

⑤1

Int. Cl.:

G 09 c, 1/00

BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT



⑤2

Deutsche Kl.:

42 n, 14

⑩

⑪

# Offenlegungsschrift 2 101 834

⑳

Aktenzeichen: P 21 01 834.8

㉑

Anmeldetag: 15. Januar 1971

㉒

Offenlegungstag: 22. Juli 1971

Ausstellungspriorität: —

㉓

Unionspriorität

㉔

Datum: 16. Januar 1970

㉕

Land: Schweden

㉖

Aktenzeichen: 524-70

㉗

Bezeichnung: Chiffriervorrichtung

㉘

Zusatz zu: —

㉙

Ausscheidung aus: —

㉚

Anmelder: AB Transvertex, Norsborg (Schweden)

Vertreter: Sturm, E., Dipl.-Chem. Dr. phil., Patentanwalt, 8000 München

㉛

Als Erfinder benannt: Florin, Bengt, Hägersten (Schweden)

Benachrichtigung gemäß Art. 7 § 1 Abs. 2 Nr. 1 d. Ges. v. 4. 9. 1967 (BGBl. I S. 960): —

DT 2101834

PATENTANWALT  
Dr. ERNST STURM

Deutsche Bank AG. München Kto. Nr. 21/34120  
Postscheckkonto: München 91707

8 MÜNCHEN 23, den 15. 1. 1931  
LEOPOLDSTR. 20/IV  
(Concordiahaus)  
Telefon 396451  
Telegrammanschrift: Isarpatent  
2101834  
11 786 Ho/Mü.

AB T r a n s v e r t e x  
Fittja Industriområde,  
Norsborg / Schweden  
-----

Chiffriervorrichtung

Die Erfindung betrifft eine Chiffriervorrichtung, insbesondere zum Anzeigen von Kennwörtern.

Eine Chiffre üblicher Art dient dazu, den chiffrierten Klartext unleserlich zu machen. Der Klartext ist lediglich dem Chiffrierer und demjenigen Dechiffrierer zugänglich, der über den Schlüssel für die in Frage kommende Chiffre verfügt. Jemand, der unbevollmächtigt in den Besitz des chiffrierten Textes gelangt und dessen Inhalt erfahren möchte, muß sich illegal entweder den zum chiffrierten Text gehörenden Klartext bzw. den vom Chiffrierer verwendeten Schlüssel beschaffen, oder er muß unter Zuhilfenahme der Chiffre den Schlüssel rekonstruieren. Eine Rekonstruktion des Chiffrierschlüssels wird natürlich erheblich vereinfacht, wenn man Zugang sowohl zur Chiffre als auch zum zugehörigen Klartext hat.

Bei Kennwortübermittlungen, beispielsweise zwischen zwei Radiostationen, gelangt ein unbevollmächtigter Zuhörer in den Besitz sowohl der Chiffre als auch des Klartextes. Damit ist eine unvermeidbare Schwachstelle bei der Verwendung von Chiffren dieser Art gegeben, und daher muß der Schwierigkeitsgrad für ein Entziffern der Chiffre extrem hoch liegen.

Der Erfindung liegt nun die Aufgabe zu Grunde, eine Vorrichtung zu schaffen, mit welcher diese Schwachstelle völlig ausgeglichen werden kann. Dabei macht sich die Erfindung eine weitere fundamentale Eigenschaft von Chiffren zur Kennwortübertragung zu nutze. Kennwortsignale müssen nämlich vom Empfänger nicht dechiffriert werden.

Zur Lösung dieser Aufgabe ist die Chiffrier Vorrichtung nach der Erfindung dadurch gekennzeichnet, daß mindestens zwei Einheiten vorgesehen sind, von denen jede einen schrittweise bewegbaren Einstellmechanismus sowie eine Mehrzahl von Zählern aufweist, wobei jede Einstellung des Einstellmechanismus einem Zähler entspricht, und daß die Einheiten von Übertragungsmitteln zwischen den Zählern der einen Einheit und dem Einstellmechanismus der nächstfolgenden Einheit zu einer endlosen Reihe verbunden sind, wobei die Übertragungsmittel nach Betätigung der Einstellmechanismen der Einheiten den jeweiligen Einstellmechanismus diejenige Anzahl von Schritten durchführen lassen können, welche von dem augenblicklich aktiven Zähler der vorhergehenden Einheit der endlosen Reihe bestimmt ist. Auf diese Weise ist die Vorrichtung so ausgebildet, daß sie sich nicht dazu eignet, das Kennwortsignal oder die Chiffre zu dechiffrieren.

