(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2.076.145**
(A n'utiliser que pour le classement et les commandes de reproduction.)

(21) *N° d'enregistrement national :* **71.01322**
(A utiliser pour les paiements d'annuités, les demandes de copies officielles et toutes autres correspondances avec l'I.N.P.I.)

(13) DEMANDE DE BREVET D'INVENTION

1re PUBLICATION

(22) Date de dépôt..... 15 janvier 1971, à 16 h 3 mn.
(41) Date de la mise à la disposition du public de la demande..... B.O.P.I. — «Listes» n. 41 du 15-10-1971.

(51) Classification internationale (Int. Cl.).. G 09 c 1/00.

(71) Déposant : Société dite : AB TRANSVERTEX, résidant en Suède.

Titulaire : *Idem* (71)

(74) Mandataire : Office de brevets Z. Weinstein.

(54) **Appareil de chiffrement.**

(72) Invention de :

(33) (32) (31) Priorité conventionnelle : *Demande de brevet déposée en Suède le 16 janvier 1970, n. 524/1970 au nom de la demanderesse.*

La présente invention concerne généralement et a essentiellement pour objet un dispositif formant appareil de chiffrement, de cryptographie ou analogue et les diverses applications et utilisations résultant de sa mise en oeuvre ainsi que les systèmes, ensembles, mécanismes, machines, équipements et installations pourvus de tels dispositifs.

Un chiffre, formant écriture chiffrée ou cryptographiée ou cryptogramme usuel , a pour but de celer , masquer ou tenir secret le texte en clair qui a été chiffré ou cryptographié. Le texte en clair est accessible seulement à l'opérateur de chiffrement ou de cryptographie et à l'opérateur de déchiffrage ou de décryptage qui possède ou a à sa disposition la clé ou le code du chiffre valable pour le chiffre ou la cryptographie en question. Une personne non autorisée, qui est en possession d'un texte chiffré ou cryptographié ou cryptogramme et qui désire connaître son contenu, doit entrer illégalement en possession soit du texte en clair correspondant au texte chiffré de cryptogramme ou bien de la clé ou du code cryptographique utilisé par l'opérateur de chiffrement, ou bien ladite personne doit reconstituer cette clé à l'aide du chiffre. La reconstitution d'une clé de chiffrement formant code cryptographique est évidemment facilitée à un haut degré si l'on a accès à la fois au chiffre et au texte en clair correspondant à celui-ci.

Dans le cas de la signalisation, communication ou transmission d'un mot de passe, d'ordre, de consigne ou de ralliement, par exemple entre deux stations de radiodiffusion ou d'émission radiophonique, un auditeur non autorisé a accès au chiffre ainsi qu'au texte en clair. Ceci constitue une faiblesse inévitable de chiffres de ce type et par conséquent, la résistance à l'analyse cryptographique du chiffre, c'est-à-dire au déchiffrage ou décryptage, doit être extrêmement élevée. Avec l'appareil conforme à la présente invention, la faiblesse précitée a cependant été compensée par l'utilisation d'une autre propriété fondamentale de chiffres ou de la cryptographie pour la signalisation de mots de passe. Un signal de mot de passe n'a pas besoin d'être déchiffré, décrypté ou transcrit en clair par le récepteur ou destinataire.

L'appareil de chiffrement ou de codage cryptographique conforme à l'invention est caractérisé en ce qu'il comprend au moins deux unités comportant chacune un mécanisme de composition, d'affichage, de réglage, de positionnement ou analogue destiné à effectuer un mouvement pas à pas et une pluralité de compteurs, chaque position d'affichage ou de composition du mécanisme d'affichage étant liée à un compteur, lesdites unités étant reliées entre elles pour former une série sans fin par des moyens transmetteurs entre les compteurs d'une unité et de mécanisme de composition ou d'affichage de l'unité suivante en étant reliés à celui-ci, lesquels moyens transmetteurs, après avoir actionné les mécanismes d'affichage des unités, sont susceptibles de faire accomplir aux mécanismes d'affichage respectifs le nombre de pas ou d'échelons qui est déterminé par le compteur momentanément actif de l'unité précédente suivante de la série. Ainsi des propriétés telles sont conférées à l'appareil que le signal de mot de passe (chiffre) ne peut pas être déchiffré ou décrypté avec cet appareil.

