RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INDUSTRIE

SERVICE
de la PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION

P.V. n° 906.831 — N° 1.331.129

Classification internationale : G 09 c

Machine cryptographique. (Invention : Per-Erik AHLMAN et Vigo Waldemar LINDSTEIN.)

Société dite : AB TRANSVERTEX résidant en Suède.

Demandé le 13 août 1962, à 15h 25m, à Paris.

Délivré par arrêté du 20 mai 1963.

(*Bulletin officiel de la Propriété industrielle,* n° 26 de 1963.)

L'objet principal de la présente invention est de rationaliser et de simplifier la production des chiffres dans une machine cryptographique, lesquels chiffres sont ordinairement produits plus ou moins manuellement et avec une grande quantité de tableaux et des séries de clefs arrangés d'avance. L'inconvénient de tels systèmes est, entre autres, que les séries de clefs ne peuvent pas être produites sur place en relation avec le chiffrement.

Ces inconvénients sont éliminés par la présente invention sans que la sécurité du chiffre ne soit réduite par rapport aux méthodes précitées. La machine produit dans une forme d'exécution une série de clefs de $26 \times 25 \times 23 \times 21 \times 19 = 5.965.050$ éléments de clefs qui permettent le chiffrement du même nombre de lettres. Comme le chiffrement dépend en dernier lieu d'un choix arbitraire d'un nombre d'alphabets de chiffrement qui peuvent être changés tous les jours, on peut considérer les séries de clefs de deux jours différents comme non analogues.

Une forme d'exécution de l'invention est décrite ci-dessous :

La figure 1 est une vue de la machine d'en haut avec le couvercle partiellement coupé;

La figure 2 est une section verticale de la machine;

La figure 3 est une vue de la machine par derrière et avec le couvercle enlevé;

La figure 4 est une vue de la machine de côté avec le couvercle partiellement coupé pour faire voir un détail du mécanisme d'alimentation;

La figure 5 montre un porte-alphabets agrandi;

La figure 6 montre une bande d'alphabet.

Sur une base 1 sont fixés deux côtés 3 et 4. Entre ces côtés est monté un axe 2, sur lequel peuvent tourner cinq roues à ergots 5, 6, 7, 8 et 9 avec les divisions 19, 21, 23, 25 et 26. Chacune de ces cinq roues à ergots est munie d'une roue dentée respectivement 10, 11, 12, 13 et 14 avec la même division que la roue à ergots en question, lesquelles sont déplaçables par rapport aux roues à ergots (avec un cliquet d'arrêt ou analogue pour le réglage entre elles des roues à ergots avant respectivement le commencement du chiffrement et du déchiffrement).

Les roues à ergots 5-9 sont munies d'ergots 15, qui sont déplaçables axialement soit en position active, soit en position passive.

Sur leur périphérie, les roues à ergots sont munies d'évidements 16, avec des signes (lettres ou chiffres) pour le réglage initial de la clef. Selon leur position axiale, les ergots 15 peuvent agir (ergots actifs) ou ne pas agir (ergots passifs) sur des bras 17 dans le sens inverse de celui des aiguilles d'une montre. Chacun des bras 17 est muni à son extrémité supérieure d'une plaque 18 munie d'un chiffre. La plaque qui appartient à la roue à ergots 5 est marquée d'un 1, la plaque qui appartient à la roue à ergots 6 est marquée d'un 2, etc. On peut lire ces chiffres soit dans une file supérieure de fenêtres 20, soit dans une file inférieure de fenêtres 21 dans un couvercle 19. Les bras 17 peuvent tourner sur un axe 22 et sous l'action des ressorts 48 tendent à tourner dans le sens des aiguilles d'une montre. Chacune des cinq roues dentées 10-14 engrène avec des roues dentées 23-27, fixées sur l'axe 22. Toutes les roues dentées 23-27 ont la même division, d'où il s'ensuit que toutes les roues à ergots sont tournées d'une division quand l'axe 22 est tourné d'un pas de dent. A l'une des extrémités de l'axe 22 (fig. 1) est fixée une roue à cliquet 27′ avec la même division que les roues dentées. Près de cette roue à cliquet se trouve un levier 28, qui peut tourner autour de l'axe 22 et qui est muni d'un cliquet d'alimentation par pas 29, qui est monté sur un tourillon 31. Sous l'action d'un ressort 30, le cliquet 29 est maintenu engrené avec la roue dentée 27′. A chaque enforcement du levier 28, l'axe 22 est alimenté d'une division dans le sens de rotation. (Les butées-limites pour le mouvement du levier 28 et de l'axe 22 ainsi que le ressort de rappel de ces organes ne sont pas montrés). Sur le prolongement de la base 1 en dehors de dispositif pour l'avancement des roues à ergots décrit ci-dessus, se trouvent des porte-alphabets 32 et dans ces porte-alphabets on peut placer des bandes 33 munies des

