HAGELIN-CRYPTOS

CD-57

.176

HAGELIN · CRYPTOS

CRYPTO AG
ZUG
Switzerland

POCKET CRYPTOGRAPHER TYPE CD-57

Operation Instructions

Introduction

The machine CD-57 has been designed for needs of extreme portability where the direct printing of the texts can be dispensed with.
The ciphers obtained with this machine are of the double substitution type, and mechanically produced.
Twelfe different key wheels are available, of which six are used in the machine, where they can be placed in any desired sequence. Depending on the key wheels to be used, key series from about 700 000 000 to about 6 000 000 000 signs will be obtained. With a judicious use of the settings

ENGLISH

FRANCAIS

DEUTSCH

ESPANOL

(as indicated below) and with the observation of normal precautions, the ciphers produced with the CD-57 machines will be of a very high class. Key wheels with the following number of divisions and pins are available: 25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46 and 47. Every individual pin can be placed either in active or inactive position.

The stepping mechanism, which consists of six displacement disks, each acted by one of the six key wheels in use, translates the action from the active pins in key wheels into a displacement of the alphabet disk. Each one of the six disks is provided with a moveable lug, and the position of the lug determines the number of steps which the corresponding key wheel will cause the alphabet disk to be displaced. There are 17 positions provided for the lugs giving steps from 0 to 16. When arranging the lugs in their (different) positions, the choice of positions should be such as to depending which key wheels have pins in an active position, all 26 displacement steps should be obtainable. As the maximum number of steps is limited to 40, it must also be observed that the sum of the lug settings should be less or equal to this number.

A large number of suitable lug combinations is possible, and the following could serve as an example:
The lug in the disk No.1 in position: 1, in No.2 position: 2, in No.3 position: 4, in No.4 position: 8, in No.5 position: 10 and in disk No.6 position: 15. When all 6 key wheels are active at the same time, the maximum of 40 steps will be obtained, i.e. the alphabet disk will make not only a complete turn (26 steps) but 14 additional steps.
When all key wheels are inactive, there will be 0 step.
In the above example, the 64 possible combinations will allow all the steps from 0 to 40, some of them by 2 or 3 different combinations. The possibility of having such a large number of 40 steps is cryptographically of high value.
The ciphering (enciphering and deciphering) is done by reading from the letter to be ciphered on the stationary alphabet ring (2) to the corresponding letter on the moveable alphabet disk (3) inside the ring. This will be the enciphered or deciphered letter.
At each operation the stepping mechanism acts on the alphabet disk and displaces this disk (3) to one of the 26 pos-

sible positions relative to the alphabet ring (2).

Operating instructions

I. Preparation

To establish correspondence between two or more points, the machines used must have the same key settings. These settings are basic settings, which remain in use for a certain amount of time and operational settings, which have to be different for every message ciphered.
The basic settings consist of: The choice of key wheels, the arrangement of their pins, the order in which the key wheels are put into the machine, the position of the lugs in displacement disks. An additional basic setting could be the use of different alphabet rings.
The operational settings consist of: The initial or starting position of the key wheels and the position of the alphabet ring.
The basic settings can be effected only with the machine opened. Be sure that the operating lever (1) is locked in its inner or closed position, before attempting to open the machine. To open, turn the knurled knob (81) at the top of the machine (see

fig. 2). (Some models have a knob to be pushed in.)

a) Key wheels

Turn the counter (7) to zero forward or backward by introducing the crank (8) into the hole (13). Be sure that the operating lever (1) is locked in its inner position. The key wheels are then taken out in the following way:
First pull the holding spring (51) gently up, and swing it away (see fig.3) Then turn the machine upside down, and let the key wheels fall into the palm of your hand. The six key wheels are now put on to the desk with the side showing the pins, up (see fig. 3). To arrange the pins correctly, a list has to be used. Following the instructions, the pins are turned over with their longer end either outwards, which is the active position, or inwards where they are inactive. This can be done either by using a fingernail or the back of the crank (8). Be sure that the pins are put into their final positions. Once done so, replace the six key wheels, pin-side down one by one in the sequence agreed upon. (It is adviced to turn the wheels before they are pushed down completely to the initial

position, where the letters or figures agreed upon on the crown will register with the index (58)]. Make sure that the key wheels can be rotated freely, in either direction. Return the holding spring (51) to its closed position.

b) Displacement disks

Now the lugs (31) on the displacement disks are arranged in accordance with the instructions. Use the slotted end of the crank (8) to lift the respective lugs (31) gently out of their present positions and move them over one by one to the notches corresponding with the numbers (32) indicated (fig. 4).

c) Alphabets

If different alphabets are used, and the alphabet ring has to be replaced, remove same in the following way:
First hold your fingers over the protecting glass (82) and push this off, from inside the lid of the machine, then take off the alphabet ring (2). Replace the alphabet ring according to instruction and snap on the glass.
Close the machine, unless it is to be used immediately after making the basic settings. The machine is now

ready for use, but for the ciphering of every single message, the operational settings have to be made in accordance with agreement between the correspondents.