Es ergibt sich ohne weiteres, daß bei einer Chiffre, deren Art auch dann nicht ihre Dechiffrierung ermöglicht,

wenn der verwendete Schlüssel bekannt ist, extreme Schwierigkeiten auftreten, wenn man versucht, den in Frage stehenden Schlüssel zu rekonstruieren.

Bei dem Chiffriersystem der Vorrichtung nach der Erfindung wird die äußere Einstellung des Schlüssels vom Klartext bestimmt, der aus einer Zeitangabe (und zwar von der Angabe des Zeitpunkts, in dem die Chiffrierung des Kennwortsignals erfolgt) und aus zwei Buchstaben einiger der Rufsignale der miteinander in Informationsaustausch stehenden Stationen besteht. Da sich der Zeitpunkt, in dem das Kennwortsignal entsteht, auf das Aussehen der Chiffre bestimmend auswirkt, sind zwei oder mehr Kennwortsignale, die zwischen den gleichen Gesprächspartnern, jedoch zu unterschiedlichen Zeitpunkten ausgetauscht werden, in ihrem Aussehen <sup>von</sup> einander verschieden.

Die Einstellungen der Vorrichtung werden unregelmäßig fortgeschaltet, so daß jede Einstellung direkt oder indirekt alle anderen Einstellungen betätigt, und zwar derart, daß eine leichte Abwandlung einer Einstellung gegenüber einer anfänglichen Einstellung eine durchgreifende Änderung der endgültigen Einstellungslagen sowie eine entsprechende Änderung der Chiffre mit sich bringt.

<u>Beispiel</u>	I	II
Klartext	AAAA	AAAB
Chiffre	DGYD	KKPB

Auf der beiliegenden Zeichnung sind Ausführungsbeispiele der Vorrichtung nach der Erfindung dargestellt. Die Zeichnung zeigt in:

Fig. 1 eine lediglich mechanisch arbeitende Ausführungsform einer Chiffriervorrichtung;

Fig. 2 im Schnitt entlang der Linie II-II nach Fig. 1 die Art und Weise, in der Klinken eine mit einer Schaltnocke versehene Rolle betätigen und in der eine Rolle dazu gebracht wird, eine weitere Rolle fortzuschalten;

Fig. 3 eine perspektivische Ansicht einer Rolle, die mit Kugeln versehen ist ;

Fig. 4 einen Schnitt entlang der Linie IV-IV nach Fig. 1;

Fig. 5 einen Schaltplan für eine elektronisch arbeitende Vorrichtung.

Auf einer Welle 32 sind vier Einstellrollen 19 bis 22 und vier Betätigungsrollen 2 bis 5 angeordnet. Jede der Einstellrollen kann in 26 unterschiedliche Winkellagen 40 gemäß Fig. 3 eingestellt werden, wobei der Winkel  $\alpha$  zwischen diesen Winkellagen  $360^\circ : 26$  beträgt. Jede Einstellrolle ist mit 26 Kugeln 18 versehen, die in sechs Ringreihen 41 derart angeordnet sind, daß jeweils eine Kugel zu jeder Winkellage gehört. Die Kugeln können auf der Linie der gleichen Winkellagen 40 in gewünschter Weise in axialer Richtung von einer Ringreihe 41 in eine andere Ringreihe verschoben werden.

Die Kugeln in jeder Ringreihe 41 werden von einer Klinken 12 bis 17 abgetastet, deren anderes Ende <sup>mit</sup> einer der Betätigungsrollen zusammenwirkt. Jede dieser Betätigungsrollen umfaßt sechs axial abgeteilte Abschnitte, und jeder Abschnitt besteht aus einer Schaltnocke 6 bis 11. Jede Ringreihe von Kugeln auf einer Einstellrolle wirkt über eine Klinken mit einem einen Schaltnocken aufweisenden Abschnitt einer Betätigungsrolle zusammen. Die Klinken sitzen schwenkbar auf einer Achse 34.