Prix du fascicule : 2 francs

63 2191 0 73 409 1

alphabets réciproques. Chaque porte-alphabet est marqué d'un ou de deux chiffres 34 (fig. 1). Finalement, un curseur 38 muni d'une fenêtre 39, d'un alphabet ordonné 40 et d'une oreille 41 est déplaçable le long d'un axe 35 fixé avec des plaques 36 et 37.

Le mode d'emploi de la machine est le suivant (tant pour le chiffrement que pour le déchiffrement). La position initiale des roues à ergots selon la convention entre l'émetteur et le récepteur est mise au point manuellement. Dans l'une des deux files de fenêtres 20 ou 21 on lit le plus petit des deux nombres qui s'y montrent (par exemple « 13 » dans la fig. 1, formé par les chiffres « 1 » et « 3 »). On place le curseur dans une position telle que sa fenêtre 39 encadre la bande 33, dont le porte-alphabet est marqué du nombre 13. On cherche la lettre qui sera chiffrée (ou déchiffrée) dans l'alphabet ordonné 40 et on lit la lettre correspondante sur la bande. Ensuite, on presse le levier 29. Chacune des roues à ergots est alimentée d'une division et les plaques 18 occupent de nouvelles positions. On lit le plus petit nombre de la nouvelle position et on place le curseur sur le porte-alphabet correspondant, etc.

Comme le chiffrement et le déchiffrement s'effectuent dans des conditions exactement identiques, on comprend immédiatement le grand avantage du fait qu'on cherche respectivement les lettres du texte en clair et les lettres du chiffre dans un alphabet ordonné.

RÉSUMÉ

Machine cryptographique comprenant un certain nombre de roues à ergots qui, respectivement, lors du chiffrement et du déchiffrement, sont alimentées ensemble de manière que chaque roue soit alimentée d'un ou de plusieurs pas en même temps que les autres. A chaque position des roues à ergots, les ergots en question (un pour chaque roue à ergots) actionnent des bras dont le nombre est égal au nombre des roues à ergots. En outre, les bras coopèrent avec des organes indicateurs qui, selon les positions des ergots, occupent l'une des deux positions et y forment deux combinaisons, l'un des ergots actifs et l'autre des ergots passifs, et desquelles on se sert pour choisir un de plusieurs alphabets désordonnés.

