HAGELIN-CRYPTOS

CRYPTO AG.
ZUG
(Switzerland - Suisse)

A-1130-c

SCHLUESSELGERAET TYP HX-63

(Vorläufige Beschreibung)

I) AUFBAU:

Das Gerät ist nach dem Baukastenverfahren zusammengesetzt. Die verschiedenen Funktionsgruppen sind in einem Hauptgestell montier und bestehen aus:

a) Netzgerät, Hilfsaggregate, Motor.

b) Tastatur und Funktionsschalter, nachstehend V/E-Schalter genannt.

c) Durchgangsradwandler, nachstehend Wandler genannt und Modifikator.

d) Druckwerk.

Die elektrischen Verbindungen sind steckbar ausgeführt.

II) FUNKTIONSGRUPPEN: (Darstellung)

a_1) Netzgerät: Transformator für 110/220 V, Wechselstrom 40...60 Hz mit Gleichrichter. Interne Spannungen 12 V=, sodass das Gerät auch durch einen (separaten) Akkumulator betrieben werden kann. Es besteht die Möglichkeit, den Akkumulator über das Netzgerät zu laden.

Post address Adresse postale Zug, Weinbergstrasse 10 Phone Téléphone (042) 4 36 32 Cable Télégrammes CRYPTO ZUG

a_2) Motor: Ein 12 Volt Gleichstrom-Permanentfeldmotor mit angebautem Fliehkraftregler treibt über Vorgelege, Druckwerk und Wandler.

b_1) Tastatur: Dreireihige Schmaltastatur mit Belegung der Buchstaben und Zeichen weitgehend nach Alphabet No. 2 CCITT. (Fig.1).

b_2) V/E Schalter: Dieser Umschalter weist normal 5 Stellungen auf:

"AUS"

"EIN" Hier kann die Ausgangslage der D-Räder elektrisch eingestellt werden.

"K" Klar

"V" Verschlüsseln

"E" Entschlüsseln

Dazu "PE" = Durchlauftaste, falls Zusammenarbeit mit dem Zusatzgerät PEH-61 gewünscht wird. (Siehe Abschnitt V).

c_1) Wandler: Enthält 9 Durchgangsräder (D-Räder) mit je 41 umstellbaren Durchgängen und 41 verstellbaren Stiften. Elektromagnetische Fortschaltmechanismus. (Nähere Auskunft über die Theorie des Fortschaltungssystemes siehe Druckschrift A-1149.)

c_2) Modifikator: Dieses Schaltelement gestattet die Vertauschung der 41 Verbindungen an der Klarseite des Wandlers.

c_3) Umschaltmöglichkeit: auch für die Geheimseite.

d) Druckwerk: Doppeldruckwerk mit stehendem Druck bei ca 8...10 Zeichen/Sek., Druck auf 17,4 mm breitem Streifen mit automatischer Längsteilung für Klar- und Geheimtextdruck. Der Klartext kann alle Buchstaben und Zeichen, sowie technische Symbole enthalten, die auf der Tastatur verzeichnet sind. Der Geheimtext enthält normalerweise nur 26 Buchstaben.

III) ARBEITSWEISE:

Der Text wird normalerweise auf der Tastatur geschrieben. Auf beiden Streifen erscheinen übereinander der Klar- und der Geheimtext, wodurch eine bequeme Textkontrolle möglich ist. In der Stellung "Klar" des V/E-Schalters können offene Texte auf beiden Streifen gleichzeitig identisch geschrieben werden (z.B.Adresse). Es muss nur noch darauf geachtet werden, dass für korrespondierende Geräte sämtliche Einstellungsvariablen sinnvoll und identisch angeordnet werden.

IV) EINSTELLUNGSVARIABLEN (Schlüsselmittel)

In Zahlen anzugeben, welchen Sicherheitsgrad das HX-Gerät bietet, ist unmöglich. "Absolute Sicherheit" bieten diejenigen Verfahren, bei denen homogenes Material nur in einer für Entzifferungszwecke unzureichenden Menge anfällt. Ein erstklassiges Gerät sollte deshalb bequeme Möglichkeiten haben, den statistischen Charakter der einzelnen Sprüche auch bei intensivstem Verkehr zu kürzen. Beim HX-Gerät sind solche Variationsmöglichkeiten in reichem Masse vorhanden (siehe auch Fig. 2):

a) Es befindet sich an der Eingangsseite des Wandlers - wo die von der Ausgangsseite des Wandlers zurückgeführten 15 Leitungen angeschlossen sind - der sog. Modifikator, der aus 26 und 15 Kontaktscheiben mit je 26 bzw. 15 Lagen besteht;

mit dessen Hilfe können die 41 zum Wandler führenden Leitungen in 25! & 16! verschiedene Anordnungen geschaltet werden. Von dieser Zahl sollten bis zu 10^{30} Möglichkeiten cryptologisch sinnvoll sein. Es wird hier auf die grosse Anzahl von Rückführungen zum Wandler besonders hingewiesen, sowie darauf, dass Modifikator (und eventuell Umschaltung) die Möglichkeit bieten, die Lagen auch von diesen Leitungen an den Eingangs- bzw. Ausgangsseiten des Wandlers zu verändern.

