HAGELIN CRYPTOS

No. I 1088-b

# TASCHENCHIFFRIERGERAET CD-57

Techn. Beschreibung

HAGELIN-CRYPTOS

No. I 1088-b

# TASCHENCHIFFRIERGERAET
# CD-57

## Techn. Beschreibung

---

Inhaltsverzeichnis

HAGELIN-CRYPTOS

CRYPTO AG.
ZUG
(Switzerland - Suisse)

No. I 1088-b

# TASCHENCHIFFRIERGERAET TYP CD-57

Technische Beschreibung

## I. Einleitung

### A. VORWORT

Der steigende Bedarf an Taschenchiffriergeräten hat zur Entwicklung der CD-57 geführt. Dieses Gerät ist für solche Anwendungsfälle zu empfehlen, wo Kleinheit die Hauptforderung darstellt und wo auf gedruckte Meldungen verzichtet werden kann.

Gegenüber bisher bekannten Taschengeräten weist die CD-57 eine grössere Sicherheit auf; sie bietet ausserdem die Möglichkeit, mit grösseren - druckenden Geräten unserer Fabrikation (C-4 und C-52/CX-52) zusammenzuarbeiten, was beim Aufbau von Nachrichtenorganisationen von Vorteil ist.

### B. ALLGEMEINE BEMERKUNGEN

Die kryptographischen Funktionen der CD-57 Geräte sind analog denjenigen in den C und CX Geräten. Der Aufbau ist - der gedrängten Bauweise wegen - gegenüber diesen Geräten jedoch etwas verändert worden. Trotzdem besteht die Möglichkeit die verschiedenen Gerätetypen so auszurüsten, dass eine gegenseitige Korrespondenz ermöglicht wird, was im Hinblick des Aufbaues eines Chiffrierdienstes zwischen CD/C/CX/M-209 wesentlich ist.

Die wichtigsten Merkmale im Vergleich zu den angeführten grösseren Geräten sind folgende:

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

1) Kleine Abmessungen (80 x 130 x 80 mm) und niedriges Gewicht (650 gr.)

2) Dasselbe Gerät dient sowohl zum Verschlüsseln, wie zum Entschlüsseln.

3) Raschheit. Da kein Druckmechanismus vorliegt, fällt das "Einstellen" der Buchstaben weg. Es wird lediglich "abgelesen" und, falls nötig von Hand notiert - in vielen Fällen aber direkt in das Telephon oder das Funkgerät diktiert. Es sind Arbeitsgeschwindigkeiten von 40 Zeichen/min. möglich.

## C. DEFINITIONEN

Verschiedene Ausdrücke erheischen eine Erklärung. Da bis z.Z. keine international anerkannten Wörterbücher über Kryptographen bestehen, seien die in der folgenden Beschreibung verwendeten Spezialausdrücke näher beschrieben:

Primärer Text: Derjenige Text, bzw. diejenigen Buchstaben, die verarbeitet werden müssen. Beim Verschlüsseln also der Klartext, beim Entschlüsseln der Geheimtext.

Sekundärer Text: Diejenigen Buchstabenfolgen, die durch das Gerät erzeugt werden. Beim Verschlüsseln der Geheimtext, beim Entschlüsseln der Klartext.

Relativlage. Stellung des primären zum sekundären Alphabet in der Grundstellung, d.h. bei Umstellschrittzahl 0 oder 26.

Inverse Alphabete. Zwei Buchstabenfolgen, deren 26 Buchstaben gegeneinander in umgekehrter Richtung angeordnet sind.

Verschlüsseln/Entschlüsseln. Vom Gerät aus gesehen sind beide Funktionen identisch, sie werden speziell im Text erwähnt, falls es sich um spezifische Erklärungen einer Funktion handelt. Im Allgemeinen wird der Ausdruck chiffrieren angewendet werden.

Schlüssel. Das Gerät besitzt verschiedene Elemente, die in ihren Anordnungen verändert werden können. Das Einstellen dieser Elemente nach Instruktionen erfolgt um die verschiedenen Geräte zu gleichartigen Operationen zu veranlassen, die ein Chiffrieren überhaupt erst ermöglicht.

Man unterscheidet Grundschlüssel, die während des Betriebes stets gleich bleiben, und Ausgangsschlüssel, die während des Betriebes sich verändern können.

Die Grundschlüssel umfassen:

a) Anordnung der Anschläge auf dem Umstellzylinder.

b) 1) Auswahl der Stifträder
   2) Anordnung derselben
   3) Anordnung der Stiften auf den Stiftscheiben.

Die Ausgangsschlüssel umfassen:

a) Stellung der Stiftscheiben in Bezug auf die Bezugslinie.

b) Relativlage (Stellung des feststehenden Buchstabenringes).

Umstellung und Vorschub.

Der Chiffriervorgang besteht im Vordrehen der Buchstabenscheibe gegenüber einer Ausgangslage. Dies geschieht schrittweise in 1/26 Kreisteilungen. Die Bewegung, die die Buchstabenscheibe so ausführt,nennen wir Umstellung, sie wird durch Umstellschritte bewirkt. Eine Serie von solchen Schritten wird Umstellschrittfolge oder Substitutionsschrittfolge genannt; oft wird sie auch kurz mit Schlüsselfolge bezeichnet.