Jede der Einstellrollen 21 und 20 trägt jeweils einen Ziffernring 24 und 25 für die Zeitziffern sowie jeweils einen Buchstabenring 28 und 29 mit einem ungeordneten

Alphabet. An der Einstellrolle 19 sind zwei Buchstabenringe 25 und 30 angeordnet, von denen der erstere mit einem geordneten Alphabet und der letztere mit einem ungeordneten Alphabet versehen ist. Zur Einstellrolle 22 gehören zwei Buchstabenringe 27 und 31, die rechts auf der Welle 32 sitzen und über Zahnräder 36 und 37, eine Welle 24' sowie Zahnräder 38 und 39 derart mit der Einstellrolle 22 verbunden sind, daß sich letztere bei einer Drehung der Buchstabenringe 27 bis 31 um den gleichen Betrag dreht. Der Buchstabenring 27 trägt ein geordnetes Alphabet, während der Buchstabenring 31 mit einem ungeordneten Alphabet versehen ist.

Die anfängliche Einstellung erfolgt in der Weise, daß man die Einstellrollen 19 und 22 mittels der geordneten Alphabete 26 und 27 mit dem gewünschten Stationssignal in Übereinstimmung bringt und die Einstellrollen 21 und 20 mittels der Ziffernringe 24 und 25 auf die Zeitzahl einstellt. Das Kennwort besteht aus zwei zweistelligen Gruppen, die von den ungeordneten Alphabeten 28 bis 31 der Einstellrollen wiedergegeben werden, nachdem ein Handrad 1 eine vorbestimmte Anzahl von Drehungen im Uhrzeigersinn und gegen den Uhrzeigersinn durchgeführt hat, und zwar zwischen Winkelstellungen, die von einem Anschlag 42 nach Fig. 4 und einem Arm 43 auf der Welle 32 festgelegt sind.

Die Betätigungsrollen 2 bis 5 sind derart auf der Welle 32 angeordnet, daß sie dem Handrad bei seiner Drehung im Uhrzeigersinn folgen, und zwar aufgrund eines Reibschlusses mit der Welle 32, auf welcher das Handrad 1 befestigt ist. Eine Kugel 44 wird von einer Feder 45 gegen die Achse 32 gedrückt. Der Winkelbereich, über den beispielsweise die Betätigungsrolle 5 der Achse folgen kann, wird durch die Schaltnocken 6 bis 11 sowie eine Gruppe von Klinken 12 bis 17

bestimmt. Die drei verbleibenden Betätigungsrollen 2 bis 4 weisen ebenfalls entsprechende Schaltnocken und Gruppen von Klinken auf. In jeder Gruppe der Klinken wird lediglich eine Klinke von einer Kugel betätigt, und zwar derart, daß das andere Ende der Klinke in den Aktionsbereich seiner Schaltnocke eintritt.

Die Einstellrollen 19 bis 22 stehen auf der Welle 32 still, wenn das Handrad 1 gedreht wird. Eine der Schaltnocken an jedem der vier Betätigungsrollen kommt zum Anschlag gegen vier der vierundzwanzig Klinken. Jede Betätigungsrolle ist mit einem Vorschubhaken 23 versehen, der mit einer Vorschubscheibe 33 zusammenwirkt. Letztere ist in 26 Abschnitte gemäß Fig. 2 unterteilt und sitzt fest an einer Einstellrolle. Bei einer Drehung einer Betätigungsrolle unter der Wirkung der Welle 32 im Uhrzeigersinn folgt der Vorschubhaken 23 der Vorschubscheibe der zugehörigen Einstellrolle und überstreicht eine gleiche Anzahl von Stufen. Auf diese Weise wirken die Rollen paarweise zusammen, so daß beispielsweise der Vorschubhaken der Betätigungsrolle 5 mit der Vorschubscheibe der Einstellrolle 21 zusammenarbeitet. Andere derartige Rollenpaare bestehen jeweils aus den Rollen 4, 20 oder 3, 19 und 2, 22.

