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

AUSGEGEBEN AM 19. JUNI 1952

REICHSPATENTAMT

PATENTSCHRIFT

Nr. 767 367

KLASSE 21a[1] GRUPPE 21

L 97914 VIIIa/21a[1]

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. phys. Gerhard Grimsen, Eßlingen/Neckar

ist als Erfinder genannt worden

C. Lorenz A. G., Stuttgart

Verschlüsselungseinrichtung zur zeitlichen Vertauschung von Fünfer-Alphabet-Impulsen

Patentiert im Deutschen Reich vom 11. Mai 1939 an

Patenterteilung bekanntgemacht am 24. April 1952

Bei der Verschlüsselung von Nachrichten, die mit Hilfe der modernen Mehrfach-Alphabete, z. B. Fünfer-Alphabete, übertragen werden, ergeben sich als Angriffspunkt für die Verschlüsselung verschiedene Möglichkeiten:

Einmal ist es möglich, die Polarität der einzelnen Impulse innerhalb des Fünferstrombildes nach besonderen Rezepten zu ändern. Es ist auch weiterhin vorgeschlagen worden, die zeitliche Reihenfolge des Strombildes innerhalb seiner fünf Stromschritte zu vertauschen.

Es ist weiterhin eine Verschlüsselungseinrichtung bekanntgeworden, die die Einwirkung des Klartextes auf die Verschlüsselungsanordnung vorsieht. Bei dieser bekannten Einrichtung handelt es sich um eine chiffrierende Fernschreibmaschine. Es geht daher der Eingriff in den Vorschub der den Mischtext erzeugenden Nockenräder von der Wahl bestimmter Typenhebel aus, d. h. bei der Übertragung bestimmter vorher festgelegter Klartextbuchstaben wird der Vorschubmechanismus angehalten. Bei dieser bekannten Einrichtung ist also das Vorhandensein bestimmter Buchstaben dafür maßgebend, ob die Verschlüsselungseinrichtung in ihrem Lauf gehemmt werden soll oder nicht.

Weiterhin bekanntgewordene Einrichtungen zur geheimen Übertragung von Telegraphierzeichen sehen vor, daß beim Drücken einer Sendetaste die Weiterschaltung des Verschlüsselungssystems stattfindet, und zwar wird bei dieser bekannten Einrichtung der Verschlüsselungsmechanimus ein oder mehrere Schritte vor- oder rückwärts geschaltet, je nachdem, was für eine Taste gedrückt worden ist. Auch bei dieser bekannten Einrichtung ist die Weiterschaltung des Schlüsselmechanismus abhängig von vorher bestimmten Tasten. Es sind auch Einrichtungen bekanntgeworden, bei denen eine Beeinflussung des Schlüsselmechanismus in Abhängigkeit von einem vorher gegebenen Zeichen stattfindet.

Zur weiteren Erschwerung des Dechiffrierens verwendet die vorliegende Verschlüsselungseinrichtung zur zeitlichen Vertauschung von Fünfer-Alphabet-Impulsen mindestens fünf fünfarmige Wähler mit mindestens 24 Schritten. Bei dieser Einrichtung werden erfindungsgemäß bei allen übertragenen Buchstaben die jedem der fünf Zeichenelemente des Buchstabens zugeordneten Teile der Verschlüsselungseinrichtung, je nachdem, ob das entsprechende Zeichenelement des zuletzt übertragenen Buchstabens stromerfüllt oder stromleer war, einzeln weitergeschaltet oder nicht weitergeschaltet. Wie eingangs erwähnt, werden zur Vertauschung der fünf Impulse eines Strombildes, die für einen bestimmten Buchstaben charakteristisch sind, fünf Wähler verwendet, die im allgemeinen bei der Übertragung eines jeden Buchstabens um je einen Schritt weiterbewegt werden. Die Kontaktbänke dieser Wähler sind entsprechend den fünf Möglichkeiten der Vertauschung verdrahtet, so daß alle Vertauschungsmöglichkeiten eintreten können und daß schon bei gemeinsamem gleichzeitigem Antrieb aller fünf Wähler eine gewisse Mischung im Rahmen der Zeit erfolgt, die das Entziffern wesentlich erschwert. Zur Erschwerung der Dechiffrierung ist nun der Antrieb dieser fünf fünfarmigen Wähler von dem Klartext, der verschlüsselt werden soll, insofern abhängig gemacht worden, als durch eine Auswählvorrichtung geprüft wird, ob der einzelne von den fünf Impulsen, aus denen jeder Klartextbuchstabe besteht, stromerfüllt oder stromleer ist. Ist beispielsweise ein einzelner Impuls stromerfüllt, wird in die Fortschaltung des Wählers nicht eingegriffen. Ist dagegen ein einzelner Impuls stromleer, wird der Vorschub eines der fünf Wähler für einen Schritt unterdrückt, je nachdem, welcher von den fünf Impulsen stromleer ist. Hierdurch wird erreicht, daß, ausgehend von einer bestimmten Anfangsstellung, die Relativstellung der fünf Vertauschungsglieder sich in Abhängigkeit von dem jeweils übertragenen Klartext ändert, so daß bereits nach wenigen Buchstaben des jeweils vorliegenden Telegramms trotz gleicher Ausgangsstellung die Schlüsselstellung eine andere geworden ist.