Il est manifeste qu'un chiffre, dont la nature ne permet pas le déchiffrage même avec la connaissance de la clé appliquée, rend extrêmement difficile toute tentative de reconstituer la clé en question.

Avec le système de chiffrement ou de cryptographie de l'appareil décrit dans la suite, le positionnement, affichage ou réglage de composition externe de la clé est déterminé par le texte transcrit en clair, lequel est constitué par le coup d'horloge (le temps, moment ou instant quand le signal de mot de passe est chiffré) et par deux lettres de certains des signaux d'appel des stations communiquant entre elles. Comme l'instant, auquel le signal de mot de passe est produit, est déterminant pour l'apparition, l'apparence ou l'aspect du chiffre, deux ou un plus grand nombre de signaux de mot de passe, échangés entre les mêmes correspondants mais à des instants ou moments différents, diffèrent les uns des autres par leur apparence ou aspect.

On fait avancer irrégulièrement les affichages ou positionnements de composition de l'appareil, de façon que chaque

affichage actionne directement ou indirectement tous les autres affichages, de telle manière que le plus léger changement d'un affichage, pour passer d'un affichage initial à un autre affichage, provoque un changement complet de la position finale de tous les affichages et une variation ou modification correspondante du chiffre.

Exemple	I	II
Texte en clair	AAAA	AAAB
Chiffre	DGYD	KKPB

L'invention sera mieux comprise et d'autres buts, caractéristiques, détails et avantages de celle-ci apparaîtront plus clairement à la lecture de la description explicative qui va suivre en se reportant aux dessins schématiques annexés, donnés uniquement à titre d'exemples illustrant des modes de réalisation de l'invention et dans lesquels:

- la figure 1 représente une vue d'un mode de réalisation purement mécanique de l'appareil de chiffrement;
- la figure 2 montre, suivant une coupe transversale suivant la ligne II-II de la figure 1, comment des loqueteaux, formant cliquet d'arrêt, verrous de blocage ou d'enclenchement dans l'appareil, actionnent une roue pourvue d'un taquet de butée ou d'arrêt ou analogue et comment une roue dans l'appareil est amenée à faire avancer une autre roue;
- la figure 3 représente une vue en perspective d'une roue pourvue de billes;
- la figure 4 représente une vue en coupe transversale suivant la ligne IV-IV de la figure 1; et
- la figure 5 est un schéma du circuit de connexion ou de câblage pour l'appareil fonctionnant électroniquement.

Quatre roues de composition ou d'affichage 19 à 22 et quatre roues de commande 2 à 5 sont montées sur un arbre 32. Sur chacune des roues de composition, qui sont destinées à être placées dans vingt six positions angulaires différentes 40 de division uniforme (figure 3), l'angle $\alpha = 360°$: 26 entre les positions angulaires et un nombre total de vingt six billes 18 est disposé de telle façon suivant six circonférences ou anneaux 41

qu'il y a toujours une bille dans chaque position angulaire. Les billes peuvent être déplacées axialement à l'intérieur de la même position angulaire 40 pour passer d'un anneau ou cercle 41 à un autre anneau ou cercle de la manière désirée.

Les billes dans chaque circonférence ou couronne 41 sont détectées par un loqueteau, cliquet ou verrou analogue 12-17, dont l'autre extrémité coopère avec l'une des roues de commande, dont chacune comprend six portions de distribution ou répartition axiale et chaque portion comprend un taquet de butée ou bossage d'arrêt 6-11. Chaque couronne de billes sur la roue de composition ou d'affichage coopère, par l'intermédiaire d'un loqueteau ou cliquet avec une portion de roue de commande ou menante pourvue d'un taquet d'arrêt. Les cliquets sont montés pivotants sur un arbre 34.