Beim nächsten Betätigungsschritt wird das Handrad 1 gegen den Uhrzeigersinn gedreht. Dieser Bewegung folgt die Betätigungsrolle aufgrund des Reibschlusses <sup>mit</sup> und der Welle, und der Vorschubhaken 23 nimmt die Einstellrolle um ebenso viele Schritte mit, wie sich die Schaltnocken bei der vorhergegangenen Betätigung bewegen konnten, bevor sie von den Klinken gestoppt wurden.

Aufgrund der Fortschaltbewegung der Einstellrollen betätigen vier neue Kugeln vier der vierundzwanzig Klinken,

welche in ihren Aktionsbereich oder in den der Schalt-  
nocken hineingelangt sind.

Bei einer nachfolgenden Drehung im Uhrzeigersinn werden diese Klinken abgetastet, und die Vorschubhaken 23 überstreichen so viele Stufen auf den Einstellrollen, wie sich die Schaltnocken drehen müssen, bis sie auf die Klinken treffen.

Während des nächsten Betätigungsschritts wird das Handrad gegen den Uhrzeigersinn gedreht, und die Einstellrollen werden in eine neue Lage fortgeschaltet. Dementsprechend betätigen vier neue Kugeln 16 die Klinken.

Die Arbeitsweise der Vorrichtung nach der Erfindung basiert also darauf, daß die Vorschubelemente immer diejenigen Betriebsbedingungen (Einstellung der Einstellrollen) beeinflussen, welche vorbestimmend sind für den Vorschub während des nächstfolgenden Betätigungsschritts. Um sämtlichen Rollen den gleichen unregelmäßigen Vorschub zu erteilen, sind die Rollen mittels der Übertragungswelle 24' zu einem Ring zusammengekoppelt. Dementsprechend schaltet die Betätigungsrolle 2 die Einstellrolle 22 fort. Eine ausreichende Anzahl von Drehungen des Handrades 1 führt dazu, daß die anfänglichen Einstellungen, die mittels der Einstellrollen bei jeder Kennwortänderung vorgenommen werden, den Vorschub sämtlicher Einstellrollen bewirken.

Die Einstellrollen, die Betätigungsrollen, ihre relativen Bewegungen sowie der Antrieb der gesamten Vorrichtung können ohne weiteres einer elektronischen Steuerung unterworfen werden, d.h., sie können von elektronischen Elementen und Kopplungen ersetzt werden.



Eine Ausführungsform einer elektronisch arbeitenden Vorrichtung geht aus Fig. 5 hervor. Bei dieser Vorrichtung sind sämtliche Rollensätze 2, 19 und 3, 20 sowie 4, 21 und 5, 22 durch untereinander identisch ausgebildete elektronische Einheiten 51, 61, 71 und 81 ersetzt. Jede dieser Einheiten besteht aus einem Schaltregister 52, 62, 72 und 82, von denen jedes in geeigneter Weise aus einer Reihe bistabiler Mitnehmer 1 bis 26 zusammengebaut ist. Jedes Schaltregister ist an eine Lampenreihe 53, 63, 73 und 83 angeschlossen. Die anfängliche Einstellung des Zeit- und Stationssignals wird von den Schaltern 54, 64, 74, 84 bewirkt. Die Schaltregister, von denen ein Schritt gepolt ist, werden durch Schließen des jeweiligen Schalters 54, 64, 74 und 84 schrittweise fortgeschaltet. In den vom jeweiligen Schaltregister gesteuerten Lampenreihen leuchtet lediglich eine Lampe auf, und zwar aufgrund des gepolten Schaltregisters, wobei durch Betätigung des jeweiligen Schalters die Lage des erleuchteten Punktes verändert werden kann. Links von der Lampenreihe 53 sind Zeitangaben angeordnet, während sich auf der rechten Seite ein ungeordnetes Alphabet befindet. Bei der Ursprungseinstellung der Einheit 51 wird die Stellung des erleuchteten Punktes schrittweise aufwärts geschaltet bis zur gewünschten Zahlenangabe der Stunde (beim Ausführungsbeispiel nach Fig. 5 handelt es sich dabei um die Zahl 04, d.h., die Lampe bei der Zahl 04 leuchtet auf), und zwar mittels des Schalters 54. In gleicher Weise wird die erste Einstellung der verbleibenden Schaltregister 62, 72 und 82 vorgenommen. Die Lampenreihe 63 zeigt die Minuten an, während die Lampenreihen 73 und 83 gemeinsam eine Anzeige der zweistelligen Gruppen des Stationssignals ergeben. Um anschließend die Anfangseinstellung zu vervollständigen, wird diese Einstellung in Chiffren geschrieben. Hierzu läßt man den allen Einheiten gemeinsamen Schalter 91 eine vorbestimmte Anzahl von Schließ-

