DEUTSCHES REICH

AUSGEGEBEN AM
20. FEBRUAR 1926

REICHSPATENTAMT

PATENTSCHRIFT

— № 425454 —

KLASSE 42n GRUPPE 14

(A 43119 IX/42n)

Aktiebolaget Cryptograph in Stockholm.

Chiffrierapparat.

Patentiert im Deutschen Reiche vom 27. September 1924 ab.

Für diese Anmeldung ist gemäß dem Unionsvertrage vom 2. Juni 1911 die Priorität auf Grund der Anmeldung in Schweden vom 28. September 1923 beansprucht.

Die Erfindung bezieht sich auf einen Chiffrierapparat, welcher infolge seiner Bauart gegenüber bisher gebauten handlichen Apparaten vergleichbarer Art eine Vereinfachung der mechanischen Einzelheiten und eine dadurch bedingte Ermäßigung der Anfertigungskosten und Abmessungen aufweist und gleichzeitig eine vereinfachte Handhabung, ebenso wie die Herstellung von Chiffrierungen verwickelterer Art und mit längerer Mutationsperiode als bisher zuläßt.

Ein Ausdehnen, soweit praktisch möglich, der Länge der dem Chiffrieren zugrunde liegenden Reihe von verschiedenen Einstellungen der Chiffrierorgane im Verhältnis zueinander, welche Reihe die aufeinanderfolgenden Möglichkeiten der Zeichensubstitutionen im Laufe des Chiffrierens bestimmt und hier wie bei allen mechanischen Apparaten periodisch werden muß, ist von größter Bedeutung für die Chiffresicherheit, welche bekanntlich teilweise von dem Verhältnis zwischen der Periodenlänge der Mutationsreihe und der Länge der Chiffre bzw. des zu chiffrierenden Textes abhängt.

(Mit Mutationsreihe wird hier und in dem Folgenden die Zifferreihe gemeint, deren Glieder die Abstände innerhalb einer gewissen Normalreihe »Alphabet« zwischen den in klarem Text und Chiffre aufeinanderfolgenden entsprechenden Zeichen angeben.)

Außer von dem soeben erwähnten Verhältnis hängt die Chiffresicherheit auch von der durch Erscheinungen in der Chiffre mehr oder weniger hervortretenden Regelmäßigkeit der Mutationsreihe ab. Da bei Anwendung einer Normalreihe mit n Zeichen nur n verschiedene Glieder in der Mutationsreihe eingehen können, müssen mehrere oder weniger derselben in einer Reihe mit einer Periodenlänge von beispielsweise x—n Gliedern zu verschiedenen Malen wiederholt werden. Da es unstreitig eintreten kann und bei fortgesetztem Chiffrieren früher oder später eintreten muß, daß Wiederholungen von Zeichenkombinationen im Text mit Wiederholungen von Kombinationen von Gliedern der Mutationsreihe zusammenfallen, so können die Faktoren und Kongruenzverhältnisse der Wiederholungsintervalle laut in der Kryptologie bekannten Gesetzen Anweisung zu Wahrscheinlichkeitsfolgerungen, betreffend die mathematische Bauart der Mutationsreihe, geben, welche in ihrer Ordnung die Deutung einer Chiffre durch Außenstehende erleichtern können.

Abgesehen von der Ausdehnung der Periodenlänge ist es also bei jedem Chiffrierapparat erwünscht, teils das Entstehen glei-

cher Wiederholungsintervalle und eine gleichförmige Verteilung derselben innerhalb der Mutationsperiode möglichst weit zu verhindern, teils Primzahlintervalle zu ermöglichen ebenso wie solche, deren Primfaktoren nicht dieselben sind wie die derjenigen, welche in den Bewegungsperioden der mechanischen Organe des Apparates eingehen oder die Anordnung der Schlüsselorgane bestimmen.

Der Hauptzweck vorliegender Erfindung ist, diesen Wunsch soweit wie möglich zu erreichen. Ein anderer Zweck ist, einen schnellen und bequemen Austausch der auf den ganzen Chiffrierverlauf einwirkenden Organe und die verschiedene Anordnung und Einstellung dieser Organe im Verhältnis zueinander zu erleichtern.