Sur chacune des roues de composition 21 et 22 est montée une couronne de nombres respectivement 24 et 25 pour le nombre ou numéro de temps et une couronne de lettres respectivement 28 et 29 avec un alphabet en désordre. Sur la roue de composition 19 sont prévues deux couronnes de lettres, dont une comprend un alphabet ordonné 26 et l'autre un alphabet en désordre 30. La roue de composition 22 est associée aux couronnes de lettres 27, 31 montées sur l'extrémité de droite de l'arbre 32, lesquelles couronnes de lettres sont reliées de telle façon à la roue de composition 22 par l'intermédiaire des roues dentées 36, 37, de l'arbre 24' et des roues dentées 38, 39 que, lors de la rotation des couronnes de lettres 27, 31, la roue de composition 22 tourne autant que les couronnes de lettres. La couronne de lettres 27 comprend un alphabet ordonné et la couronne de lettres 31 comprend un alphabet en désordre.

Le réglage de composition ou affichage initial est effectué en positionnant les roues de composition 19 et 22 au moyen des alphabets ordonnés 26 et 27 sur le signal de station désiré et les roues de composition 21 et 20 au moyen des couronnes de lettres 24 et 25 sur le nombre ou numéro de temps. Le mot de passe comprend deux groupes de deux chiffres qui sont lus sur les alphabets en désordre 28-31 des roues de composition après un nombre prédéterminé de tours dans le sens de rotation des aiguilles

d'une montre et dans le sens de rotation inverse des aiguilles d'une montre de la poignée 1, formant bouton, manette ou analogue, entre des positions angulaires déterminées par un élément de butée 42 (figure 4) et par un bras 43 sur l'arbre 32.

Les roues de commande 2-5 sont agencées de telle façon sur l'arbre 32 qu'elles suivent la poignée 1 lors de sa rotation dans le sens de rotation des aiguilles d'une montre, en raison du frottement contre l'arbre 32 sur lequel la poignée 1 est montée (la bille 44 étant pressée par un ressort 45 contre l'arbre 32). L'angle, dont la roue 5 par exemple peut tourner pour suivre l'arbre, est déterminé par les bossages d'arrêt ou taquets de butée 6 à 11 par un groupe de loqueteaux ou de cliquets 12 à 17. Les trois roues de commande restantes 2à 4 comprennent des taquets d'arrêt ou bossages de butée correspondants et leurs propres groupes de cliquets. Dans chaque groupe de cliquets, seul un cliquet est actionné par une bille, de telle manière que l'autre extrémité du cliquet pénètre dans le domaine d'action de son taquet de butée ou bossage d'arrêt.

Les roues de composition 19-22 sont agencées de telle façon sur l'arbre 32 qu'elles restent immobiles quand on tourne la poignée 1. L'un des taquets de butée ou bossages d'arrêt sur chacune des quatre roues de commande bute contre quatre des vingt quatre loqueteaux/verrous ou cliquets. Chaque roue de commande est associée à un crochet d'avance 23 agissant contre un disque d'avance 34 qui est divisé en vingt six parties (figure 2) et rigidement relié à une roue de composition. Lors de la rotation d'une roue de commande par l'arbre 32 dans le sens des aiguilles d'une montre, le crochet d'avance 23 suit tout du long et va chercher un nombre égal de pas, d'échelons ou de dents sur le disque d'avance 33 de la roue d'affichage associée. De cette manière, les roues fonctionnent par paires, de sorte que par exemple, le crochet d'avance de la roue de commande 5 coopère avec le disque d'avance de la roue de composition 21. D'autres telles paires de roues sont respectivement les paires 4,20-3,19 et 2,22.

