Nr. 312238

Nr. 312238

SCHWEIZERISCHE EIDGENOSSENSCHAFT

EIDGENÖSSISCHES AMT FÜR GEISTIGES EIGENTUM

PATENTSCHRIFT

Veröffentlicht am 29. Februar 1956

Klasse 52

Gesuch eingereicht: 16. Januar 1953, 17½ Uhr. — Patent eingetragen: 31. Dezember 1955.

HAUPTPATENT

Boris Caesar Wilhelm Hagelin, Zug (Schweiz).

Schaltungsvorrichtung für Verschlüsselungsgeräte.

In Verschlüsselungsgeräten, die zur Herstellung einer normalen Geheimschrift in gedruckter Form dienen, kommt für gewöhnlich nur die Wiedergabe der 26 Buchstaben des internationalen Telegraphenalphabetes in Betracht. Bei der Telegraphierverschlüsselung in Fernschreibverbindungen aber wurde bisher ein System vorwiegend benutzt, das die Verschlüsselung sämtlicher 32 Zeichenkombinationen des Fernschreiberalphabetes erfordert, aber nichtsdestoweniger wegen seiner Einfachheit (Stromschrittinversion) dominiert hat. Dieses System weist aber gewisse Nachteile auf:

Erstens kann die Geheimschrift auf dem Fernschreiber nicht in gedruckter Form dargestellt werden, da ja die Buchstabenreihe des Fernschreibers nur 26 Schriftzeichen umfaßt. Ferner bildet die Verschlüsselung von regelmäßig wiederkehrenden Signalen, wie z. B. zur Wagensteuerung bei Blattschreibern, eine chiffriertechnische Schwäche. Es ist daher wünschenswert, nur solche Zeichen zu verschlüsseln, die zum Text gehören, wobei jedoch Zwischenräume und Zeichenwechselsignale (wie «Zi», «Bu») mit einbegriffen sind, da diese, wenn sie unverschlüsselt bleiben, sehr gefährlich werden könnten.

Ein weiterer Wunsch beim Fernschreibchiffrieren geht dahin, daß man wenigstens in gewissen Fällen die Geheimschrift in gedruckter Form darstellen könnte. Es ist beispielsweise der Fall denkbar, wo infolge unterbrochener Fernschreibverbindung die Mitteilung auf andere Art weitergeleitet werden muß. Eine Wiedergabe der Geheimsignale, die sonst über die Leitung in Form von Druckzeichen gingen, würde dies gestatten, indem der Empfänger an seinem Gerät diesen Text wieder entschlüsseln kann. In solchen Fällen sollte die Geheimschrift aber nur die 26 Buchstaben umfassen (bzw. so viel Schriftzeichen, als der Fernschreiber in der Buchstabenstellung wiedergeben kann).

Der oben angegebenen Forderung, das heißt nur Textzeichen zu verschlüsseln bzw. mit ein und demselben Verschlüsselungsmechanismus eine Geheimschrift herzustellen, die von Fall zu Fall eine verschiedene Zahl von Zeichen aufweist, kann dadurch genügt werden, daß man die an sich bekannten, sogenannten Chiffrier-Durchgangsräder verwendet, wobei aber eine neuartige Schaltung vorgesehen werden muß. Es sei hierbei daran erinnert, daß bei der Verwendung von Durchgangsrädern, wo jedem Zeichen des Geheimschriftalphabetes ein besonderer Stromkreis zugeordnet ist, bei Fernverschlüsselung Vorkehrungen getroffen werden müssen, die beim Senden eine Übersetzung in das Telegraphier-Impulssystem und beim Empfang eine Rückübersetzung des Telegraphenalphabetes in das Mehrfach-Stromkreissystem durchführen.

Die vorliegende Erfindung betrifft eine Schaltungsanordnung bei Verschlüsselungsgeräten mit Durchgangsrädern, bei denen die Zahl der Durchgänge mindestens eines Durchgangsrades größer ist als die Zahl der zu

benützenden Eingangs- und Ausgangsleiter des Gerätes, die dadurch gekennzeichnet ist, daß jeder nicht an einen Eingangsleiter angeschlossene Eingang des genannten Durchgangsrades mit einem nicht an einen Ausgangsleiter angeschlossenen Ausgang eines Durchgangsrades verbunden ist.