Die Zeichnung zeigt eine Ausführungsform eines Chiffrierapparates gemäß der Erfindung.

Abb. 1 ist ein Längsschnitt und

Abb. 2 ein Grundriß, teilweise im Schnitt.

Abb. 3 ist ein Querschnitt, der die Antriebsvorrichtung veranschaulicht.

Abb. 4 zeigt die Anordnung der Kette, die infolge ihrer Zusammensetzung einer beliebigen Zahlenreihe entspricht.

In einem Kasten 1 von viereckigem Querschnitt ist eine Achse 2 drehbar gelagert, auf welcher zwei mittels Stangen 4 miteinander fest verbundene kreisförmige Scheiben 3 befestigt sind. An dem Umkreise der Scheiben 3 sind in achsialer Richtung angebrachte Stäbe 5 je an der Außenseite mit einer Zeichen-Normalreihe (einem Alphabet) versehen und auswechselbar befestigt. Das von den Scheiben 3 und den Stäben 5 gebildete Organ wird als »Zylinder« bezeichnet.

Auf der Achse 2 ist ferner ein Schaltrad 6 befestigt, mit dem eine von einer Feder 7 beeinflußte Klinke 8 in Eingriff steht. Diese Klinke wird von dem einen Arm eines zweiarmigen, auf der Achse 2 drehbar gelagerten Hebels 9 getragen, dessen anderer Arm von einer an dem Kasten 1 befestigten Feder 10 beeinflußt wird, welche bestrebt ist, den Hebel 9 in der in Abb. 3 gezeigten Lage zu halten. Das Schaltrad 6 hat eine der Anzahl der Stäbe 5 des »Zylinders« gleiche Anzahl Zähne.

Auf der Achse 2 ist außerdem ein Schaltrad 11 drehbar gelagert, auf dessen Nabe ein Stiftrad 12 befestigt ist, welches von einer Mutter 13 mit Sperrmutter 14 festgehalten wird. In dem Stiftrad 12, welches aus zwei Scheiben zusammengesetzt sein kann, sind in gleicher Entfernung voneinander radiale Ausbohrungen vorgesehen, in welche Stifte 15 eingesetzt werden können.

Das Stiftrad ist mit einem zylindrischen Flansch 16 versehen, auf welchem Zeichen angebracht sind, und zwar eines für jedes Stiftloch im Stiftrad 12, dessen jeweilige Stellung also mittels dieser Zeichen durch eine kleine Öffnung 17 (Abb. 1) im Kasten 1 abgelesen werden kann. Das Schaltrad 11, welches auch von der Klinke 8 beeinflußt wird, hat die gleiche Anzahl Zähne, wie das Stiftrad 12 Stiftlöcher hat, und diese Anzahl ist geringer als die Anzahl der Zähne des Schaltrades 6. Die beiden Zahnanzahlen sind im Verhältnis zueinander und zu den Bewegungen des Hebels 9 so gewählt, daß der Hebel 9 bei voller Herabdrückung aus der in Abb. 3 gezeigten Lage das Schaltrad 6 um zwei Zahnlängen, aber das Schaltrad 11 um nur eine Zahnlänge bewegt. Die Drehung des Hebels 9 nach unten wird dadurch begrenzt, daß die Klinke 8 mit einem Sperrstift 18 in Eingriff gelangt. Die beiden Schalträder 6 und 11 werden mittels einer Sperrfeder 19 in ihren Lagen festgehalten.