Au cours du pas ou de la phase de fonctionnement suivant,

on fait tourner la poignée 1 dans le sens inverse de rotation des aiguilles d'une montre, ainsi, en raison de la friction contre l'arbre, la roue de commande suit tout le long et le crochet d'avance 23 entraîne la roue de composition sur autant de pas ou d'échelons que les bossages d'arrêt formant taquet de butée ont pu parcourir au cours du pas ou de la phase de fonctionnement précédent avant qu'ils soient arrêtés par les cliquets.

En raison du mouvement d'avancement des roues de composition, quatre nouvelles billes actionnent quatre des vingt quatre cliquets qui se sont avancés dans leur domaine d'action ou dans celui des taquets de butée.

Au tour suivant dans le sens de rotation des aiguilles d'une montre, es cliquets sont détectés et les crochets d'avance 23 vont chercher autant de pas ou d'échelons sur les roues de composition, que les taquets de butée ont dû tourner jusqu'à ce qu'ils rencontrent les cliquets.

Pendant le pas de fonctionnement suivant, la poignée 1 est tournée dans le sens inverse de rotation des aiguilles d'une montre et les roues de composition sont avancées jusqu'à une nouvelle position. Par conséquent, quatre nouvelles billes 18 actionnent les cliquets.

L'appareil est ainsi basé sur le principe consistant en ce que les parties d'avance ou pièces d'entraînement de l'appareil influencent tout le temps les conditions (affichage de la roue de composition) qui sont préjudiciables à l'avance ou l'entraînement pendant le prochain pas de fonctionnement suivant. Pour impartir la même avance irrégulière à toutes les roues, les roues ont été accouplées ensemble à une couronne par l'intermédiaire de l'arbre de transmission 24. La roue de commande 2 fait ainsi avancer la roue de composition 22. Un nombre suffisant de tours de la poignée 1 produit l'effet que les affichages initiaux, effectués par les roues de composition pour chaque échange de mots de passe, actionnent l'avance de toutes les roues de composition.

Les roues de compositions ainsi que les roues de commande, leurs mouvements relatifs et la commande d'entraînement de

l'appareil entier peuvent évidemment être soumis à un système de commande électronique, c'est-à-dire qu'ils peuvent être remplacés par des éléments et connexions électroniques.

Un mode de réalisation de l'appareil actionné électroniquement est représenté sur la figure 5. Dans cet appareil, chaque groupe de roues respectivement 2,19-3,20-4,21 et 5,22 est remplacé respectivement par des unités électroniques 51,61, 71 et 81 de construction relative identique. Chacune des unités comprend un registre de décalage respectivement 52,62,72 et 82, dont chacun est assemblé de manière appropriée à une série de leviers oscillants, culbuteurs ou basculeurs bistables 1-26. A chaque registre de décalage est respectivement associée une rangée de lampes 53, 63, 73 et 83. Le réglage ou affichage primaire du temps et du signal de station est effectué respectivement au moyen d'interrupteurs électriques 54,64,74 et 84. Les registres de décalage, ayant un échelon, étage ou pas connecté à un pôle, sont avancés pas à pas en fermant les interrupteurs respectifs 54,64,74 et 84. Dans les rangées de lampes, commandées par les registres de décalage respectifs, seule une lampe est allumée en raison du registre de décalage connecté au pôle et, en actionnant l'interrupteur respectif, la position allumée peut être déplacée. Du côté gauche de la rangée de lampes 53, il y a des indications de temps et du côté droit, il y a l'alphabet non ordonné. Pour le réglage d'affichage primaire de l'unité 51, la position allumée est avancée pas à pas jusqu'au nombre horaire désiré (qui est 04 dans l'exemple représenté sur la figure 5, c'est-à-dire que la lampe est allumée en 04) par l'interrupteur 54. De la même manière, le réglage d'affichage primaire est effectué avec les registres de décalage restants 62,72 et 82. La rangée de lampes 63 indique des minutes et les rangées de lampes 73 et 83 indiquent ensemble le groupe de deux chiffres pour le signal de station. Après l'achèvement de l'affichage primaire, cet affichage ou composition est à écrire sous forme chiffrée ou cryptographique, ce qui est exécuté en fermant un interrupteur 91 commun à toutes les unités pendant un nombre prédéterminé de fois, lequel, pour l'appareil conforme à la figure 1, correspond à la rotation de la poignée 1 pendant un

