**Erteilt auf Grund des inzwischen aufgehobenen § 30 Abs. 5 Pat.-Ges.**

AUSGEGEBEN AM
13. JUNI 1952

REICHSPATENTAMT

# PATENTSCHRIFT

№ 767 351

KLASSE **21 a¹** GRUPPE 21

*L 94819 VIII a/21 a¹*

Nachträglich gedruckt durch das Deutsche Patentamt in München

(§ 20 des Ersten Gesetzes zur Änderung und Überleitung von Vorschriften auf dem Gebiet des gewerblichen Rechtsschutzes vom 8. Juli 1949)

Dr. Gerhard Grimsen, Eßlingen/Neckar

ist als Erfinder genannt worden

C. Lorenz A. G., Stuttgart

## Verfahren zur Verschlüsselung von Nachrichten, die nach dem Prinzip der Telegrafier-Mehrfach-Alphabete übertragen werden

Patentiert im Deutschen Reich vom 21. Mai 1938 an
Patenterteilung bekanntgemacht am 20. März 1952

Es sind Chiffrierverfahren vorgeschlagen, die sich der Prinzipien der modernen Fernschreibtechnik bedienen und bei denen allgemein ein Klartext mit einem Schlüsseltext nach bestimmten Vorschriften gemischt und ausgesandt wird, um auf der Empfangsseite unter richtiger Anwendung desselben Schlüsseltextes wieder Klartext zu erzeugen. Um diesen Schlüsseltext zu speichern, hat man vorgeschlagen, die bekannten Lochstreifengeräte der Fernschreibtechnik zu verwenden, d. h. der Schlüsseltext wird in Form eines Lochstreifens vorbereitet und dieser durch die Abfühlvorrichtung eines automatischen Senders in elektrische Strombilder umgewandelt, die dann mit den elektrischen Strombildern des Klartextes durch weitere Vorrichtungen gemischt werden. Fügt man Anfang und Ende dieses Lochstreifens zu einem endlosen Bande zusammen, so hat man eine Einrichtung eines dauernd wandernden Schlüssels. In diesen bekanntgewordenen Verfahren wird der Mischtext durch zwei Lochstreifen erzeugt. Dieser gewonnene Mischtext wird mit dem Klartext zur Aussendung gebracht.

Im praktischen Betrieb bringt dieses Verfahren jedoch Störungen mit sich, da der Papierstreifen als solcher empfindlich gegen Zerreißen ist und da vor allen Dingen beim Dauerbetrieb des endlosen Schlüsselstreifens die Kombinations- und Transportlöcher durch das häufige Abtasten der Fühlhebel und vor allen Dingen durch den Vorschub des Transporträdchens ausreißen und dadurch Störungen im Vorschub hervorrufen, wodurch der ganze Betrieb gestört wird und der empfangene Text in keiner Weise in Klartext umgewandelt werden kann. Man hat schon vorgeschlagen, an Stelle des Papierstreifens Metallfolie zu verwenden, die zwar den Übelstand des Ausreißens der Transportlöcher vermeidet, aber wegen ihrer mechanischen Steifheit allgemein Schwierigkeiten in der Führung des Streifens mit sich bringt und auf diese Weise zu Transportschwierigkeiten führt, da die Vorschubkräfte natürlich nur in bestimmten Grenzen gehalten werden können und vor allen Dingen die Geschwindigkeit der modernen Apparate (sieben Zeichen je Sekunde) verhältnismäßig hoch ist.

Um diese Nachteile zu vermeiden, werden erfindungsgemäß die in der Geheimtelegrafie für die Verschlüsselung an sich bekannten Speicherwerke (I, II, III, IV) für den Schlüsseltext paarweise (I, II und III, IV) zusammengefaßt und zwei oder mehrere dieser so gewonnenen Zwischenschlüssel zum Hauptschlüssel zusammengefaßt, so daß die Gesamtverschlüsselung also einen kaskadenartigen Aufbau besitzt.

Solche Speicherwerke sind in der Apparatetechnik der modernen Telegrafie bekannt, z. B. als Namengeber. Hier sind auf einem Zylinder die Strombilder eines bestimmten begrenzten Textes durch Einsetzen von Metallstiften gespeichert, die von Kontakthebeln abgefühlt werden. Diese Speicher vermeiden alle Nachteile, die aus der Benutzung des Papierstreifens bzw. Metallbandes herrühren. Sie haben in gewissen Fällen den Nachteil, daß auf einer solchen Trommel nur eine verhältnismäßig geringe Zahl von Buchstaben gespeichert werden kann, wenn diese Trommel nicht große Dimensionen und eine erhebliche Masse annehmen soll, die wiederum eine schnelle schrittweise Bewegung erschwert.