Durch die Stifte 15 des Stiftrades 12 wird ein mit Aussparungen für die Stifte 12 versehenes Treibrad 20 beeinflußt, welches auf einem in einem Lager 21 eingesetzten Zapfen 22 drehbar gelagert ist. Auf der Nabe des genannten Treibrades sitzt ein achtseitiges Prisma 23, welches dazu dient, die Bewegungen des Treibrades 20 auf eine Kette zu übertragen, die aus Gelenken 24^a und 24^b von verschiedener Höhe und in Übereinstimmung mit einer beliebigen Zifferreihe geordnet zusammengesetzt ist. Diese Kette läuft um eine verstellbare Leitrolle 25. Jedesmal, wenn ein Stift 15 das Treibrad 20 beeinflußt, wird dieses um $^1/_8$ einer Umdrehung gedreht, wobei die Kette um eine Gelenklänge vorwärts bewegt wird. Gegen die Kette liegt gegenüber dem Prisma 23 eine Rolle 26 an, die auf einem Zapfen am Ende eines Armes 27 gelagert ist. Der Arm 27 ist an dem einen Ende einer Achse 28 befestigt, welche in einem herausstehenden Teil des Lagers 21 gelagert ist. An dem anderen Ende der Achse 28 ist, um 90° gegen den Arm 27 versetzt, ein Arm 29 befestigt, der durch ein Gelenk 30 mit einem auf der Achse 2 drehbar gelagerten Bügel 31 verbunden ist, welcher von einer Feder 32 in solcher Weise beeinflußt wird, daß die Rolle 26 gegen die Kette 24^a, 24^b gedrückt gehalten wird. Wenn die Rolle 26 gegen ein niedriges Gelenk 24^b anliegt, nimmt der Bügel 31 die mit vollen Linien in Abb. 3 gezeichnete Lage ein, während er gezwungen wird, die mit Strichlinien in derselben Abbildung gezeichnete Lage einzunehmen, wenn die Rolle 26 von einem hohen Kettengelenk 24^a beeinflußt wird. In der oberen Wandung des Apparatkastens ist eine längliche Ablesungsöffnung 34 angebracht, deren Größe zwei nebeneinanderliegenden Stäben des »Zylinders« entspricht.

Der Bügel 31 ist im Verhältnis zu dieser Ablesungsöffnung so angeordnet, daß er je nach seiner jeweiligen Lage den einen oder den anderen der gerade unter der Ablesungsöffnung befindlichen Stäbe deckt, und ist an seiner Außenseite mit einem Alphabet (Abb. 2) versehen.

Wenn der jetzt beschriebene Apparat zum Chiffrieren verwendet werden soll, wird der »Zylinder« 3, 5 mittels einer auf der Achse 2 außerhalb des Kastens befindlichen geriffelten Scheibe 33 in eine vorher vereinbarte Lage eingestellt. Je nach Vereinbarung wird vor oder nach ein- oder mehrmaligem Herabdrücken des Hebels 9 der dem ersten Buchstaben des Originaltextes entsprechende Buchstabe des auf dem Bügel 31 befindlichen Alphabetes aufgesucht. Der diesem Buchstaben gegenüberliegende Buchstabe in dem durch die Ablesungsöffnung 34 sichtbaren Zylinderalphabet wird als erstes Zeichen der Chiffre aufgeschrieben. Nachher drückt man den Hebel 9 herab und sucht den dem zweiten Textbuchstaben entsprechenden Buchstaben des Bügelalphabetes auf und verzeichnet den diesem Buchstaben gegenüberstehenden Buchstaben des durch die Ablesungsöffnung sichtbaren Zylinderalphabetes als zweites Chiffrezeichen und wiederholt dann die entsprechende Manipulation für jedes folgende Zeichen des Originaltextes.

Daß ein Dechiffrieren einer mittels des oben beschriebenen Apparates hergestellten Chiffre bewerkstelligt werden kann, geht daraus hervor, daß die verschiedenen Alphabete bei dem Dechiffrieren dieselben relativen Stellungen wie bei dem Chiffrieren nacheinander einnehmen werden.

Ob die Zeichen des Bügelalphabetes und des Zylinderalphabetes in entgegengesetzter Reihenfolge erscheinen, oder ob sie beliebig in paarweise reziproker Ordnung angebracht sind, also nach einem der Typen:

I. a b c d e f g h i j k l m n o p q r s t u v w x y z
II. z y x w v u t s r q p o n m l k j i h g f e d c b a

e d c b a z y x w v u t s r q p o n m l k j i h g f

j i h g f e d c b a z y x w v u t s r q p o n m l k usw.,

oder

I. a b c d e f g h i j k l m n o p q r s t u v w x y z
II. j m k x y g f p l a c i b v z h s w q u t n r d e o p s j w i h l f e c m g k z u a t v b q o r d n z y usw.,

wo I das Bügelalphabet und II die Zylinderalphabete bezeichnen, ist ohne Bedeutung. Die Zeichensubstitutionen können in genau gleicher Weise sowohl beim Chiffrieren als beim Dechiffrieren geschehen.