II. Operation

Turn the crown with alphabet ring (2) until the letter agreed upon registers with the red mark. Turn the counter (7) to the initial position number agreed upon as per paragraph a before, be sure that the operating lever (1) is in its locked position–[or turn the key wheels, until the letters or figures on the crown of the key wheels agreed upon will register with the index (58). When doing this, be sure that the operating lever (1) is in its closed position)]. Ciphering can now begin.
The machine is best held in the left hand, as shown in fig. 1. Release the operating lever (1) by sliding the catch (12) downwards and allow the lever to move outwards as far as possible. To operate the machine, push the operating lever (1) inwards with the thumb and release again. After each operation the letter to be ciphered is read on the outer alphabet ring (2) and the corresponding enciphered or de-

ciphered letter on the moveable inner disk (3) is written down or transmitted directly by phone or radio. The same procedure is used both for enciphering and deciphering. The letter to be treated will always be seeked on the outer alphabet ring and the ciphered letter (when enciphering) or the clear letter (when deciphering) will be found on the inner moveable alphabet disk. Please note that when no inverse alphabets are used, ciphering will be done from the disk to the ring and deciphering from the ring to the disk.
The counter will show the number of letters registered. If for any reason a repetition is needed, or an enciphered message is to be checked before transmission, the starting position or any desired place in the message can easily be obtained by using the crank (8) and moving it in the return direction until the counter (7) shows the desired place in the message. [Do this with the lever (1) in the locked position.]

Weight and dimensions

Width: 3¼" (80 mm), Length: $5^1/_8$" (135 mm), Thickness: 1½" (40 mm), Weight with 6 keywheels: about 23 ounces (650 grams).

Illustrations

Fig. 1: shows the machine in the hand of the operator with the operating lever (1) in its outer (released) position, ready for use. In the position shown, the letter C on the alphabet ring (2) will correspond with the ciphered letter H which is to be read on the disk (3), or the letter U corresponds with P. When the machine is not in use, the lever (1) is pushed in and the catch (12), which is seen beneath the lever, is pushed upwards so that it will lock the lever.

Legend:
(1) Operating lever
(2) Alphabet ring
(3) Alphabet disk
(12) Catch
(13) Crank hole

Fig. 2: shows the machine with the lid open. The following main parts are shown:

(1) Operating lever
(3) Alphabet disk on top of the stepping mechanism
(5) Key wheels mounted on the central bearing (9)
(6) Control lever assembly
(7) Counter
(8) Crank

(51) Holding spring for the key wheels
(58) Reference bar for the starting position of key wheels
(81) Knob to open the lid
(82) Protecting glass

The small crank (8) visible in the lid is used:

a) to turn the key wheels forward or backward to the desired position. This position is marked by the counter.

b) to move the lugs on the stepping mechanism.

Fig. 3: shows the machine with the lid open and with the key wheels (5) placed upside down in the foreground. It will be recognized that the key wheels consist of two main parts: A crown (55) carrying the pins and a center (52) marked with the number of pins of the key wheel. In this center is a gear for the advancement of the key wheel. The central bearing (9) is hollow and inside is a modified maltese cross with four driving vanes. When the operating lever (1) is pushed inwards, the cross makes one fourth of a revolution and a vane acts on the gears in the key wheel centers, advancing all the key wheels by one step.

A connecting gear wheel (11) between the central bearing and the counter will advance the counter by one unit for each operation.

Legend:
(5) Key wheels
(9) Central bearing
(10) Drining cross
(11) Connecting gear wheel for counter
(51) Holding spring for key wheels
(52) Key wheel center
(53) Active pin
(54) Inactive pin
(55) Key wheel crown

Fig.4 shows how to arrange the lugs (31):
(31) Lugs
(32) Reference number for the lugs

Special instructions to be given

Basic settings

Choice of key wheels, arrangement of the pins and sequence of the key wheels.
Arrangement of the lugs.
Alphabet ring (eventually).