Wenn man das nunmehr gebräuchliche Fernschreiberalphabet zugrunde legt, gibt es 29 Zeichen, die unter allen Umständen verschlüsselt werden sollten, und zwar die 26 Buchstaben, ferner ein Zeichen für Wortzwischenraum und zwei Zeichen für Wechselsignale. Die Durchgangsräder sind deshalb für 29 Durchgänge einzurichten. In den Fällen, wo man eine Geheimschrift herzustellen wünscht, die nur 26 Schriftzeichen aufweist (was voraussetzt, daß die Druckschrift nur 26 von den 32 Zeichenkombinationen des Fernschreibers umfaßt), werden also nur je 26 Leitungen von und zu den Durchgangsrädern führen. Nun weisen die Durchgangsräder aber 29 Ein- und Ausgangsstellen auf, von denen keine einzige offengelassen werden darf, soll ein unbehinderter Stromdurchgang für alle Kreise und bei allen denkbaren Schaltungsmöglichkeiten der Durchgangsräder gewährleistet werden. Zur Lösung dieser anscheinend unlösbaren Aufgabe verbindet man in Anwendung der Erfindung die in dem obigen Beispiel vorhandenen drei unbesetzten Eingangskontakte mit den drei unbesetzten Ausgangskontakten in willkürlicher Weise. Hierdurch wird das System für eine Verschlüsselung von 26 Zeichen verwendbar.

In der beiliegenden Zeichnung zeigen die Fig. 1 bis 3 je ein Ausführungsbeispiel des Erfindungsgegenstandes.

In Fig. 1 der Zeichnung ist das oben erläuterte Schaltungsprinzip veranschaulicht. Es bezeichnen in Fig. 1 die Bezugsziffern 1, 2 und 3 drei Durchgangsräder, die je fünf Durchgänge aufweisen, von denen im Beispiel nur drei für die Verschlüsselung in Anspruch genommen sind. Es gibt somit zwei nicht besetzte Eingangskontakte und ebenfalls zwei nicht besetzte Ausgangskontakte. Die drei Eingangsleiter sind mit *A*, und die drei Ausgangsleiter sind mit *B* bezeichnet. Die nicht besetzten Eingangskontakte sind mit *C* und die beiden nicht besetzten Ausgangskontakte sind mit *D* bezeichnet. In diesem Beispiel sind der erste und der zweite Eingangsleiter, von oben gerechnet, mit dem ersten bzw. dritten Ausgangskontakt *B* lediglich über die Durchgänge der Räder verbunden. Die beiden nicht besetzten Eingangskontakte *C* sind einerseits mit den nicht besetzten Ausgangskontakten *D* durch Umgangsleiter 5 bzw. 6 verbunden, die somit außerhalb des Durchgangsradsystemes verlaufen. Ferner ist der erste Eingangskontakt *C* mit dem zweiten Ausgangskontakt *D* derart über Durchgänge der Räder verbunden, daß die beiden Umgangsleiter 5, 6 in Reihe geschaltet sind. Der zweite Eingangskontakt *C* ist über Durchgänge der Räder mit dem zweiten Ausgangsleiter *B* verbunden, während der erste Ausgangskontakt *D* mit dem dritten Eingangsleiter *A* in Verbindung steht. Es besteht somit eine Verbindung zwischen dem dritten Eingangsleiter *A* und dem zweiten Ausgangsleiter *B* über die beiden in Reihe geschalteten nicht besetzten Kontakte *C* und *D*, wodurch alle Durchgänge der Räder zur Herstellung der Verbindungen zwischen den drei Leitern *A* und den drei Leitern *B* in Verbindung genommen sind.

Es kann vorkommen, daß gewisse Stromkreise je nach den durch die Lage der Durchgangsräder bedingten Verbindungen, Mehrfachdurchgänge aufweisen. Im Sonderfall kann der Stromkreis eines einzelnen Zeichens dreimal die Durchgangsräder durchfließen. Die Vorbeischaltung kann dabei mittels Schaltern ein-, aus- oder umgeschaltet werden, wie in Fig. 2 veranschaulicht ist, wo die Bezugsziffern 7 und 8 Stromschalter bezeichnen, die den Leitern 5 und 6 zugeordnet sind.

Es ist ferner möglich, die Zahl der Stromkreise bei den Durchgangsrädern höher zu wählen, als für die Verschlüsselung der in Betracht kommenden Zeichen unbedingt erforderlich ist. Eine derartige Ausführung hätte gewisse zusätzliche chiffriertechnische Verwicklungen zur Folge.