Die Stiftscheiben werden während des Chiffriervorganges ebenfalls schrittweise verdreht, wobei die Schritte 1/n des Kreisumfanges betragen wenn n die Stiftzahl der Scheibe angibt. Die Bewegung der Stiftscheibe wird durch Vorschubschritte bewirkt, dies zum Unterschied der Bewegung der Buchstabenscheibe.

## II Allgeimeine Beschreibung

### A. GLIEDERUNG

Die Mechanik des Gerätes ist auf einer gepressten Montageplatte aus Stahl angeordnet, die mit 4 Schrauben im Gehäuse befestigt ist, das aus einer unteren (Boden) und einer oberen (Deckel) Hälfte besteht, welche beide aus Leichtmetallspritzguss bestehen.

Wir können folgende Hauptteile unterscheiden:

| | | | |
|---|---|---|---|
| 1) | Gehäuse | Gruppen-Nr. | 1 |
| 2) | Montageplatte | " | 2 |
| 3) | Umstellzylinder mit Buchstabenscheibe | " | 3 |
| 4) | Stiftradgruppe | " | 4 |
| 5) | Vorschubmechanik | " | 5 |
| 6) | Abtastmechanik | " | 6 |
| 7) | Antriebsmechanik | " | 7 |

Die Gruppennummer tritt in der nachfolgenden Detailbeschreibung an erster Stelle auf, nachfolgende Zahlen werden zur Bezeichnung von Unterelementen verwendet. Die folgende Zusammenstellung ist nicht vollständig, sondern soll nur die zur Erläuterung des Gerätes notwendigen Teile darstellen, wobei - soweit möglich - Bezug auf die anschliessenden Illustrationen genommen wird.

**

Zusammenstellung der wichtigsten Bestandteile

Teile in [ ]-Klammern sind nicht dargestellt, jedoch Unterelemente davon.

| | | sichtbar in Fig. |
|---|---|---|
| [1] | Gehäuse | 1, 5 |
| 11 | Deckel | 1, 5 |
| 1101 | Marke | 1 |
| 111 | Scharnierstift | 5 |
| 112 | Verschlussfeder | 4 |

** Für vollständige Zusammenstellung ist der Ersatzteilkatalog massgebend.

| | | sichtbar in Fig. |
|---|---|---|
| 1121 | Verschlussfederknopf | 3, 5 |
| 113 | Haltefeder für Hilfskurbel | 5 |
| 1131 | Hilfskurbel | 5, 9, 10 |
| 114 | Rasthebel für Buchstabenkranz | 4 |
| 1141 | Rasthebelfeder | 4 |
| [116] | Buchstabenkranz | |
| 1161 | Einstellring (oder-Krone) | 2 |
| 116101 | Lochkranz | 4 |
| 11611 | Alphabetenring | 2 |
| 1162 | Glasdeckel | 1 |
| 1163 | Sicherungsring | 1 |
| 12 | Grundplatte | 5 |
| 2 | Montageplatte | 5, 8 |
| [201] | 3 Zyl.-Schrauben | |
| 21 | Federgehäuse | 7, 9 |
| 211 | Steg | 7 |
| [212] | Benzing-Sicherung | |
| 22 | Stütze | 6 |
| 221 | Stiftradhaltefeder | 6 |
| [222] | Benzing-Sicherung | |
| 23 | Gehäuse für Malteserkreuz | 7 |
| 231 | Führungsstift für Stiftträder | 7 |
| 24 | 3 Stützen | 7 |
| [241] | 3 Benzing-Sicherungen | |
| 242 | Stützplatte | 7 |
| 25 | 2 Zählerstützen | 5 |
| [251] | Zyl.Schrauben | |
| 26 | Gravur für Anschläge | 6 |
| 27 | Bezugslinienstab | 6 |
| 28 | Sperrschieber | 3, 11 a |
| [281] | Blattfeder | |
| [282] | Stift | |
| 3 | Umstellzylinder | 5, 8 |
| 31 | (6) Zahnscheiben | 9, 11 b |
| 3102 | Nase | 12 |
| 311 | Klinke | 12 |

| | | sichtbar in Fig. |
|---|---|---|
| [312] | Klinkenfeder | |
| 313 | Anschlag | 9, 12 |
| [32] | Benzing-Sicherung | |
| [33] | Welle | |
| [34] | Alphabetenträger | |
| 3401 | Nase | 12 |
| [3402] | Stift | |
| 341 | Ablesescheibe | 10, 11 b, 12 |
| [342] | Nute | |
| 35 | Ritzel | 11 |
| [351] | Führungsscheibe | |
| [352] | Benzing-Sicherung | |
| 4 | Stiftradgruppe (6Stück) | 5, 6 |
| 41 | Stiftrad (12 Teilungen) | 7 |
| [411] | Stiftenkranz | |
| 4111 | Stift aktiv | 7 |
| 4112 | Stift inaktiv | 7 |
| [412] | Scheibenlager | |
| [4121] | Ritzel | |
| [4122] | Klinke | |
| [4123] | Klinkenfeder | |
| [5] | Vorschubmechanik | |
| 51 | Malteserkreuz | 7 |
| 5101 | Schlitz für Hilfskurbel | 10 |
| [511] | Ritzel | |
| 52 | Zwischenrad | 8 |
| 53 | Zähler | 5, 6 |
| 531 | Zählerritzel | 8 |
| 6 | Abtastmechanik | 5 |
| 61 | Spannbügel | 11 b |
| 611 | Steuerrolle | 11 |
| 62 | (6) Abtasthebel | 11 b, 12 |
| 621 | Schraubenfeder | 11 b |
| [7] | Antriebsmechanik | |
| 71 | Antriebsbügel | 2, 11 a |
| [7101] | Sektorschlitz | |