Operational settings

Initial positions for the key wheels.
Position of the alphabet ring.

HAGELIN · CRYPTOS

CRYPTO AG
ZUG
Suisse

CRYPTOGRAPHE DE POCHE TYPE CD-57

Instructions d'emploi

Le cryptographe de poche CD-57 est prévu pour les emplois qui exigent un petit appareil léger et qui peuvent renoncer au texte sous forme imprimée.
Du point de vue cryptologique, l'appareil fonctionne selon le principe du déplacement irrégulier de l'alphabet, en formant la clé mécaniquement.
Parmi 12 roues-clés différentes qui sont à disposition, on peut choisir librement 6 roues-clés pour les mettre dans l'appareil. Selon le choix des roues-clés, on peut produire des séries de clé avec des périodes allant de 7×10^8 jusqu'à 6×10^9 pas d'avancement.

FRANCAIS

DEUTSCH

ESPANOL

Une grande sécurité du message secret peut donc être obtenue si la mise à la clé (voir plus bas) est faite soigneusement.
Les roues-clés sont livrables dans les 12 divisions suivantes: 25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46 et 47. Six roues-clés sont compris dans le prix de la machine. Ces roues-clés sont munies d'ergots de commande, dont chacun peut être mis dans une position active ou inactive. Le nombre de ces ergots est égal au nombre de la division de la roue-clé.
L'influence des ergots actifs de chaque roue-clé est transformée sur un système d'avancement pour produire le chiffre. On peut obtenir de 0 jusqu'à 16 pas d'avancement par chaque roue-clé, mais le nombre total des pas d'avancement ne devra jamais dépasser 40. Beaucoup de combinaisons sont possibles, par exemple: La roue-clé n° 1 produira 1 pas, n° 2:2, n° 3:4, n° 4:8, n° 5:10 et n° 6:15 pas, donc en total 40 pas.
Si toutes les roues-clés ont un ergot actif dans un certain cycle d'opération, on aura alors en total 40 pas. Le disque-alphabet fait alors un tour complet (26 pas) et 14 pas supplémentaires. Si toutes les roues-clés ont un ergot inactif dans un cycle d'opération on n'aura aucun pas d'avance-

ment. Dans ce cas le disque-alphabet ne se déplacera pas.
On a 64 possibilitées pour produire le nombre de pas d'avancement. Il est evident que tous les nombres entre 0 et 40 peuvent être produits et il est important de savoir qu'un certain nombre de pas d'avancement peut souvent être obtenu par plusieurs combinaisons, ce qui est un grand avantage du point de vue cryptologique.
Pour traiter un texte (chiffrer ou déchiffrer) on doit lire lettre par lettre sur l'anneau-alphabet immobile extérieur. La lettre qui se trouve juste en face sur le disque-alphabet mobile est la lettre chiffrée ou déchiffrée.
Le système d'avancement agit sur le disque mobile de la manière que ce dernier puisse prendre une des 26 positions relatives avec l'anneau-alphabet. Pour chaque cycle d'opération la probabilité est soit-disant égale pour toutes les 26 positions relatives et elle dépend de la mise à la clé interne.

Mode d'emploi

I. – Préparatifs

Avant de la mise en service, tous les appareils qui doivent collaborer entre eux, doi-

vent être mis à la même clé de base, c. à d. les différents éléments de clé doivent être mis en positions identiques.
Les éléments de la clé de base sont: Les ergots des roues-clés, le choix des 6 roues-clés, leur suite et position dans l'appareil et enfin la mise des ergots (butées) pour le nombre de pas que chaque roue-clé pourra produire au système d'avancement, et le choix éventuel des alphabets.

On procédera comme suit:

a) Roues-clés

1° Tourner le compteur à zéro, en introduisant la manivelle (8) dans le trou (13) du palier central (9). Veillez à ce que le levier de commande (1) soit en position fermée.
2° Ouvrir l'appareil en tournant le bouton (81) du couvercle (fig. 2). (A certain modèles on pressera sur le bouton.)
3° Lever légèrement et détourner le levier (51) qui retient les roues-clés (fig. 3).
4° Renverser l'appareil et laisser tomber les roues-clés dans la main ou bien enlever ces roues une à une.
5° Mettre les 6 roues-clés sur une table, le côté des ergots en haut (voir fig. 3).