In der Abbildung ist eine beispielsweise Ausführungsform des Erfindungsgedankens dargestellt. Es sind die fünf Wähler A, B, C, D, E angenommen, die mit je fünf Armen ausgerüstet sind und deren Kontaktbahnen je 24 oder mehr Stellungen aufweisen. Durch die Verdrahtung der Kontaktbänke ist dafür gesorgt, daß mindestens alle 120 Vertauschungsmöglichkeiten vorgesehen sind, so daß bei einer gleichzeitigen Verstellung aller fünf Wähler das Eingangsstrombild in bestimmter Weise zum Ausgangsstrombild vertauscht wird. Außerdem ist jeder Vorschubmechanismus mit einer Verriegelungseinrichtung ausgestattet, die von dem Strombild des Klartextbuchstabens, der zu übertragen ist, gesteuert wird, und zwar in der Weise, daß z. B. entsprechend den 32 Möglichkeiten des Fünfer-Alphabetes die stromerfüllten Impulse den gemeinsamen Vorschub der Wählerachsen freigeben oder die stromleeren Impulse diesen unterdrücken. Die Kreise EK_1 bis EK_5 sind Fortschaltanordnungen der Wähler 1 bis 5. Die Kontakte sind die Ausgänge einer Registriervorrichtung, die die fünf Impulse des Klartextbuchstabens aufnimmt und die Kontakte entsprechend einstellt. Zum Schluß wird der Kontakt EK_{stop} geschlossen, der nunmehr entsprechend den vorbereiteten Einstellungen der Kontakte EK_1 bis EK_5 die Fortschaltung der einzelnen Wähler vornimmt, wenn Kontakt geschlossen, oder diese um einen Schritt anhält, wenn Kontakt offen. Auf diese Weise wird eine stets wechselnde Relativstellung der fünf Wählerachsen in Abhängigkeit von dem jeweils übertragenen Klartext trotz gemeinsamen Antriebs erreicht. Zur weiteren Erschwerung der Erkennbarkeit dieser Zwangsläufigkeit kann z. B. eine von Hand zu bedienende Vertauschungseinrichtung vorgesehen werden, die mit der nötigen Anzahl von Vertauschungsstellen ausgerüstet für eine wahlweise Änderung dieser Zuordnung des Vorschubmechanismus oder seiner Unterdrückung von den Strombildern des Klartextbuchstabens sorgt.

PATENTANSPRUCH:

Verschlüsselungseinrichtung zur zeitlichen Vertauschung von Fünfer-Alphabet-Impulsen durch mindestens fünf fünfarmige Wähler mit mindestens 24 Schritten, dadurch gekennzeichnet, daß bei allen übertragenen Buchstaben die jedem der fünf Zeichenelemente des Buchstabens zugeordneten Teile der Verschlüsselungseinrichtung (Wähler I bis V), je nachdem, ob das entsprechende Zeichenelement des zuletzt übertragenen Buchstabens stromerfüllt oder stromleer war, einzeln weitergeschaltet bzw. nicht weitergeschaltet werden.