nombre défini de fois ou de tours. A chaque fermeture de l'interrupteur 91, les registres de décalage 52, 62, 72 et 82 sont avancés conformément à l'exemple de la figure 5 pendant autant de pas ou d'échelons que cela est indiqué par les compteurs 106, 110, 113 et 120 sélectionnés par les registres de décalage connectés au pôle. Pendant l'avancement des registres de décalage, aucun nouveau compteur ne doit être sélectionné et par conséquent, tous les compteurs sont bloqués lors de la fermeture de l'interrupteur 91. Quand cependant l'interrupteur 91 est ouvert de nouveau, il est possible, pour les registres de décalage connectés au pôle, de choisir de nouveau quatre compteurs, par analogie avec la première rotation ou le premier tour de la poignée, lesquels compteurs, lors de la fermeture suivante de l'interrupteur 91, effectuent l'avancement des registres de décalage 52, 62, 72 et 82. La fonction des compteurs 101-124 correspond, dans l'appareil selon la figure 1, à la fonction des taquets de butée 6-11 formant cliquets d'arrêt ou analogues.

Après avoir pressé l'interrupteur 91 un nombre prédéterminé de fois, les quatre positions allumées respectivement des rangées de lampes 53, 63, 73 et 83 ont été déplacées un certain nombre de pas ou d'échelons et les lettres, dans les alphabets non ordonnés, qui peuvent maintenant être lues au voisinage des positions allumées, représentent le mot de passe.

Bien entendu, l'invention n'est nullement limitée aux modes de réalisation décrits et représentés qui n'ont été donnés qu'à titre d'exemple. En particulier, elle comprend tous les moyens constituant des équivalents techniques des moyens décrits ainsi que leurs combinaisons, si celles-ci sont exécutées selon l'esprit de l'invention.

REVENDICATIONS

1.- Appareil de chiffrement ou de cryptographie en particulier pour la signalisation ou transmission de mots de passe, caractérisé en ce qu'il comprend au moins deux unités dont chacune comporte un mécanisme de composition ou d'affichage destiné à effectuer un mouvement pas à pas et une pluralité de compteurs, chaque position d'affichage ou de composition dudit mécanisme de composition étant liée à un compteur, lesdites unités étant reliées entre elles pour former une série sans fin par des moyens transmetteur entre les compteurs d'une unité et le mécanisme de composition de l'unité suivante, lesdits moyens transmetteurs, après avoir actionné lesdits mécanismes de composition desdites unités, étant susceptibles de faire accomplir, aux mécanismes d'affichage ou de composition respectifs, le nombre de pas ou d'échelons qui est déterminé par le compteur momentanément actif de l'unité précédente suivante de ladite série.

2.- Appareil selon la revendication 1, caractérisé en ce que, pour chaque unité, le mécanisme d'affichage précité est une roue d'affichage pourvue de billes, de chevilles ou d'éléments élévateurs ou souleveurs réglables analogues et destinée à être avancée pas à pas ou par échelons dans le sens de rotation, et les compteurs précités comprennent des taquets d'arrêt ou des organes de butée analogues sur une roue de commande rotative, de telle façon que chaque pas d'affichage de la roue d'affichage est lié, directement ou par l'intermédiaire de loqueteaux ou de verrous analogues à un organe de butée prévus dans l'unité précité, tandis que les moyens transmetteurs précités comprennent des éléments d'entraînement entre ladite roue de commande dans une unité et la roue d'affichage dans une unité suivante, lesdits éléments, inclus dans l'appareil, étant reliés de telle façon les uns aux autres et à une poignée susceptible de tourner dans les deux sens opposés que, lors de la rotation dans un sens, toutes les roues d'affichage sont immobiles et toutes les roues de commande sont tournées d'un angle déterminé par les organes de butée momentanément actifs et que, lors de la rotation dans