b) Die inneren Verbindungen in jedem einzelnen D-Rad können in 41! verschiedene Kombinationen geschaltet werden. Von dieser Zahl sollten bis zu 10^{30} Möglichkeiten cryptologisch sinnvoll sein.

c) Die Reihenfolge der D-Räder:

Es sind 9! d.h. $3,6 \times 10^5$ verschiedene Folgen möglich; ausserdem können überdies beliebige 9 aus insgesamt z.B. 12 D-Rädern ausgewählt werden, die Zahl der Möglichkeiten erhöht sich dann z.B. auf 9! $(9^{12}) = 8 \times 10^7$ verschiedene Radkombinationen. Alle möglichen D-Radfolgen sind gleich gut brauchbar.

d) Die 41 Stifte an den D-Radkränzen, welche der Steuerung der D-Radbewegung dienen, könnten in 2^{41}, d.h. $2,2 \times 10^{12}$ verschiedene Aktivlagen eingestellt werden. Von dieser Zahl sollten bis zu 10^6 Möglichkeiten cryptologisch sinnvoll sein.

e) Zum Antrieb der D-Räder wird ein System verwendet, welches ein unregelmässiges Fortschaltungsschema mit einer Periodenlänge von 41^9 oder rund $3,3 \times 10^{14}$ Zeichen gewährleistet. Dieses System bietet zwei Varianten:

A) <u>System "M"</u>:

Ein Rad macht immer einen Schritt, während die folgenden Räder in einer Steuerkette so zusammengeschaltet sind, dass jedes Rad in der Kette nur dann um einen Schritt fort-

geschaltet wird, wenn irgend eines bis alle vorangehenden Räder einen aktiven Stift in der Einflusslage aufweisen.

B) System "MM":

Ein Rad macht immer einen Schritt, die übrigen Räder werden aber nur dann fortgeschaltet, wenn die Zahl der vorangehenden Räder, mit aktiven Stiften in der Einflusslage ungerade ist.

Der Unterschied zwischen A) und B) liegt darin, dass beim Syst "M" die Zahl der Fortschaltungsschritte bei den Rädern 2 bis 9 umso grösser ist, je weiter das betreffende Rad in der Steuerkette vom ersten entfernt ist, während beim System "MM" die Forschalthäufigkeit für diese Räder immer bei 50 % bleibt, vorausgesetzt, dass eine normale 50 prozentige Verteilung aktiver/inaktiver Stifte zur Verwendung kommt. Mit einem Schalter kann man das gewünschte Fortschaltsystem wählen.

f) Es kann auch die Steuerkette verändert werden; hier ergeben sich 9!, d.h. $3{,}6 \times 10^5$ verschiedene Möglichkeiten. Die Wirkung ist hier eine ganz andere als beim Vertauschen der D-Räder. Alle die möglichen Steuerketten sind gleich gut brauchbar.

g) Die vom Wandler ausgehenden 41 Leitungen können am Wandler beliebig angeschlossen werden. Es ergeben sich hier 41! oder etwa $3{,}3 \times 10^{49}$ Möglichkeiten. Von dieser Zahl sollten bis zu 10^{30} Möglichkeiten cryptologisch sinnvoll sein.

Wenn alle die Variationsmöglichkeiten, die im Vorangehenden angegeben worden sind, kombiniert (multipliziert) werden, ergeben sich astronomische Grössenordnungen, sodass selbst bei stärkstem Verkehr nur ein Bruchteil der Möglichkeiten ausgeschöpft werden kann.

Die oben genannten Schalt- und Einstellmöglichkeiten müssen natürlich in verschiedenem Masse und in einem bestimmten Umfange zur Verwendung kommen.

Hinzu kommt noch die Wahl der Ausgangslagen der D-Räder für jeden Spruch, der verschlüsselt werden soll. Da die Länge der Periode immer 41^9 oder rund $3,3 \times 10^{14}$ Zeichen umfasst, wäre es theoretisch möglich, z.B. etwa 10^{10} Sprüche von einer mittlere Länge von 10.000 Zeichen zu verschlüsseln, ohne dass sich die verwendeten Schlüsselfolgen überschneiden würden.