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

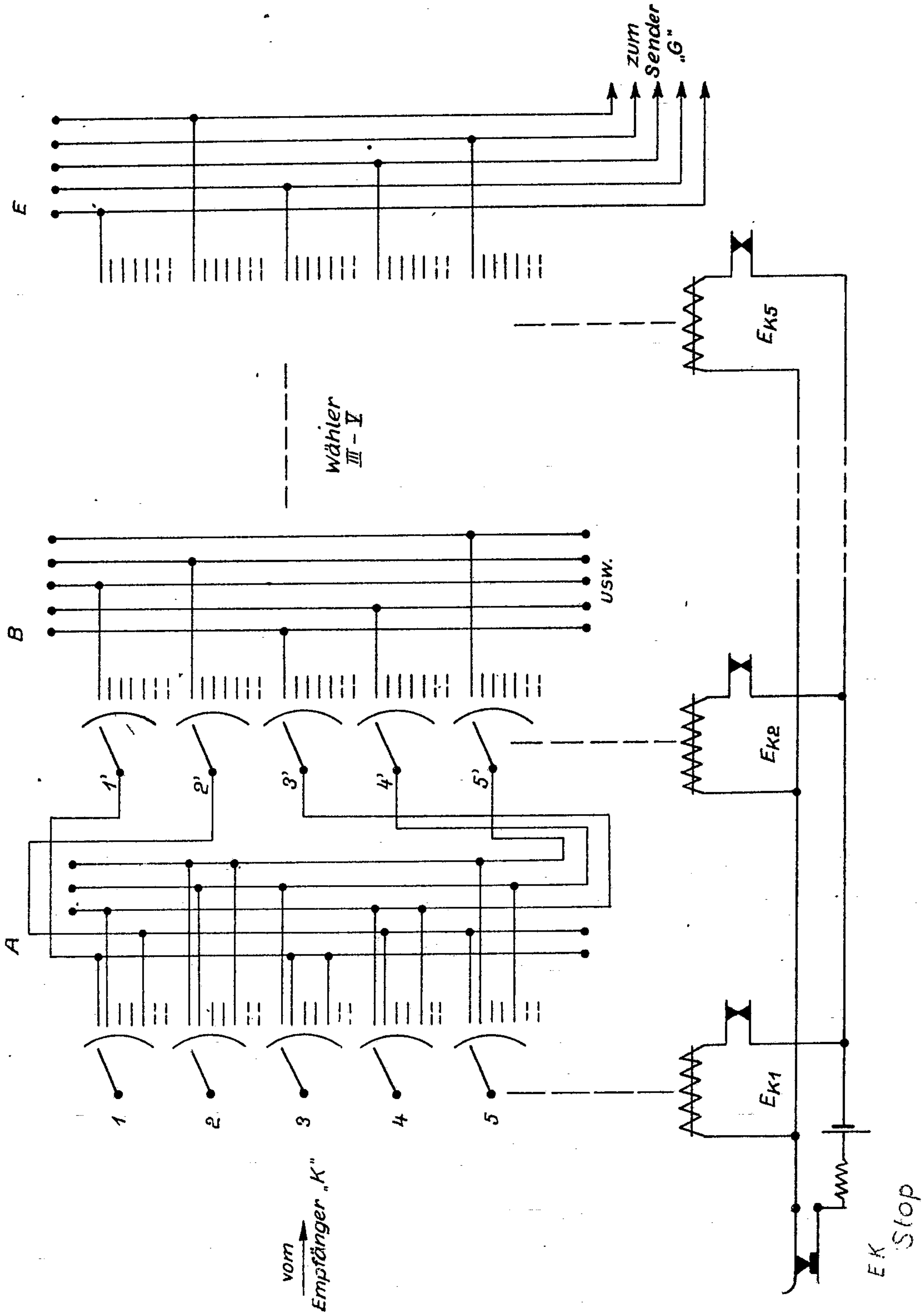
Deutsche Patentschriften Nr. 591 974, 603 261, 615 016, 621 203, 641 560;

französische Patentschriften Nr. 628 788, 798 575 (entsprechend Patentschrift Nr. 685 612);

österreichische Patentschrift Nr. 105 296.

Hierzu 1 Blatt Zeichnungen

5218 6.52


zum Sender „G“
E
Wähler III - V
B
usw.
A
1'
2'
3'
4'
5'
1
2
3
4
5
vom Empfänger „K“
EK5
EK2
EK1
EK Stop