le sens opposé, lesdites roues d'affichage sont tournées par lesdits éléments d'entraînement du même angle dont lesdites roues de commande ont été tournées au cours du pas de fonctionnement précédent suivant.

3.- Appareil selon la revendication 1 ou 2, respectivement à quatre mécanismes d'affichage et roues d'affichage, caractérisé en ce que deux respectivement desdits mécanismes d'affichage et roues d'affichage sont liés à une série de nombres à nombres de temps et à une série de lettres à alphabet non ordonné et les deux mécanismes d'affichage et roues d'affichage restants respectivement sont chacun lié à une série de lettres à alphabet ordonné et à une série de lettres à alphabet non ordonné ou désordonné.

4.- Appareil selon la revendication 2 ou 3, caractérisé en ce que toutes les roues précitées sont montées sur un arbre commun et la poignée précitée est en liaison d'entraînement positive avec ledit arbre tandis que les roues de commande précitées sont entraînées par frottement par ledit arbre suivant leurs angles de rotation déterminés par les organes élévateurs ou souleveurs précités des roues d'affichage.

5.- Appareil selon l'une des revendications 2 à 4, caractérisé en ce que les roues précitées sont disposées sur des arbres parallèles uniformément répartis le long d'un cercle et sur chaque arbre sont montées la roue de commande d'une unité précitée et la roue d'affichage d'une unité suivante tandis que l'axe ou l'arbre de la poignée précitée est disposée au centre dudit cercle.

6.- Appareil selon l'une des revendications 2 à 5, caractérisé en ce que les organes d'entraînement précités comprennent un disque d'avance disposé sur les roues d'affichage précitées et un crochet d'avance disposé sur les roues de commande précitées, lequel crochet, lors de la rotation de la poignée précitée dans le premier sens, suit la roue de commande et, sur ledit disque d'avance de la roue d'affichage restant immobile, amène ou va chercher un certain nombre de pas correspondants à la rotation de ladite roue de commande et ensuite lors de la rotation de ladite poignée dans

le sens opposé, entraîne ladite roue d'affichage d'un certain nombre de pas correspondant à la rotation de ladite roue de commande dans le pas suivant ou adjacent de fonctionnement précédent.