vorgängen durchführen. Dies entspricht einer bestimmten Anzahl von Drehungen des Handgriffs 1 bei der Vorrichtung nach Fig. 1. Bei jedem Schließen des Schalters 91 werden die Schaltregister 52, 62, 72 und 82 bei dem Ausführungsbeispiel nach Fig. 5 um so viele Schritte fortgeschaltet, wie es von den durch die gepolten Schaltregister gewählten Zählern 106, 110, 113 und 120 angezeigt wird. Während des Fortschaltvorgangs der Schaltregister müssen keine neuen Zähler ausgewählt werden, und sämtliche Zähler werden daher beim Schließen des Schalters 91 blockiert. Wird jedoch der Schalter 91 wieder geöffnet, so können die gepolten Schaltregister erneut vier Zähler auswählen, und zwar analog zur ersten Drehung des Handrades. Diese Zähler bewirken beim nächsten Schließen des Schalters 91 das Fortschalten der Schaltregister 52, 62, 72 und 82. Die Funktion der Zähler 101 und 124 entspricht der Funktion der Schaltnocken 6 bis 11 bei der Vorrichtung nach Fig. 1.

Wenn der Schalter 91 mit vorbestimmter Häufigkeit gedrückt worden ist, sind die vier erleuchteten Punkte in den Lampenreihen 53, 63, 73 und 83 eine Anzahl von Schritten bewegt worden. Die Buchstaben in den ungeordneten Alphabeten, die nun neben den erleuchteten Punkten abgelesen werden können, geben das Kennwort wieder.

P a t e n t a n s p r ü c h e

1. Chiffriervorrichtung, insbesondere zum Übertragen von Kennwörtern, dadurch gekennzeichnet, daß mindestens zwei Einheiten (2, 19 - 3, 20 - 4, 21 - 5, 22 und 51, 51, 71 und 81) vorgesehen sind, von denen jedes einen schrittweise bewegbaren Einstellmechanismus (19 - 22 und 52, 62, 72, 82) sowie eine Mehrzahl von Zählern (6 - 11 und 101 - 124) aufweist, wobei jede Einstellung des Einstellmechanismus einem Zähler entspricht, und daß die Einheiten von Übertragungsmitteln zwischen den Zählern der einen Einheit und dem Einstellmechanismus der nächstfolgenden Einheit zu einer endlosen Reihe verbunden sind, wobei die Übertragungsmittel nach Betätigung der Einstellmechanismen der Einheiten den jeweiligen Einstellmechanismus diejenige Anzahl von Schritten durchführen lassen können, welche von dem augenblicklich aktiven Zähler der vorhergehenden Einheit der endlosen Reihe bestimmt ist.

2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, daß bei jeder Einheit (2, 19 - 3, 20 - 4, 21 - 5, 22) der Einstellmechanismus eine Einstellrolle (19 - 22) ist, die Kugeln, Stifte oder ähnliche einstellbare Hubelemente (18) aufweist sowie schrittweise in Drehrichtung fortschaltbar ist, und die Zähler an einer umlaufenden Betätigungsrolle (2 - 5) angeordnete Schaltnocken oder ähnliche Anschlagenelemente (6 - 11) aufweisen, daß jeder Einstellschritt der Einstellrolle (19 - 22) direkt oder mittels Klinken (12 - 17) mit einem Anschlagenelement (6 - 11) der Einheit in Beziehung gesetzt wird, und daß/die Übertragungs-  
Übertragungsmittel

elemente (23) zwischen der Betätigungsrolle einer Einheit und der Einstellrolle der nächstfolgenden Einheit umfassen, wobei die Elemente der Vorrichtung derart miteinander und mit einem in beiden Richtungen drehbaren Handrad (1) verbunden sind, daß bei einer Drehung in einer Richtung sämtliche Einstellrollen (19 bis 22) still stehen sowie sämtliche Betätigungsrollen (2-5) über einen Winkelbereich gedreht werden, der von den augenblicklich aktiven Anschlag-elementen (3 - 11) bestimmt ist, und daß bei einer Drehung in entgegengesetzter Richtung die Einstellrollen (19 - 22) von den Übertragungselementen (23) um den gleichen Winkel gedreht werden, um den die Betätigungsrollen (2 - 5) während des vorausgegangenen Betätigungsschritts gedreht worden waren.