| | | sichtbar in Fig. |
|---|---|---|
| 7102 | Kurvenschlitz | 11 a |
| 7103 | Griff | 3 |
| 710 | Zahnsegment | 11 |
| 711 | Sperrklinke | 11 a |
| [7111] | Klinkenfeder | |
| [713] | Vorschubklinke | |
| [7131] | Klinkenfeder | |
| [714] | Schraubenfeder | |
| 72 | Antriebssegment | 11 a |
| 7201 | Zahnsegment | 11 |
| [7202] | Anschlag | |
| 721 | Winkelhebel | 11 a |
| 7211 | Zugfeder | 11 a |
| 7212 | Ausgleichshebel | 11 a |
| 7213 | Zugfeder | 11 a |
| [7203] | Benzing-Sicherung | |
| 73 | Rastklinke | 11 a |
| [7301] | Klinkenfeder | |
| [7302] | Benzing-Sicherung | |
| 74 | Klinkenrad (4-Teilung) | 11 a |

## B. BILDER

Fig. 1

gibt eine Gesamtansicht der Gerätes, es sind speziell sichtbar:

| | |
|---|---|
| Deckel | 11 |
| Marke | 1101 |
| Deckglas | 1162 mit |
| Sicherungsring | 1163 |

Fig. 2

zeigt das Gerät in Betriebsbereitschaft. Speziell zu erwähnen ist:

| | |
|---|---|
| Antriebsbügel | 71 |
| Einstellring | 1161 |
| Alphabetenring | 11611 |

Fig. 3

Seitenansicht: Zu beachten:

| | |
|---|---|
| Antriebsbügelgriff | 7103 |
| Sperrschieber | 28 |
| Verschlussfederknopf | 1121 |

Fig. 4

Ansicht des Gehäusedeckels mit

| | |
|---|---|
| Rasthebeln | 114 |
| Rasthebelfeder | 1141 |
| Lochkranz | 116101 |
| Verschlussfeder | 112 |

Fig. 5

Gerät offen. Speziell sichtbar:

| | |
|---|---|
| Montageplatte | 2 |
| Umstellzylinder | 3 |
| Stiftradgruppe | 4 |
| Abtastmechanik | 6 |
| Deckel | 11 |
| Grundplatte | 12 |
| Zählerstützen | 25 |
| Zähler | 53 |
| Scharnierstift | 111 |
| Verschlussfederknopf | 1121 |
| Hilfskurbel | 1131 |
| Haltefeder für Hilfskurbel | 113 |

Fig. 6

| | |
|---|---|
| Stiftradgruppe | 4 |
| Bezugslinienstab | 27 |
| Zähler | 53 |
| Gravur für Anschläge | 26 |

| | |
|---|---|
| Stütze | 22 |
| Stiftradhaltefeder | 221 |

Fig. 7

| | |
|---|---|
| Stifträder | 41 |
| (Teilungen 25,26,34,38,42,46) | |
| [Teilungen 29,31,37,41,43,47] | |
| Malteserkreuz | 51 |
| Gehäuse dazu | 23 |
| Führungsstab für Stifträder | 231 |
| Federgehäuse | 21 |
| Stützen | 24 |
| Steg | 211 |
| Dreieckplatte | 242 |
| Stift aktiv | 4111 |
| Stift inaktiv | 4112 |

Fig. 8

| | |
|---|---|
| Montageplatte | 2 |
| Umstellzylinder | 3 |
| Zwischenrad | 52 |
| Zählerritzel | 531 |

Fig. 9

| | |
|---|---|
| Federgehäuse | 21 |
| (6) Zahnscheiben | 31 |
| Anschlag | 313 |
| Hilfskurbel | 1131 |

Fig. 10

| | |
|---|---|
| Hilfskurbel | 1131 |
| Schlitz für Hilfskurbel | 5101 |
| Ablesescheibe | 341 |

Fig. 11 a

Unteransicht Montageplatte

| | |
|---|---|
| Antriebsbügel | 71 |
| Kurvenschlitz | 7102 |
| Sperrschieber | 28 |
| Antriebssegment | 72 |
| Sperrklinke | 711 |
| Winkelhebel | 721 |
| Zugfeder | 7211 |
| Ausgleichshebel | 7212 |
| Zugfeder | 7213 |
| Rastklinke | 73 |
| Klinkenrad (4-Teilung) | 74 |

Fig. 11 b

| | |
|---|---|
| Zahnscheiben (6) | 31 |
| Ablesescheibe | 341 |
| Spannbügel | 61 |
| Abtasthebel (6) | 62 |
| Schraubenfedern | 621 |

Fig. 12

| | |
|---|---|
| Abtasthebel (6) | 62 |
| Anschlag | 313 |
| Klinke | 311 |
| Nase | 3102 |
| Nase | 3401 |

## C. DETAILBESCHREIBUNG

### I) Aufbau

#### 1. Gehäuse

Das Gehäuse [1] besteht aus zwei Hauptteilen, die aus Spritzguss hergestellt, das ganze Gerät umschliessen.