Ein zusätzlicher Vorteil der oben beschriebenen Schaltung besteht darin, daß ein und dieselbe Verschlüsselungsmechanik sowohl für normale Fernschreiber als auch für drukkende Chiffriermaschinen verwendet werden kann, was angesichts der zunehmenden Mechanisierung der Verschlüsselungsdienste für militärische wie für diplomatische Zwecke eine weitgehende Normalisierung der Konstruktionen zuläßt.

Abänderungen sind denkbar, wo in einer Gruppe von Durchgangsrädern die einzelnen Räder verschiedenzahlige Durchgänge aufweisen und die jeweils nicht durchgeschalteten Stromkreise wahlweise unter sich geschaltet werden können, wobei eine Durchschaltung von Anfang zu Ende der Gruppe oder nur in Teiletappen derselben erfolgen kann. Ein Beispiel einer derartigen Ausführung ist in Fig. 3 der Zeichnung veranschaulicht. In diesem Beispiel haben die Räder 1 und 2, gleich wie in den Fig. 1 und 2, je fünf Durchgänge, während das Rad 3 sieben Durchgänge aufweist. Der erste Eingangsleiter *A* ist mit einem Ausgangsleiter *B* ausschließlich über die Durchgänge der Räder verbunden, während die Verbindungen zwischen den beiden übrigen Eingangsleitern *A* und den beiden übrigen Ausgangsleitern *B* auch Umgangsleiter enthalten, die sämtliche unbesetzten Durchgänge in Anspruch nehmen.

Einen andern Sonderfall stellt das wechselweise Anordnen von sich drehenden und stillstehenden Durchgangsrädern dar, wobei die letzteren überzählige Durchgänge aufweisen, die separat schaltbar sind.

Für die oben beschriebenen und etwa andern Ausführungsbeispiele der Erfindung gilt, daß die Anordnung für die Verschlüsselung eines beliebigzahligen Alphabetes verwendbar ist, wobei lediglich eine Schranke dadurch gesetzt ist, daß nicht mehr Zeichen vorhanden sein dürfen, als es Durchgänge gibt.

PATENTANSPRUCH:

Schaltungsanordnung bei Verschlüsselungsgeräten mit Durchgangsrädern, bei denen die Zahl der Durchgänge mindestens eines Durchgangsrades größer ist als die Zahl der zu benützenden Eingangs- und Ausgangsleiter des Gerätes, dadurch gekennzeichnet, daß jeder nicht an einen Eingangsleiter angeschlossene Eingang des genannten Durchgangsrades mit einem nicht an einen Ausgangsleiter angeschlossenen Ausgang eines Durchgangsrades verbunden ist.

UNTERANSPRÜCHE:

1. Schaltungsanordnung nach Patentanspruch, dadurch gekennzeichnet, daß die genannten Verbindungen Umschalter enthalten.

2. Schaltungsanordnung nach Patentanspruch, dadurch gekennzeichnet, daß wenigstens eine der genannten Verbindungen nicht das letzte mit dem ersten Durchgangsrad verbindet.

Boris Caesar Wilhelm Hagelin.

Vertreter: E. Blum & Co., Zürich.

Boris Caesar Wilhelm Hagelin

Patent Nr. **312238**
1 Blatt

Fig. 1

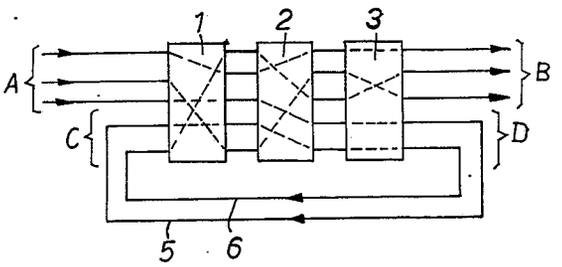

Fig. 2

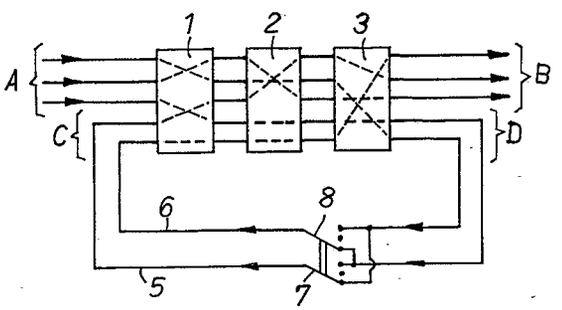

Fig. 3