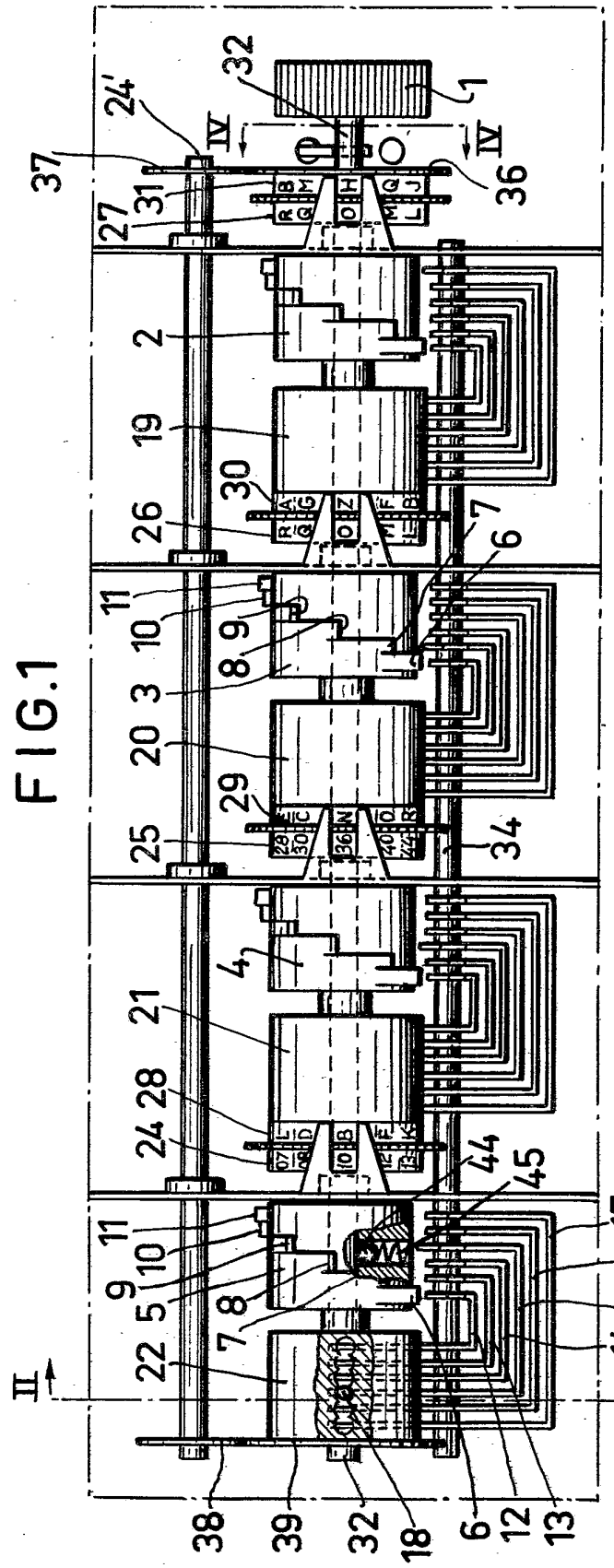
FIG.1
II
II
IV
IV
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
24'
25
26
27
28
29
30
31
32
33
34
36
37
38
39
44
45

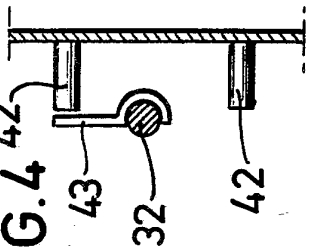
FIG.4
42
43
32
42

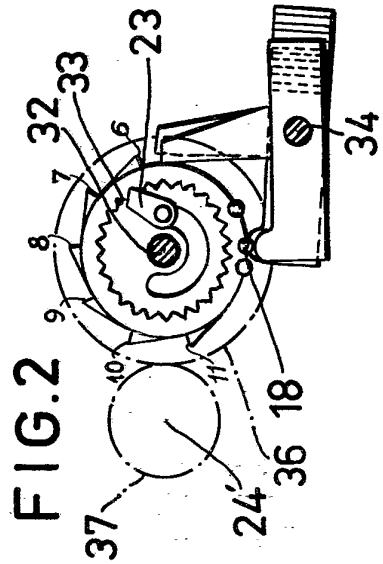
FIG.2
32
33
23
34
6
7
8
9
10
11
18
36
37
24