Die vorgenannten Variablen können in "äussere" und "innere" Schlüssel eingeteilt werden. Aeussere Schlüssel nennen wir solche Einstellungen, welche vorgenommen werden können, ohne dass die Schutzhaube des Gerätes geöffnet zu werden braucht, während die übrigen als innere Schlüssel bezeichnet werden.

Die äusseren Schlüssel sind beim HX-Gerät:

a) Die Ausgangslagen der D-Räder

Die inneren Schlüssel sind:

b) Die Modifikator-Einstellung.

c) Die Wahl des Schaltsystemes ("M" oder "MM") und die Einstellung der Steuerkette.

d) Die Veränderung der Reihenfolge der D-Räder, eventuell auch Auswahl aus einer grösseren Anzahl verfügbarer Räder.

e) Die Umstellung der Stiftkombinationen an den D-Rädern.

f) Die Umsteckung der Verbindungen in den D-Rädern und eventuell

g) die Umschaltung der Leitungen an der Ausgangsseite des DR-Wandlers.

Die Aenderungen laut f) und g) können nur unter sauberen Verhältnissen vorgenommen werden.

Die inneren Schlüssel bleiben längere Zeit gültig, während der äussere häufig gewechselt wird. Es sollten die Ausgangslage a), die Modifikationseinstellung b) und die Einstellung der Steuerkette c) einzeln oder kombiniert für jeden Spruch neu gewählt werden.

Obwohl erfahrungsgemäss bei Geräten mit D-Rädern bis zu 40 Sprüchen ohne Gefahr mit derselben Ausgangslage verschlüsselt werden könnte, ist dies prinzipiell nicht zu empfehlen. Tabellen von Ausgangslagen herzustellen, die voneindander getrennte Schlüsselserien gewährleisten, ist eine Aufgabe, die sich mit ein entsprechend programmierten Rechengerät leicht bewältigen lässt.

V) LOCHSTREIFENBETRIEB:

Wo Fernschreiblinien mit Lochstreifengeräten vorliegen, kann mit Hilfe des Zusatzgerätes PEH-61, das einen Stanzer und einen Abtaster enthält, (Druckschrift D-1134) der Verkehr automatisiert werden (Fig.3). Beim Verschlüsseln wird der Geheimtext im PEH auf Lochstreifen gestanzt. Dieser Geheimtext kann, wenn gewünscht zwecks Kontrolle gleich automatisch entschlüsselt werden; für diese Funktion muss nur die Durchlauftaste betätigt werden. Klar- und Geheimtext entsprechen dem CCITT Code.

Beim Entschlüsseln auf der Empfangsstelle wird der in Lochstreifenform vorliegende Geheimtext in den Abtaster des PEH eingelegt und im HX-Gerät automatisch entschlüsselt. Es besteht auch die Möglichkeit den Klartext durch Lochstreifen in den PEH einzugeben, und dort (beim Verschlüsselungsvorgang in der HX) einen Geheimtextlochstreifen gleichzeitig gestanzt zu bekommen.

Soll der Klartext beim Entschlüsseln auf Blattschreiber wiedergegeben werden, so kann während des automatischen Entschlüsselungsvorganges ein neuer Klar-Lochstreifen gestanzt werden, wobei durch eine im PEH eingebaute Programmierstufe die Zeichenvorschub- und Wagenrücklaufsignale in den richtigen Plätzen zusätzlich eingestanzt werden. Beim nachträglichen Drucken in einer

Lochsender/Blattschreiber Kombination werden volle Linien geschrieben.

Gleichzeitig mit der Herstellung des neuen programmierten Klar-Lochstreifens werden auf der HX Klar- und Geheimtext auf Streifen mitgedruckt.

Der kombinierte HX/PEH-Betrieb ist auf Grund der hohen Arbeitsgeschwindigkeit einem lokalen Fernschreiber-Mischbetrieb ebenbürtig; da er aber nicht auf Tarnstreifen angewiesen ist, weist er organisationstechnische Vorteile auf. Besonders vorteilhaft erweist sich dies bei vermaschten Netzen mit Querverbindungen.

VI) SONDERAUSFUEHRUNGEN:

Vereinfachung in der Ausführung kann, falls vom Kunden gewünscht, nach den folgenden Richtlinien erfolgen:

1) Die Steuerkette für das Fortschalten der D-Räder kann starr festgelegt werden (der Charakter der Bewegung wird jedoch immer durch die Umstellung der Stifte verändert); der Umschalter "M"/"MM"-Antrieb kann weggelassen werden.

2) Der Modifikator kann entfallen, oder durch eine einfache steckbare Ausführung ersetzt werden.

3) Die Anordnungen für die Zusammenarbeit mit dem PEH-Gerät können fehlen.