Im Deckel (111) ist der Buchstabenkranz für die Primär-Buchstaben drehbar angeordnet. Es wird durch die beiden Rasthebel (114), die durch die Feder (1141) zusammengezogen werden, in einer der 26 möglichen Lagen festgehalten.

Durch Drehen des Einstellringes (1161) laut Fig. 1 kann der Buchstabenkranz so verdreht werden, dass ein gewählter Buchstabe gegenüber der Marke (1101) zu liegen kommt, dies bestimmt die Relativlage der beiden Alphabete zueinander.

Durch Lösen der Rasthebel (114) nach Fig. 4 wird der Buchstabenkranz freigegeben, der nun abnehmbar ist. In der Regel ist der Kranz mit einem Alphabetenring (11611) ausgerüstet, der die 26 lateinischen Buchstaben in alphabetischer Reihenfolge trägt. Ist er durch einen anderen Ring zu ersetzen, so sind der Sicherungsring (1163) und das Deckglas (1163) zu entfernen, wodurch er freigelegt wird.

In der Grundplatte (12) befindet sich, an vier Punkten befestigt, die Montageplatte (2), auf welcher der genannte Mechanismus befestigt ist.

Der aufklappbare Deckel (11) wird mittels der Verschlussfeder (112) an der Grundplatte festgehalten. Durch Drücken des Knopfes (1121) wird er gelöst.

2. Montageplatte

Auf derselben sind alle mechanisch wesentlichen Teile angeordnet. Durch leichtes Anheben und Wegdrehen der Stiftradhaltefeder (221) werden die Stifträder (41) freigelegt, die nun nach oben abgezogen werden. Durch Lösen der 3 Zylinderschrauben [201] und der Stütze (27) wird hierauf die Montageplatte von der Grundplatte gelöst.

Die übrigen auf der Platte befindlichen Teile sind fest montiert und in der Regel nicht abzunehmen, mit Ausnahme der Ablesescheibe (341), die mit der Nute [342] im Stift [3402] des Alphabetenträgers geführt ist. Durch leichtes Verbiegen kann die Ablesescheibe (341) herausgenommen und durch eine andere ersezt werden.

Die Mechanik gliedert sich auf der Oberseite in drei Hauptteile: Die Vorschubmechanik [5], dargestellt durch das Malteserkreuz (51) in seinem Gehäuse (23). Die Abtastmechanik (6) und der Umstellzylinder (3) mit den 6 Zahnscheiben und der Ablesescheibe (341).

Auf der Unterseite ist die Antriebsmechanik angeordnet, deren Teile anhand der Funktionsbeschreibung erläutert werden.

## II. Funktionen

Anhand der losen Montageplatte, bei abgenommenen Schlüsselrädern sei wie folgt vorgegangen:

Der Sperrschieber (28) wird nach unten geschoben, wodurch der Antriebsbügel freigegeben wird, der unter der Kraft der im Gehäuse (21) sitzenden Feder nach aussen springt. Er kann nun erst wieder hereingedrückt werden, falls er bis zum Anschlag herausgesprungen ist, da die Sperrklinke (711) ein vorzeitiges Betätigen verhindert. Andererseits kann er nur wieder freigegeben werden, wenn er ganz hereingedrückt wurde - was durch die gleiche Sperrklinke (711) überwacht wird.

Beim Betätigen des Antriebsbügels (71) wird einerseits durch die Vorschubklinke [713] das Klinkenrad (74) um 90° verdreht und andererseits das Antriebssegment (72) vollständig nach innen gedreht, wodurch die Schraubenfeder [714] gespannt wird. Die Rastklinke (73) verhindert ein Ueberdrehen des Klinkenrades (74) und hält es gleichzeitig in den Rastlagen fest. Eine dritte Funktion wird durch den im Antriebsbügel befindlichen

Kurvenschlitz (7102) angelöst. Im voll eingedrückten Zustand des Bügels bewirkt eine in besagtem Schlitz laufende Steuerrolle das Anspannen des oberseits angeordneten Spannbügels (61).

Durch diesen Spannbügel werden die Abtasthebel (62) aus dem Bereich der Stiftträder entgegen der Kraft ihrer Schraubenfedern (621) herausgezogen. Die seitliche Staffelung der Bewegungen ist dabei so getroffen, dass die volle $90^{o}$ Verdrehung des Klinkenrades (74) erst erfolgt, wenn diese Hebel weggezogen werden. Dies ist deshalb notwendig, als das mit dem Klinkenrad starr gekoppelte Malteserkreuz (51) die Stiftträder (wenn sie eingesetzt sind) über ihre Ritzel [4121] um eine Teilung weiterdrehen.

Die Rasterung des Klinkenrades (74) ist so getroffen, dass in den "aufgezogenen" Stellungen des Gerätes (Antriebsbügel innen) die Abtasthebel (62) mit ihren Fühlenden stets gegenüber einem Stift der sechs eingesetzten Stiftträder zu liegen kommen.