6° Poser les ergots en position active ou inactive selon instructions spéciales. Cela se fait par l'ongle d'un doigt ou bien avec la partie postérieure de la manivelle (8). Veillez à ce que tous les ergots soient bien placés, c'est-à-dire en position active ou inactive et qu'aucun ergot ne soit en position intermédiaire.

7° Remettre les 6 roues-clés dans l'appareil, une à une, dans la suite précise par les instructions spéciales. On fait glisser les roues-clés sur le palier central (9), le côte des ergots vers le bas. Avant de les enfoncer on les tourne jusqu'à ce que la lettre de départ prévue pour la prochaine opération se trouve tout près de la barre de repère (58) (fig2). (Il sera plus difficile de tourner les roues-clés quand elles sont toutes introduites dans l'appareil.»

8° Contrôler que toutes les 6 roues-clés soient bien placées et puissent bien jouer. Veillez à ce qu'aucun ergot ne soit en position intermédiaire. Refermer ensuite le levier (51) retenant les roues-clés (fig 2).

b) Mécanisme d'avancement

Pur déplacer les ergots du système

d'avancement (31) on les lève légèrement avec la fente postérieure de la manivelle (8). On commence par l'ergot le plus bas et on le met en face de l'encoche numérotée (32) qui a été préscrite par les instructions spéciales (fig. 4). Il est à observer que le total des numéros d'encoches employés ne devra jamais dépasser le nombre de 40. Si on place deux ergots sur la même encoche, il faut la compter deux fois, car ce numéro sera contacté par deux roues.

c) Alphabets

(Si des alphabets doivent être échangés)

1° Tenir la main sur le verre de protection (82).

2° Pousser le verre de protection en dehors par l'indice de l'autre main.

3° Enlever l'anneau-alphabet (2) et échanger le selon instructions spéciales.

4° Remettre l'anneau-alphabet.

5° Remettre le verre de protection et vérifier qu'il soit bien retenu par les deux billes.

II. – Mise en service

Les appareils sont maintenant dans leur position de base. Pour chaque message

on doit mettre les éléments-clés dans une autre position de départ. Cela se fait de la manière suivante:

1° Tourner l'anneau-alphabet extérieur (2) dans une des 26 positions de façon que la lettre relative préscrite dans les instructions spéciales se trouve en face de la marque rouge.

2° A l'appareil fermé [le levier de commande (1) enclenché, position fermée], mettre la manivelle (8) dans le trou (13) et tourner la manivelle jusqu'à ce que le compteur se trouve dans la position de départ indiquée par les instructions spéciales. [A la barre (58) on pourra repérer alors le «code» de départ.]

3° Remettre la manivelle (8) dans le couvercle comme indiqué dans la fig. 2.

Pour l'opération on prend l'appareil dans la main gauche comme indiqué dans la fig. 1. En glissant la petite targette d'arrêt (12) qui se trouve à côté du levier (1), ce dernier sera libéré et sautera en dehors. Ce levier est à enfoncer et à relâcher, ce qui fait une opération de l'appareil.

Après chaque opération la lettre à traiter doit être lue sur l'anneau-alphabet extérieur (2) et la lettre correspondante qui se trouve juste en face sur le disque-alphabet intérieur (3) doit être notée à la

main ou bien sur une machine à écrire ou on peut aussi la transmettre directement par téléphone ou radio.
Pour le chiffrement et pour le déchiffrement le procédé est identique, c'est-à-dire on cherchera toujours la lettre à traiter sur l'anneau-alphabet extérieur et la lettre chiffrée (pour le chiffrement) ou la lettre déchiffrée (pour le déchiffrement) se trouve sur le disque-alphabet mobile. (En cas oû l'on emploira des alphabets non inverses on chiffrera de centre vers l'anneau et on déchiffrera de l'anneau vers le centre.)

Poids et dimensions
Largeur: 80 mm, longueur: 135 mm, épaisseur: 40 mm. Poids de l'appareil avec 6 roues-clés environ 650 g.

Illustrations
Fig.1: Cette vue montre l'appareil dans la main gauche d'un opérateur. Le levier de commande (1) se trouve en position extérieure, donc prêt pour l'opération.
Dans la position présentée, la lettre «B» de l'anneau extérieur (2) sera donc remplacée par la lettre chiffrée «I» qui peut être lue sur le disque intérieur (3) ou bien la lettre «U» donnera comme lettre chiffrée un «P».

Si l'appareil n'est pas employé, on pousse le levier (1) vers l'intérieur et on le fixe en glissant la petite targette d'arrêt (12) qui se trouve à côté de ce levier.