Sind dagegen die Bügel- und Zylinderalphabete einander regellos ungleich, so müssen, wenn beim Chiffrieren Zeichensubstitutionen von dem Bügel- zu dem Zylinderalphabet gemacht worden sind, die entsprechenden Dechiffrierungssubstitutionen von dem Zylinder- zu dem Bügelalphabet geschehen und umgekehrt.

Um die Wirkungsweise des Apparates hinsichtlich der dem Chiffrieren zugrunde liegenden Mutationsreihe zu erklären, wird im folgenden der Einfachheit halber angenommen, daß sämtliche Zylinderalphabete dem Bügelalphabet gegenüber umgekehrte Reihenfolge aufweisen und gegen die Bewegungsrichtung des Zylinders, gerechnet im Verhältnis zueinander, um einen Schritt verschoben sind.

Bei dem oben beschriebenen Apparat kann selbstverständlich eine beliebige Anzahl Alphabetstäbe verwendet werden, aber aus leicht ersichtlichen Gründen soll eine ungerade Anzahl gewählt werden. Gewisse Stäbe können an beliebigen Stellen ausgelassen oder ohne Alphabete gelassen werden. Wenn dies der Fall ist, kann es bei gewissen Gelegenheiten eintreten, daß die Ablesungsöffnung, abgesehen von dem Bügelalphabet, leer erscheint, wobei der Hebel 9 zwei oder mehrere Male nacheinander heruntergedrückt werden muß, bevor eine Zeichensubstitution stattfinden kann.

Hier wird jetzt z. B. angenommen, daß der Zylinder 29 Stäbe hat und daß die Alphabete 7 und 12 ausgelassen worden sind, so daß bei Stillstand des Bügels 31 und jeweiliger Bewegung des Zylinders um zwei Schritte die Alphabete mit Anfang bei 1 in der folgenden Aufeinanderfolge in der Ablesungsöffnung erscheinen würden:

1, 3, 5, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 2, 4, 6, 8, 10, 14, 16, 18, 20, 22, 24, 26, 28, 1, 3, 5, 9 . . . . . .

und unter den obigen Voraussetzungen eine dieser Zifferreihe gleiche Mutationsreihe ergeben.

Wenn indessen der Bügel 31, dessen Anfangslage die in Abb. 2 mit vollen Linien gezeichnete Lage sein möge, z. B. bei der ersten Zylinderbewegung seine Lage ändert, so wird nicht das Alphabet Nr. 3, sondern statt dessen das Alphabet Nr. 4 in der Öffnung sichtbar. Wenn der Bügel bei der nächsten Manipulation stillsteht, würde folglich das Alphabet Nr. 6 sichtbar werden, während bei Lageänderung des Bügels dies mit dem Alphabet Nr. 5 der Fall sein würde. Die Bewegung des Bügels dient also normal zum Herbeiführen genau derselben Wirkung hinsichtlich der relativen Bewegungen zwischen Bügel- und Zy-

linderalphabet, wie wenn sich der Zylinder abwechselnd zwei, drei oder einen Schritt drehte. Da aber außerdem leere Stäbe im Zylinder eine oder mehrere Extramanipulationen notwendig machen können, und da diese Wirkung der Leerräume nicht konstant, sondern von der zufälligen Lage des Bügels, d. h. von der Zusammensetzung und zufälligen Lage der Kette 24^a, 24^b abhängig ist, welche Lage ihrerseits auf der Anordnung und zufälligen Lage des Stiftrades 16 beruht, so ist ersichtlich, daß bei dem Ausnutzen dieser Verhältnisse eine äußerst komplizierte Alphabetwechselreihe entstehen kann, deren Beschaffenheit sich nicht durch eine allgemein gültige, analytisch verwendbare Formel ausdrücken läßt, weil die gleiche Wirkung auf mehreren verschiedenen Ursachen beruhen kann.