Bei eingedrücktem Antriebsbügel setze man nun ein beliebiges Stiftrad so ein, dass die Stiftenseite nach unten zu liegen kommt. Es ist darauf zu achten, dass die kippbaren Stifte (4111) und (4112) eindeutig nach innen oder nach aussen schauen und kein Stift senkrecht aus dem Stiftenkranz herausschaut. Man bezeichnet dabei Stifte, die nach aussen gekippt werden als aktiv (4111) und solche, die nach innen liegen, als inaktiv (4112). Man setze das Rad so ein, dass ein aktiver Stift gegenüber dem untersten Abtasthebel (62) zu liegen kommt. Wird nun der Antriebsbügel langsam freigegeben, so bemerkt man, dass nach ca. 10 mm Weg der Spannbügel (61) die Abtasthebel (62) wieder freigibt. Die 5 Hebel (62), die keinem Stiftrad gegenüber stehen, gehen unter Zug der Feder (621) in ihre Grundstellung zurück. Der unterste Hebel, der auf einen aktiven Stift trifft, bleibt jedoch in der gespannten aktiven Lage stehen.

Auf der Unterseite ist zu bemerken, dass der Winkelhebel (721), der in der gespannten Lage voll unter dem Druck des auf dem Antriebsbügel befindlichen Bolzens stand, nun wieder freigegeben

ist und seinerseits die Kraft der Feder [714] auf das Antriebssegment (72) überträgt. Dieses steht über dem Zahnsegment mit dem Ritzel (35) in Eingriff, dass mit dem Umstellzylinder (3) fest gekoppelt ist, dieser hat somit die Tendenz sich unter der Kraft der Feder [714] im Uhrzeigersinn (von oben gesehen) zu verdrehen.

Der totale nun erreichbare Verdrehungswinkel, in Schritteilungen von 1/26 des Kreisumfanges gezählt, ergibt sich nun aus der Stellung des untersten Anschlag (313). Befindet sich dieser z.B. auf der Zahl "1", so bedeutet das: 1 Schritt.

Es ist beim langsamen weiteren Loslassen des Antriebsbügels nun zu beachten, dass der unterste - aktive Abtasthebel mit seinem Rücken die unterste Klinke anhebt. Dadurch wird die Nase der zweituntersten (ersten beweglichen) Zahnscheibe freigegeben, wodurch sich der Zylinder im Uhrzeigersinn weiter dreht, bis die Nase auf den untersten Anschlag auftritt, ein weiteres Freigeben des Antriebsbügels (71) hat nun keine weitere Verdrehung des Umstellzylinders (3) mehr zur Folge.

Wird in der Lage, in der der Antriebsbügel (71) erst teilweise herausgedreht ist, ein weiterer Abtasthebel in die aktive Lage gedrückt, so gibt dieser seinerseits eine Klinke frei, und der Zylinder dreht sich um zusätzliche Schritte weiter, bis die freigegebene Nase ihrerseits auf einen Anschlag auftritt.

Anhand von Fig.12 sei dieses Prinzip näher erläutert, wobei angenommen wird, dass alle drei dargestellten Abtasthebel in aktiver Lage stehen.

Da das Ritzel (35) mit dem Alphabetenträger [34] fest verbunden ist, wird im Gerät, das voll mit Stifträdern bestückt ist, als erstes die oberste Klinke freigegeben, sofern ihr Arm aktiv ist, und die Nase (3401) des Alphabetenträgers [34] wird als erstes auf einen Anschlag treffen. Die totale Umstellbewegung besteht

dann aus soviel Schritten als der Summe der Teilumstellungen entspricht, die sich durch die einzelnen Reiterstellungen bei aktiven Abtasthebeln ergeben.

Es ist theoretisch möglich 6 x 16 = 96 Schritte zu erreichen. Das Gerät CD-57 ist aber nur bemessen, total 40 Schritte zu erzeugen, was bei der Setzung der Anschläge zu berücksichtigen ist.

Aus dem bisher Dargelegten ergibt sich folgendes:

1) Für jeden Operationsschritt werden die Stiftträder (41) um einen Schritt vorgeschoben.

2) Bei jedem Operationsschritt wird der Alphabetenträger gegenüber seiner Grundstellung im Uhrzeigersinn um eine bestimmte Schrittzahl umgestellt. Diese Schrittzahl ist die Summe der Schritte, die bei aktiven Abtasthebeln, sich durch die einzelnen Anschlagstellungen ergeben.

Da jeder der 6 Abtasthebel je nach Stellung des durch ihn abgetasteten Stiftes eine aktive oder eine inaktive Lage einnehmen kann, ergeben sich $2^6$ = 64 Möglichkeiten um 1...40 Schritte in Teilumstellungen von 0...16 Schritten zu erzeugen.

Der Zähler (53) ist über das Zwischenrad (52) so mit dem Ritzel [511] gekuppelt, dass er die Operationsschritte angibt.

In der gespannten Gerätestellung (Antriebsbügel eingedrückt) kann er mittels des Daumens über das Zwischenrad (52) vor- oder rückwärts in eine definitive Zahlstellung verdreht werden.