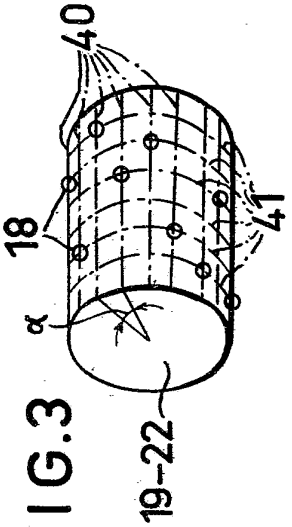
FIG.3
40
18
41
α
19-22

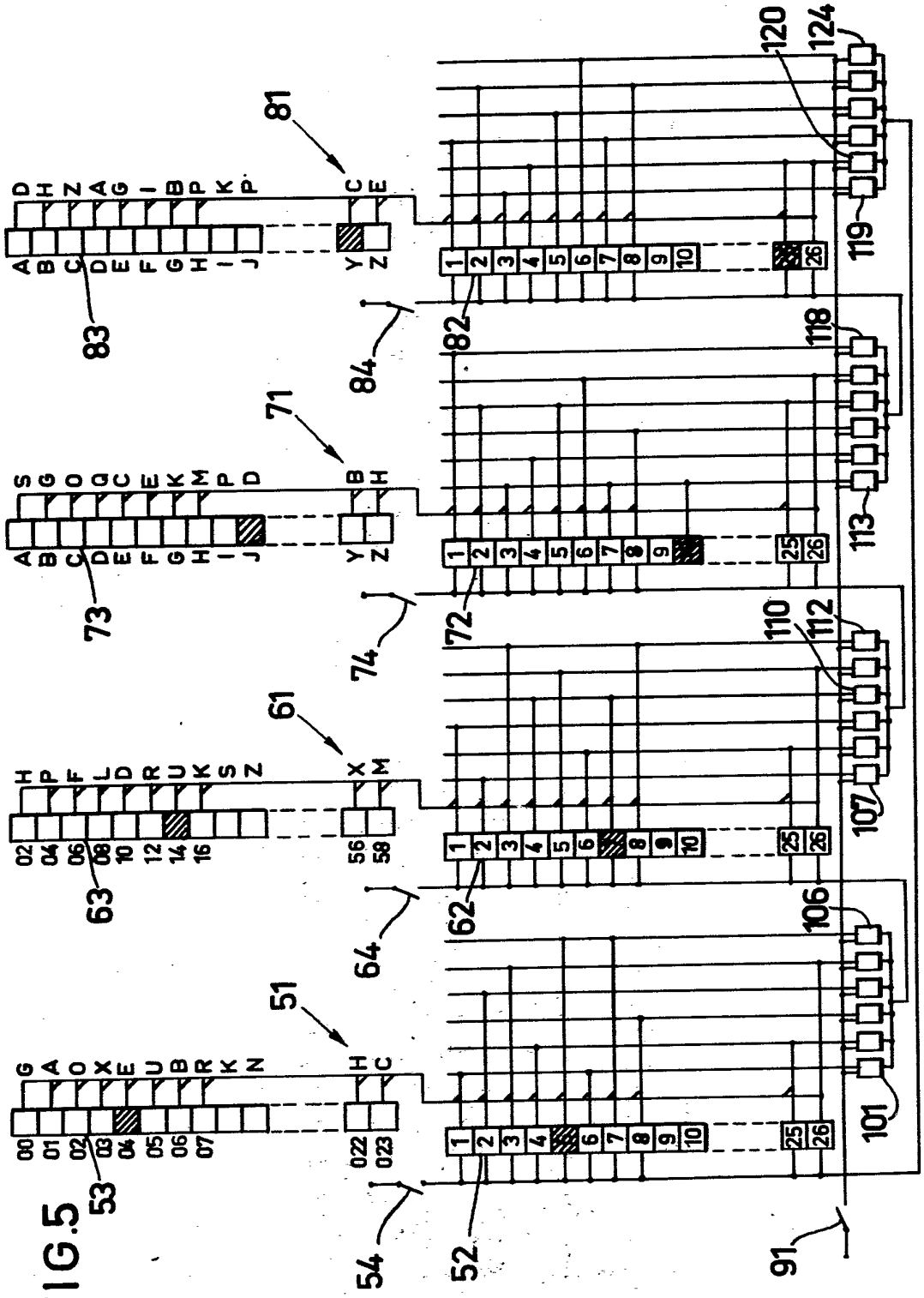
81
83
84
82
71
73
74
72
61
63
64
62
51
53
54
52
91
101
106
107
110
112
113
118
119
120
124

FIG.5