Es wird deshalb vorgeschlagen, solche Trommeln in Mehrfachschaltung zu benutzen, und zwar derart, daß z. B. vier solcher Trommeln vorgesehen sind, deren Speicherzahlen in einem besonderen Verhältnis stehen, das z. B. nach Art des Primzahlensystems gewählt werden kann, um eine möglichst lange Gesamtperiode zu erhalten. Diese vier Trommeln werden gleichzeitig je um einen Schritt vorwärtsbewegt, ihre Stifte werden von Kontakten abgefühlt, je zwei Trommeln bilden mit Hilfe von Mischrelais die erste Mischeinheit, die dann wiederum zu einer übergeordneten Einheit zusammengefaßt werden und endgültig den Schlüsseltext liefern. Auf diese Weise ist es z. B. möglich, unter Verwendung der vier Schlüssellängen von 97, 101, 103 und 107 Schritten eine Gesamtperiode von 107 972 737 zu erreichen, die den Anforderungen der Chiffriersicherheit voll entspricht und mit mechanischen Speicherwerken ohne die Mängel der Lochstreifenspeicher und auf vernünftigem Raume in leicht durchführbarer und einwandfreier Weise hergestellt werden kann.

In der Abbildung sollen die Walzen I bis IV diese mechanischen Speichereinrichtungen für die vier Grundschlüssel darstellen. Diese Steuereinrichtungen werden abgefühlt durch die Kontakte 1 bis 4. Die Schlüssel I und II werden nach dem Rezept zu einem Zwischenschlüssel im Relais *A* gemischt, die Schlüssel III und IV in derselben Weise im Relais *B*. Diese beiden Zwischenschlüssel werden dann zum Hauptschlüssel mit der erwähnten Periode im Relais $a_1$ vereinigt. Bis hierher sind nur die Vorgänge für je einen Impuls der vier Schlüsselbuchstaben dargestellt. Die Zeichnung ist sinngemäß auf fünf solcher bis hier beschriebenen Einrichtungen zu ergänzen. Es resultieren somit die fünf Kontakte der dem Relais $a_1$ entsprechenden Relais $a_1$ bis $a_5$. Diese werden mit den Abfühlkontakten eines automatischen Senders V verbunden und durch den Sendeverteiler VI zur Aussendung bereit gehalten. Auch hier sind nur die Stromläufe für den ersten Impuls des Fünferzeichens dargestellt. Beim Senden wird der Abfühlvorrichtung V der Klartextlochstreifen zugeführt, und der Bürstenarm des Senders VI liegt über ein Relais an der Fernleitung. Im Empfangszustand erhält die Abfühlvorrichtung den verschlüsselten Empfangstext, der mit Hilfe eines Empfangslochers wieder in Form des Lochstreifens gebracht wird, und der Bürstenraum des Senders VI steuert über ein Relais den Empfangsmagneten des Ortsfernschreibers, indem dann der Klartext niedergeschrieben wird. Der Vorschub der Grundschlüsselspeicher I bis IV, die Bewegung der Abtastvorrichtung V und die Kupplungsvorgänge des Senders VI sind in nicht dargestellter Weise zwangsläufig miteinander verbunden.

## Patentansprüche:

1. Verfahren zur Verschlüsselung von Nachrichten, die nach dem Prinzip der Telegrafier-Mehrfach-Alphabete übertragen werden und durch einen Hauptschlüssel verschlüsselt werden, welcher

seinerseits aus zwei Zwischenschlüsseln zusammengesetzt ist, dadurch gekennzeichnet, daß die in der Geheimtelegrafie für die Verschlüsselung an sich bekannten Speicherwerke (I, II, III, IV) für den Schlüsseltext paarweise (I, II und III, IV) zusammengefaßt werden und daß zwei oder mehrere dieser so gewonnenen Zwischenschlüssel zum Hauptschlüssel zusammengefaßt werden, die Gesamtverschlüsselung also einen kaskadenartigen Aufbau besitzt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Schlüssellängen in an sich bekannter Weise Primzahlwerte besitzen.

3. Verfahren nach Anspruch 1 und 2, dadurch gekennzeichnet, daß die Bewegung der Abtastvorrichtung und die Kupplungsvorgänge des Senders zwangsläufig miteinander gekuppelt sind.

4. Verfahren nach Anspruch 1 bis 3, dadurch gekennzeichnet, daß die Schlüssel auf einem Zylinder durch Einsetzen von Metallstiften gespeichert sind.

---

Zur Abgrenzung des Erfindungsgegenstands vom Stand der Technik sind im Erteilungsverfahren folgende Druckschriften in Betracht gezogen worden:

Deutsche Patentschriften Nr. 554 421, 603 261, 579 555, 425 454;
österreichische Patentschriften Nr. 91 059, 92 163, 130 851.

---

Hierzu 1 Blatt Zeichnungen

5211 6.52

Zu der Patentschrift **767 351**
Kl. **21 a¹** Gr. **21**