3. Vorrichtung nach Anspruch 1 oder 2 mit jeweils vier Einstellmechanismen und Einstellrollen, dadurch gekennzeichnet, daß zwei der Einstellmechanismen und Einstellrollen jeweils mit einer Ziffernreihe (24, 25) für Zeitangaben und einer Buchstabenreihe (28, 29) für ein ungeordnetes Alphabet in Beziehung stehen und daß die beiden verbleibenden Einstellmechanismen und Einstellrollen jeweils eine Buchstabenreihe (26, 27) mit einem geordneten Alphabet und eine Buchstabenreihe (30, 31) mit einem ungeordneten Alphabet aufweisen.

4. Vorrichtung nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß alle Rollen (2 - 5, 19 - 22) auf einer gemeinsamen Welle (32) angeordnet sind, daß das Handrad (1) in direkter Antriebsverbindung mit der Welle (32) steht und daß die Betätigungsrollen von der Welle unter Reibschluß um ihre Winkelbeträge gedreht werden, die von den Hubelementen (18) der Einstellrollen (19 - 22) festgelegt sind.

*R*

5. Vorrichtung nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß die Rollen auf parallelen Wellen gleichmäßig verteilt entlang einer Kreisbahn angeordnet sind und daß jede Welle die Betätigungsrolle einer Einheit und die Einstellrolle einer nächstfolgenden Einheit trägt, wobei die Welle des Handrades (1) im Zentrum der Kreisbahn vorgesehen ist.

6. Vorrichtung nach einem der Ansprüche 2 bis 5, dadurch gekennzeichnet, daß die Übertragungselemente eine Vorschubscheibe (33), die an den Einstellrollen (19 - 22) sitzt, sowie einen an den Betätigungsrollen (2 - 5) angeordneten Vorschubhaken (23) aufweisen, wobei der Vorschubhaken bei einer Drehung des Handrades in der ersten Richtung der Betätigungsrolle (2 - 5) folgt sowie auf der Vorschubscheibe (33) der stillstehenden Einstellrolle eine Anzahl von Schritten überstreicht, die der Drehung der Betätigungsrolle entspricht, und anschließend bei einer Drehung des Handrads (1) in entgegengesetzter Richtung die Einstellrolle (19 - 22) um eine Anzahl von Schritten mitnimmt, welche der Drehung der Betätigungsrolle (2 - 5) während des vorhergegangenen Betätigungsschrittes entspricht.