4) Falls auch Handbetrieb erwünscht wird, weisen wir auf die Maschine, Typ HX-61 hin. Hier ist die normale Arbeitsgeschwindigkeit jedoch auf ca 5 Zeichen/Sek. beschränkt bei Handbetrieb etwa 1 Zeichen/Sek.

Abmessungen: 400 x 400 x 230 mm Gewicht: 16 kg

Beilage: Fig. 1/2/3
Zug, März 1964 OSt/iz

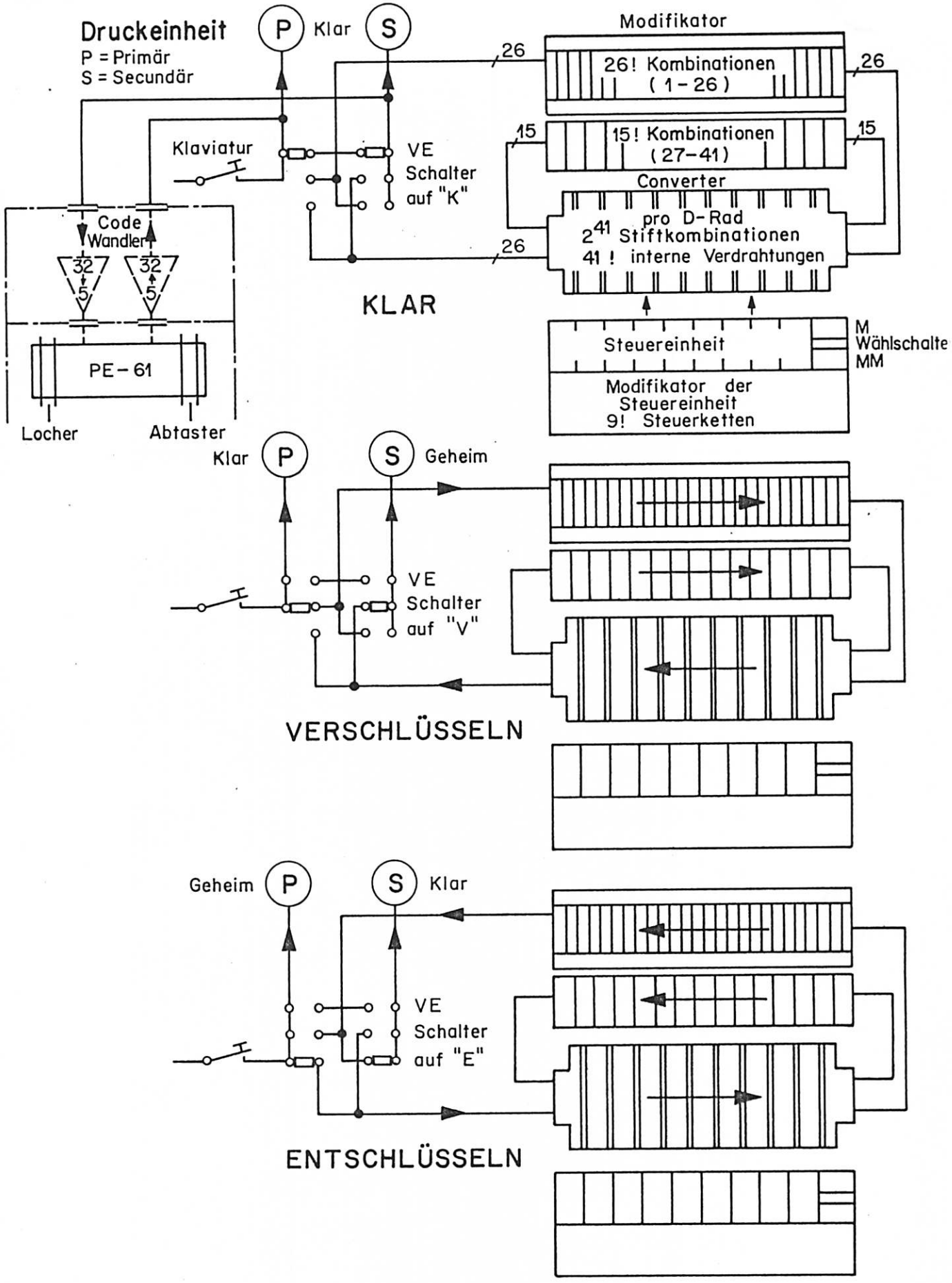
Tastenanordnung zu HX

CRYPTO AG. ZUG (Schweiz)

1130

Fig.1

20.11.63 B.



Blockschema HX - 63

1130

Fig. 2

12.3.64 Hau.

CRYPTO AG. ZUG (Schweiz)

HX - 63 (HR)

PEH - 61

HX (HR)

.130

Fig. 3

CRYPTO AG. ZUG (Schweiz)