Sind die sechs Schlüsselräder eingelegt, so wird vorteilhafterweise die Hilfskurbel nach Fig.10 verwendet, die ebenfalls in beiden Drehrichtungen verwendbar ist.

Da in dieser Lage ausserdem das Malteserkreuz (51) ausser

Eingriff zu den Ritzeln [4121] der Stifträder steht, können diese von Hand einzeln ebenfalls verdreht werden. Da sie eine eigene zusätzliche Rasterung besitzen, ist ihre Ruhelage stets eindeutig.

## D. BETRIEB

Das Gerät CD-57 ist in der Regel mit 6 Stifträdern ausgerüstet, die aus dem Angebot der folgenden Teilungen ausgewählt wird: 25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46, 47. Sie tragen am Umfang Buchstaben- und Zahlenmarkierungen wie auch analoge Markierungen bei den Stiften.

Soll das Gerät für Zusammenarbeit mit schreibenden Maschinen eingesetzt werden, so sind 6 bestimmte ausgewählte Räder der Serie nach der Druckschrift 1092 einzusetzen. Im anderen Falle ist die Auswahl frei.

1) Die Räder werden so vor sich hingelegt (Fig.7), dass die Stiftseite oben ist, hierauf werden von Hand, oder mittels der Hilfskurbel die Stifte nach Instruktion in die aktive resp. inaktive Lage gebracht.

2) Die Anschläge (313) werden nach Fig.9 mit der Hilfskurbel in die gewünschte Stellung gebracht indem sie leicht angehoben werden. Man beachte, dass die Summe der erzeugbaren Schrittzahlen 40 nicht überschreitet.

3) Der Antriebsbügel (71) wird eingeschoben und nach Fig.3 mit dem Sperrschieber verriegelt.

4) Der Zähler wird nach Fig.8 in die vereinbarte Stellung gedreht.

5) Die Stifträder (41) werden in der gewünschten Reihenfolge übereinander eingesetzt, Stiftseite nach unten. Man beachte, dass kein Stift aus den Stiftkränzen heraus vorsteht. Hierauf wird nach Fig.6 die Stiftradhaltefeder (221) eingedreht

bis sie auf dem Führungsstab (231) einrastet.

6) Die Stiftträder (41) werden von Hand einzeln verdreht bis am Bezugslinienstab (27) das gewünschte Kennwort (Ausgangsschlüssel) erscheint (in Fig. 6: AAA AAA).

7) Der Deckel (11) wird zugeklappt, nachdem die Hilfskurbel (1131) nach Fig. 5 versorgt wurde.

8) Nach Fig. 1 wird durch Verdrehen des Buchstabenkranzes [116] am Einstellring (1161) die Relativlage eingestellt.

Das Gerät ist nun betriebsbereit.

9) Zum Ver- oder Entschlüsseln wird so vorgegangen, dass der Antriebsbügel (71) freigegeben wird. Hierauf wird er einmal ganz hereingedrückt und wieder herausgelassen. Jetzt wird am Buchstabenkranz [116] der gewünschte Primärbuchstabe gesucht und der ihm entsprechende Sekundärbuchstabe auf der Buchstabenscheibe (341) abgelesen und notiert. Für den zweiten Buchstaben wird der Antriebsbügel (71) einmal voll hereingedrückt und wieder freigelassen, u.s.w.

10) Wird eine weitere Meldung verarbeitet, so erübrigt es sich in der Regel die Stiftträder einzeln neu einzustellen. Man wird mit der Hilfskurbel nach Fig.10 - bei eingedrücktem Antriebsbügel (71) das Gerät auf einen neuen Zählerstand drehen, worauf es für eine neue Meldung bereit ist.

Für weitere Erläuterungen siehe auch Druckschrift 1080.

## E. KRYPTOLOGISCHE GRUNDLAGEN

Wie in I, Seite 3 erwähnt, werden beim Gerät zwei Schlüsseleinstellungen unterschieden:

1) Innere (Grund-) Schlüssel

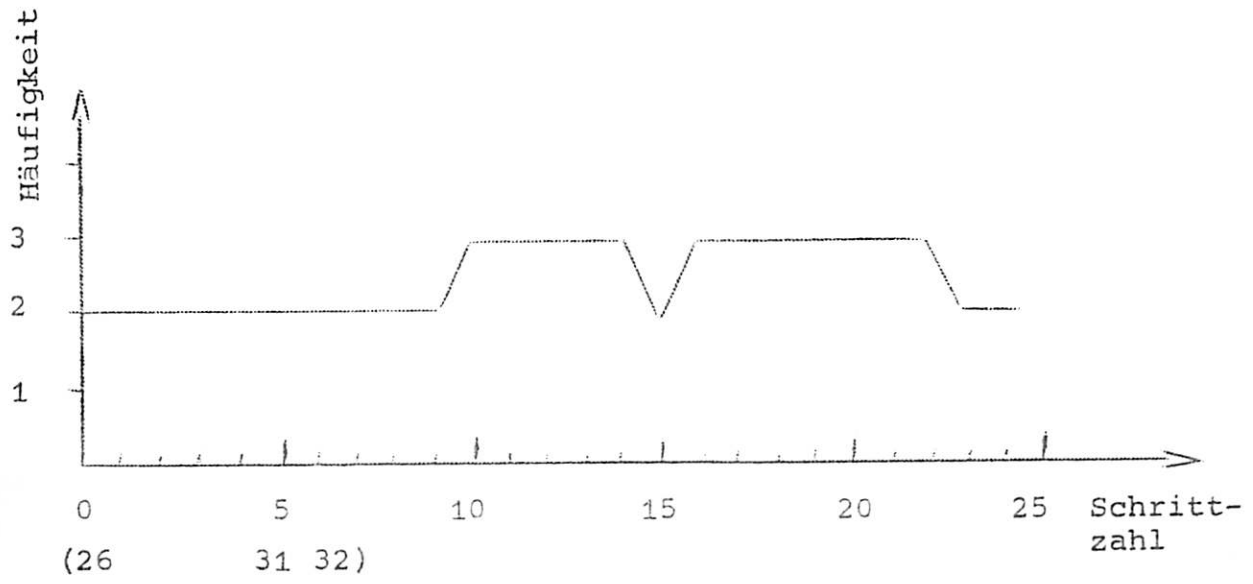
a) Stellung der Anschläge (313)