So können z. B. Ablesungen von den Alphabeten Nr. 1 und 5 unmittelbar nacheinander von irgendeiner der untenstehenden Annahmen abhängen:

a) Zylinderbewegung von 1 bis 3, Leerraum bei 3, weitere Bewegung des Zylinders bis 5, wobei die Kette entweder stillstehen oder zwei gleiche Gelenke nacheinander haben kann.

b) Zylinderbewegung von 1 bis 3, wobei die Kette von hohem zu niedrigem Gelenk wechselt, welches Ablesungslage 4 ergibt, Leerraum bei 4, weitere Bewegung des Zylinders bis 5, welche Lage also Ablesungslage wird, weil die Kette wieder von niedrigem zu hohem Gelenk wechselt.

c) Zylinderbewegung von 1 bis 3 mit Ablesungslage 2 infolge Kettenwechsels von niedrigem zu hohem Gelenk, Leerraum bei 2, weitere Bewegung des Zylinders bis 5, welche Lage Ablesungslage wird wegen des Kettenwechsels von hohem zu niedrigem Gelenk.

Daß reine Primzahlintervalle innerhalb einer auf solche Weise erhaltenen Mutationsreihe entstehen können, welche mit der Ablesungsfolge der Alphabete tatsächlich nicht identisch zu sein braucht, weil sie nicht nur von den beliebigen Verschiebungen der Zylinderalphabete im Verhältnis zueinander, sondern auch von deren gegebenenfalls verschiedener Beschaffenheit abhängt, ist ohne ausführlichen Beweis ersichtlich.

Vorausgesetzt, daß der Zylinder eine ungerade Anzahl $2N + 1$ Stäbe enthält, daß die Stiftscheibe für S-Stifte eingerichtet und die Kettengelenkzahl K ist, und daß diese Zahlen keinen Faktor gemeinsam haben, so wird die Periodenlänge $P = (2N + 1)\ S \cdot K$ Manipulationen, und wenn eine gewisse Anzahl Leerräume T im Zylinder vorkommen, wird $P = (2N + 1 - T)\ S \cdot K$ Zeichensubstitutionen, weil Periodizität erst dann entstehen kann, nachdem alle Chiffrierorgane in ihre Ausgangsstellungen im Verhältnis zueinander zurückgekommen sind.

Die Teile in dem obenbeschriebenen Apparat, welche auf die Zusammensetzung der Chiffre einwirken können, sind für Umstellung oder Auswechseln leicht und bequem zugänglich. Zu diesem Zweck sind die Wände 34, 36 des Kastens als abnehmbare Deckel eingerichtet, und die Seite des Kastens neben der Kette 24^a, 24^b ist bei 37 schwenkbar. Wenn die Reihenfolge der Alphabetstäbe im Zylinder geändert werden soll, wird die Scheibe 33 entfernt und die Wand 34 weggenommen. Darauf entfernt man einen Stift 35, welcher den Zylinder auf der Achse 2 festhält, und der Zylinder kann dann herausgenommen werden. Wenn die Stifte 15 des Stiftrades 12 gewechselt werden sollen, werden die Muttern 14 und 13 losgeschraubt, worauf die Wand 36 sich entfernen und das Stiftrad 12 sich herausnehmen läßt.

Patent-Anspruch:

Chiffrierapparat mit mehreren sich in ihrer Lage gegenseitig bestimmenden Organen, von denen eines eine Reihe von Normalzeichenserien trägt und sich bei jedem Chiffriervorgang um einen gewissen Winkel dreht, gekennzeichnet durch die Verbindung von vier Organen, nämlich eines hin und her beweglichen, eine Normalzeichenserie tragenden Organs (31), das in bezug auf ein zweites, eine Reihe von Zeichenserien tragendes und als Zylinder ausgebildetes Organ (3, 5) hinter einer Ablesungsöffnung derart angeordnet ist, daß eine der Serien des Zylinders durch diese Öffnung an der einen oder der anderen Seite des hin und her beweglichen Organs (31) sichtbar ist und die jeweilige Lage dieses ersten Organs (31) durch ein eine beliebige Ziffernreihe darstellendes, schrittweise bewegtes drittes Organ (24^a, 24^b) bestimmt wird, dessen Bewegung durch ein viertes Organ (12, 15) geregelt wird, das gleichfalls nach einer beliebigen Ziffernreihe eingerichtet ist und sich bei jedem Chiffriervorgang um einen gewissen Winkel dreht.