Société dite : AB TRANSVERTEX

Par procuration :
Cabinet CHÉREAU

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

FIG.1

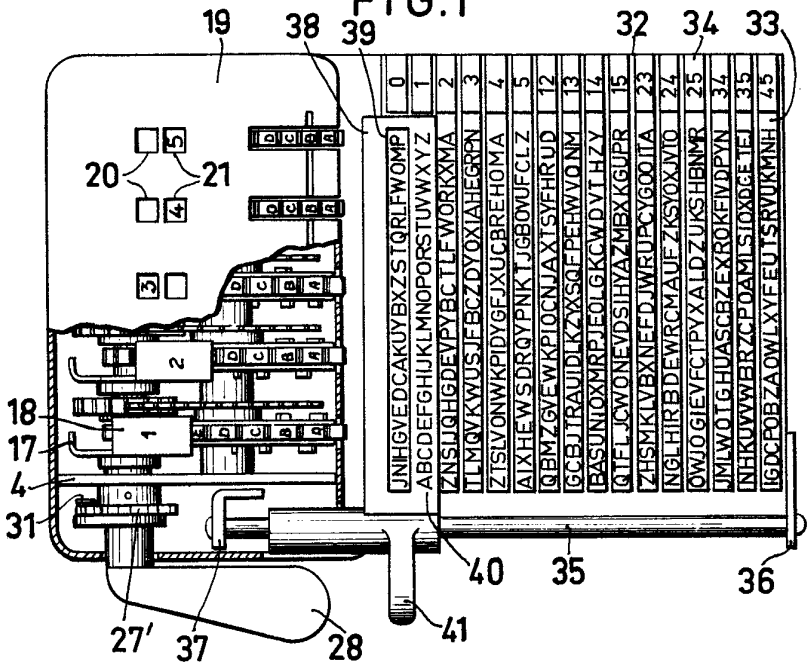

FIG.2

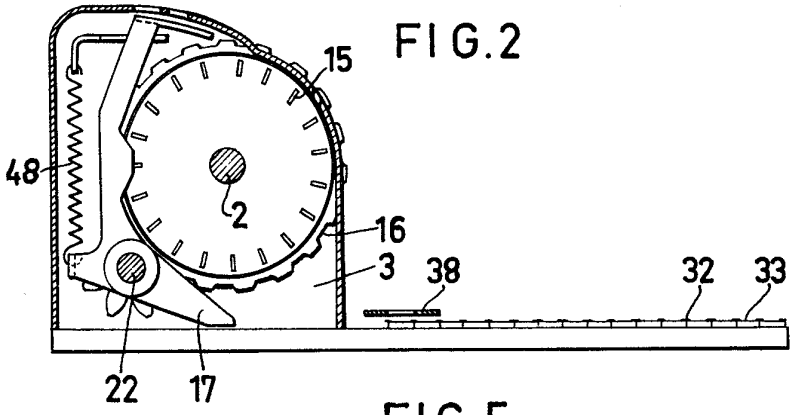

FIG.5

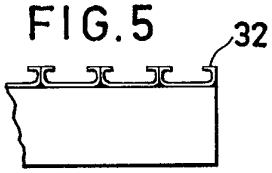

FIG.3

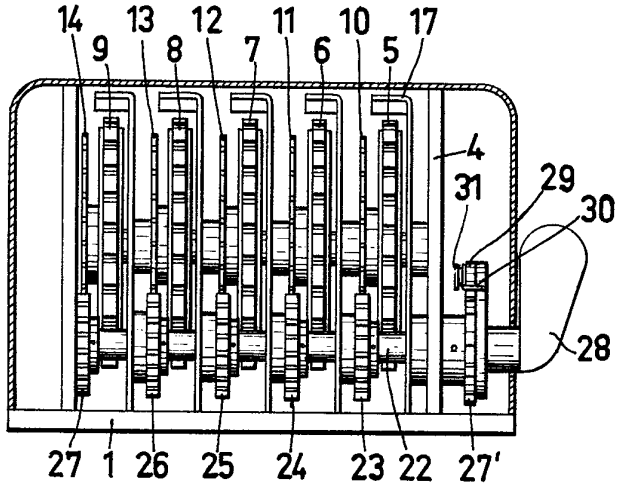

FIG.4

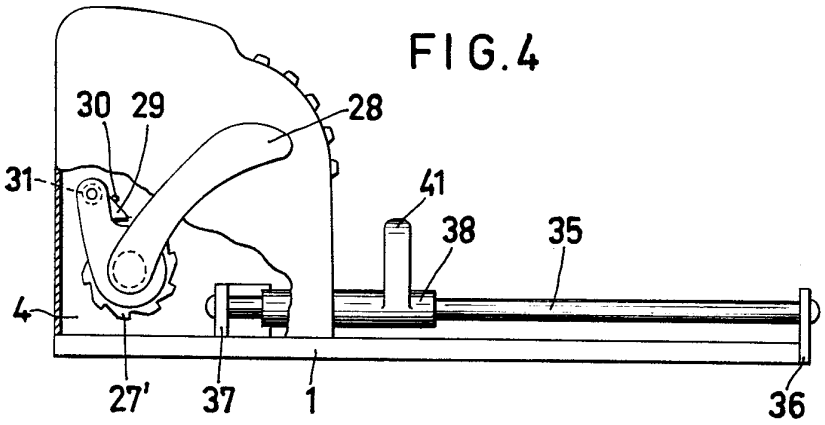

FIG.6