b) Stellung der Stifte [411]

c) Auswahl und Reihenfolge der Stiftträder (41)

2) Aussere (Ausgangs-) Schlüssel

1 a) Die Einstellung der Anschläge bestimmt die verschiedenen Umstellschrittsummen. Da sechs Anschläge vorliegen, ergeben sich $2^6$ = 64 Kombinationen von wirksamen oder unwirksamen Anschlägen. Wie erwähnt, darf die totale Umstellschrittzahl 40 nicht überschritten werden. Es ist aus kryptologischen Ueberlegungen angezeigt, solche Einstellungen zu suchen, dass eine gleichmässige Verteilung der Schrittzahlen 0...25 (wobei 26...40 als Wiederholung von 1...15 zu werten sind) auf die 64 Möglichkeiten erfolgt. Dies ist aber unmöglich zu erzielen, da die Zahl der Buchstaben im Alphabet kein ganzes Mehrfaches von der Schrittzahl ist. (2 x 26 = 52 + Rest 12 = 64). In der beiliegenden Tabelle I ist ein Beispiel gezeigt, bei dem sich eine sehr gute Verteilung ergibt, die wie folgt aussieht:



Es ist ersichtlich, dass die Umstellschrittzahlen 0...9 und 16 je auf zwei und die Schrittzahlen 10...15 und 17...22 je auf drei verschiedene Arten kombiniert werden können. Es ist aus der Tabelle I auch ersichtlich, dass alle 64 Kombinationen ausgenützt werden.

In der Regel ist es nicht möglich rein rechnerisch eine gute Einstellung zu finden. Man wird vorteilhafterweise die verschiedenen Kombinationen tabellarisch darstellen und kontrollieren.

1b) Pro Rad ergeben sich, da jeder Stift zwei Lagen einnehmen kann, $2^n$ Einstellungen, wenn n die Schrittzahl eines Rades darstellt. Unter Annahme der üblicherweise verwendeten Räder 29, 31, 37, 41, 43 und 47 ergeben sich ein Total von $29 + 31 + 37 + 41 + 43 + 47 = 2^{228} = 4{,}2 \times 10^{68}$ Kombinationsmöglichkeiten. Es ist nun aber zu berücksichtigen, dass in der Regel zwischen 40 und 60 % der Stifte eines Rades aktiv sein soll. Ebenso sollten höchstens 5 Stifte hintereinander die gleiche Lage haben. Unter Berücksichtigung dieser Einschränkungen ergeben sich aber immer noch ca $10^{15}$ praktische Möglichkeiten.

1c) Alle 12 Räder könnten in ca $6{,}8 \times 10^7$ Kombinationen eingesetzt werden. Da aber nur 6 Räder gleichzeitig verwendet werden, ergeben sich rund $6 \times 10^5$ Möglichkeiten die Räder einzusetzen.

Die Ausgangslage der Räder ist - an und für sich - wie aus dem bisher gesagten hervorgeht, für die Abklärungen der Möglichkeiten ohne Belang. Die Ausgangslage ändert ja mit jedem Schritt, und bei den erwähnten Rädern 29, 31, 37, 41, 43 und 47 ergibt sich nach einer Periode von rund $2{,}8 \times 10^9$ Schritten wieder die gleiche Stellung.

Für den praktischen Einsatz sind die verschiedenen Ausgangs-

stellungen weiter nicht wahllos festzulegen, da sie u.U. zufällige Stellungen einer früheren Schrittfolge darstellen könnten. Z.B. wird die Ausgangslage IKLMNO als schlecht zu betrachten sein, wenn bei einer vorherigen Meldung ABCDEF eingestellt wurde, da diese ja nach 8 Schritten mit der gewählten identisch ist; mit anderen Worten die beiden Schlüsselserien sind nach 8 Schritten genau gleich, was für die Sicherheit sehr schädlich ist, da ein potentieller Gegner hier sofort einhaken kann.