Hierzu 1 Blatt Zeichnungen.

BERLIN. GEDRUCKT IN DER REICHSDRUCKEREI

Zu der Patentschrift **425454**
Kl. 42n Gr. 14

Abb. 1.

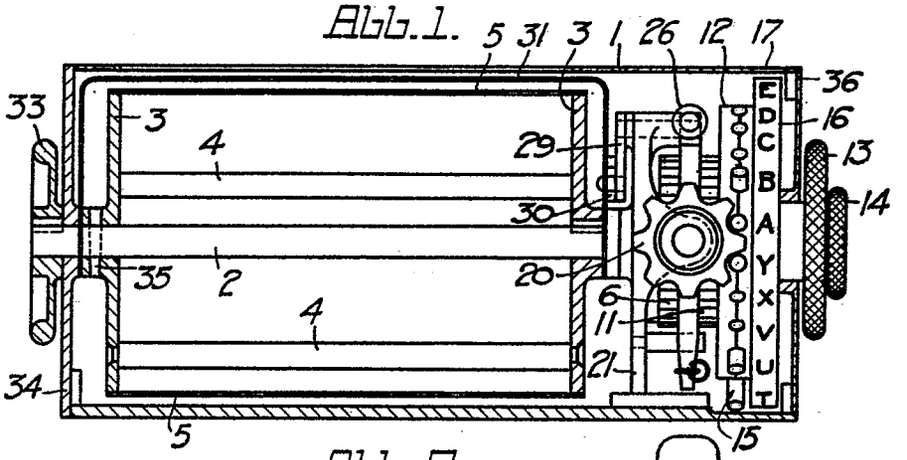

Abb. 2.

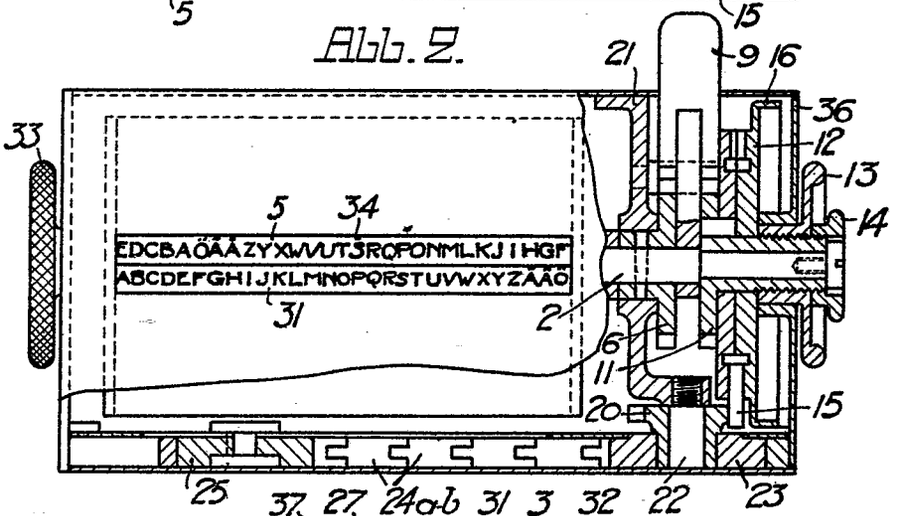

Abb. 3.

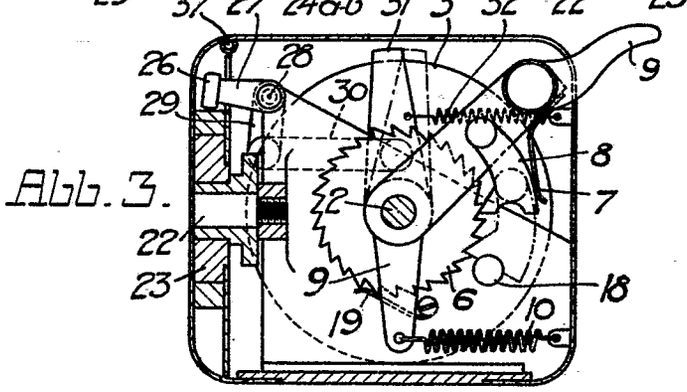

Abb. 4.