles, pouvant être déplacés sur un ou plusieurs lecteurs et s'y immobiliser en certains points bien repérés, lequel (ou lesquels) index, fixe un point (ou fixent des points) de départ de la lecture d'un texte, différent du point (ou différents des points) de départ de la lecture du texte qui lui est conjugué.

Albert GENTET.

Pour la vente des fascicules, s'adresser à l'Imprimerie Nationale, 27, rue de la Convention. Paris (15e).

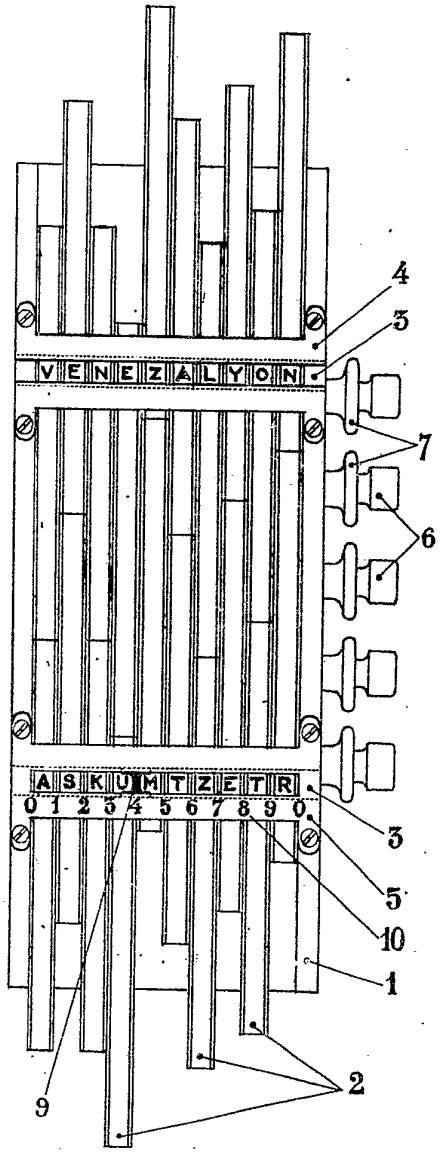

Fig. 1

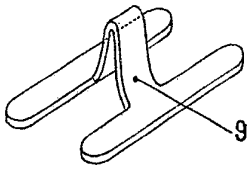

Fig. 3

Fig. 2