Das Taschengerät wird in der Regel für die Verarbeitung von Kurzmeldungen bis zu je max. 300 Buchstaben eingesetzt. Wenn die Ausgangsschlüssel festgelegt werden, so soll, beim lediglichen Verstellen des Zählers mindestens stets die nächste ungefähre 1000er Stellung für eine neue Meldung gewählt werden. Wenn die neuen Schlüssel in Form eines Kennwortes festgelegt werden, so sollen sie so errechnet werden, dass sie innerhalb ca 1000 Schritten einer früheren Meldung nicht vorkommen.

2 Die Relativlageneinstellung bietet 26 Möglichkeiten. Sie ist lediglich als Verschleierungszusatz zu betrachten und kryptologisch ohne grössere Bedeutung.

Zusammenfassend kann gesagt werden, dass das Gerät den Anforderungen entspricht, wenn die erläuterten Gesichtspunkte beachtet werden und wenn Meldungen von ca 300 Zeichen als Norm angesehen werden. Die inneren Elemente sind dann lediglich ca alle 2...3 Wochen zu wechseln.

Dezember 1963
OSt/iz

Beilagen: 12 Figuren
1 Tabelle

Tabelle I

I 1088-b

**Beispiel:**

| Platz No. | Anschlag auf |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 4 |
| 4 | 7 |
| 5 | 8 |
| 6 | 10 |

Dies ergibt ein Total von 32 Umstellschritten. Die einzelnen Schrittsummen (total 64 Kombinationen) ergeben sich wie folgt:

Einzeldarstellung

| Kombination der Auslösungen | Schrittzahl | Kombination der Auslösungen | Schrittzahl |
|---|---|---|---|
| 0 | 0 | 6 | 10 |
| 1 | 1 | 16 | 11 |
| 2 | 2 | 26 | 12 |
| 12 | 3 | 126 | 13 |
| 3 | 4 | 36 | 14 |
| 13 | 5 | 136 | 15 |
| 23 | 6 | 236 | 16 |
| 123 | 7 | 1236 | 17 |
| 4 | 7 | 46 | 17 |
| 14 | 8 | 146 | 18 |
| 24 | 9 | 246 | 19 |
| 34 | 11 | 346 | 21 |
| 124 | 10 | 1246 | 20 |
| 134 | 12 | 1346 | 22 |
| 234 | 13 | 2346 | 23 |
| 1234 | 14 | 12346 | 24 |
| 5 | 8 | 56 | 18 |
| 15 | 9 | 156 | 19 |
| 25 | 10 | 256 | 20 |
| 35 | 12 | 356 | 22 |
| 45 | 15 | 456 | 25 |
| 125 | 11 | 1256 | 21 |
| 135 | 13 | 1356 | 23 |
| 145 | 16 | 1456 | 26 |
| 235 | 14 | 2356 | 27 |
| 245 | 17 | 2456 | 27 |
| 345 | 19 | 3456 | 29 |
| 1235 | 15 | 12356 | 25 |
| 1245 | 18 | 12456 | 28 |
| 1345 | 20 | 13456 | 30 |
| 2345 | 21 | 23456 | 31 |
| 12345 | 22 | 123456 | 32 |

tabellarische Darstellung

| Einzel Schrittzahl | Platz 1 | 2 | 3 | 4 | 5 | 6 | Häufigkeit d. Schrittzahl |
|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 4 | 7 | 8 | 10 | |
| 0 | 0 | 0 | | | | | | 2 |
| 1 | 1 | | 1 | | | | | 2 |
| 2 | 2 | | | 2 | | | | 2 |
| 3 | 3 | | | 3 | | | | 2 |
| 4 | 4 | | | | 4 | | | 2 |
| 5 | 5 | | | | 5 | | | 2 |
| 6 | 6 | | | | 6 | | | 2 |
| 7 | 7 | | | | 7 | 7 | | 2 |
| 7 | 8 | | | | 8 | 8 | | 2 |
| 7 | 9 | | | | 9 | 9 | | 2 |
| 7 | 10 | | | | 10 | 10 | 10 | 3 |
| 7 | 11 | | | | 11 | 11 | 11 | 3 |
| 7 | 12 | | | | 12 | 12 | 12 | 3 |
| 7 | 13 | | | | 13 | 13 | 13 | 3 |
| 7 | 14 | | | | 14 | 14 | 14 | 3 |
| 8 | 15 | | | | | 15 | 15 | 3 |
| 8 | 16 | | | | | 16 | 16 | 3 |
| 8 | 17 | | | | | 17 | 17 | 3 |
| 8 | 18 | | | | | 18 | 18 | 3 |
| 8 | 19 | | | | | 19 | 19 | 3 |
| 8 | 20 | | | | | 20 | 20 | 3 |
| 8 | 21 | | | | | 21 | 21 | 3 |
| 8 | 22 | | | | | 22 | 22 | 3 |
| 10 | 23 | | | | | | 23 | 2 |
| 10 | 24 | | | | | | 24 | 2 |
| 10 | 25 | | | | | | 25 | 2 |
| 10 | 26 | | | | | | 0 | |
| 10 | 27 | | | | | | 1 | |
| 10 | 28 | | | | | | 2 | |
| 10 | 29 | | | | | | 3 | |
| 10 | 30 | | | | | | 4 | |
| 10 | 31 | | | | | | 5 | |
| 10 | 32 | | | | | | 6 | |
| | | | | | | | | 64 |