<sup>13</sup>  
Leerseite

FIG.1

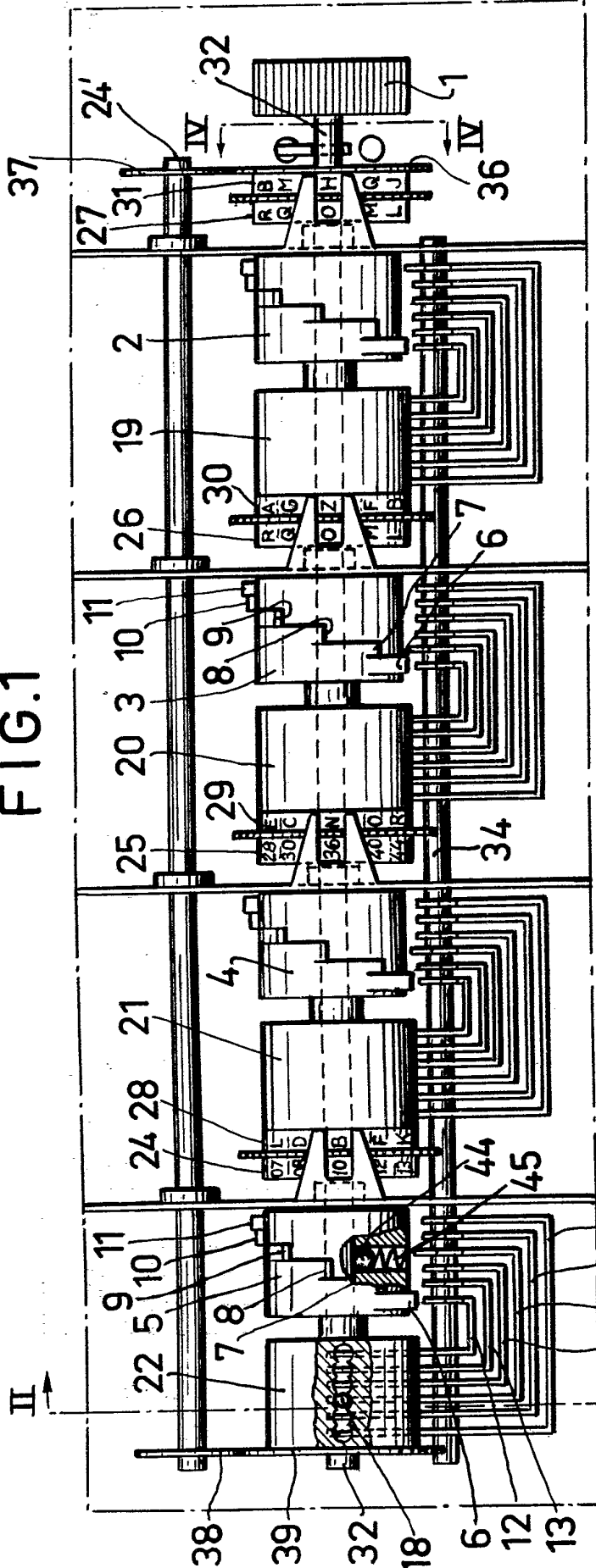


FIG.2

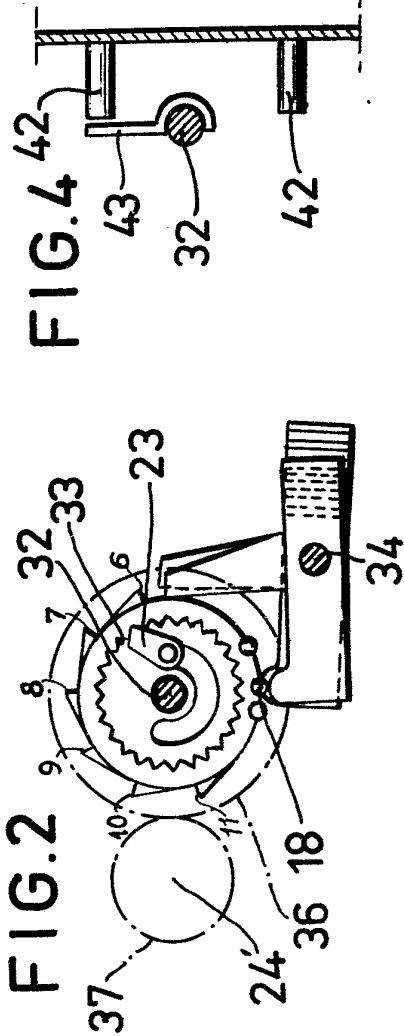
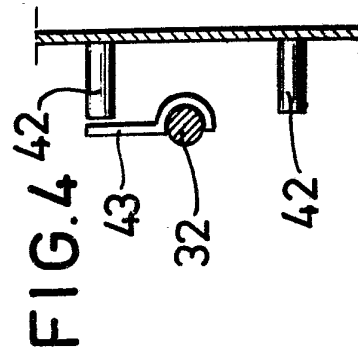
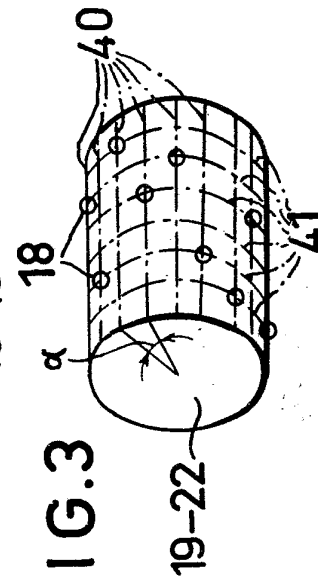


FIG.3



109830/1377