Légende:
(1) levier de commande
(2) anneau-alphabet
(3) disque-alphabet mobile
(12) targette d'arrêt
(13) trou pour la manivelle

Fig. 2: Ici le couvercle de l'appareil est ouvert. On voit:

(1) levier de commande
(3) disque-alphabet
(5) roues-clés
(6) groupe des leviers de commande
(7) compteur
(8) manivelle
(51) levier (pour retenir les roues-clés)
(58) barre de repère pour l'indication de la position de départ des roues-clés
(81) bouton pour ouvrir le couvercle
(82) verre de protection

La manivelle (8) visible dans le couvercle sert à:

a) tourner le méchanisme d'avancement jusqu'à la position désirée. Cette position est marquée par le compteur.
b) poser les ergots (31) du système d'avancement.

Fig. 3: Montre également l'appareil ouvert. Les roues-clés (5) sont enlevées et renversées, le côté des ergots vers le haut. On reconnait que la roue-clé est composée de deux parties:
a) d'une couronne (55) qui porte des ergots et
b) d'un disque interne (52) qui reste immobile et qui porte le numéro de sa division. Au centre de ce disque se trouve le pignon d'entraînement de la roue-clé.

Le palier central (9) est creux et on y voit la croix de Malte (10) pour l'entraînement des roues-clés. La croix de Malte a 4 dents d'entraînement qui avancent les roues-clés par les pignons. Par chaque opération du levier de commande (1) la croix de Malte est avancée d'un quart de tour. Une roue dentée (11) avance le compteur d'une unité après chaque opération.

Légende: (5) roues-clés
(9) palier central
(10) croix de Malte pour l'entraînement

(11) roue dentée pour le compteur
(51) levier pour retenir les roues-clés
(52) disque interne de la roue-clé
(53) ergot actif
(54) ergot inactif
(55) couronne de la roue-clé

Fig. 4: Sur cette illustration on voit comment on doit procéder pour déplacer les arrêts du système d'avancement.
(31) ergot du système d'avancement
(32) encoche numérotée

Instructions spéciales

Position de base

Ergots, choix et suite des roues-clés, position des arrêts du système d'avancement. (Eventuellement: anneau-alphabet.)

Position de départ

Numéro du compteur («code» de départ des roues-clés).
Lettre de repère sur la marque rouge.

HAGELIN · CRYPTOS

CRYPTO AG
ZUG
Schweiz

TASCHENCHIFFRIERGERÄT
CD-57

Gebrauchsanleitung

Das Taschengerät Typ CD-57 wurde für jene Anwendungsgebiete entwickelt, bei denen in erster Linie ein kleines, handliches Gerät verlangt wird und wo auf den Schlüsseltext in gedruckter Form verzichtet werden kann.
Das Gerät arbeitet kryptologisch nach dem Prinzip der unregelmässigen Alphabetverschiebung, mit rein mechanischer Schlüsselbildung.
Es stehen Schlüsselräder mit 12 verschiedenen Teilungen zur Verfügung, wovon 6 nach beliebiger Wahl in das Gerät eingesetzt werden. Je nach Wahl dieser Schlüsselräder können Schlüsselperioden von

DEUTSCH

ESPANOL

7×10^8 bis 6×10^9 Schriften entstehen. Bei einer vernünftigen Einstellung des Schriftmechanismus (siehe unten) wird daher eine sehr grosse Sicherheit des verschlüsselten Textes gewährleistet. Die Schlüsselräder sind in folgenden Teilungen lieferbar: 25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46 und 47. Sie sind mit Fühlerstiften versehen, die einzeln in aktive oder inaktive Lage gestellt werden können, wobei die Anzahl der Stifte im Schlüsselrad seiner Zahnteilung entspricht.

Der Schriftschaltmechanismus, der durch die Schlüsselräder beeinflusst wird, übersetzt den Einfluss der aktiven Stifte in eine Schrittzahl von 0 bis 16 Schritten pro Rad. Es ist jedoch zu beachten, dass die maximale Schrittzahl bei diesem Gerät auf 40 beschränkt ist. Diese Zahl kann sich zum Beispiel wie folgt zusammensetzen: Schlüsselrad 1 erzeugt 1 Schritt, Nr. 2: 2, Nr. 3: 4, Nf. 4: 8, Nr. 5: 10 und Nr. 6: 15 Schritte.

Wenn in einem Arbeitsmoment alle 6 Stifträder aktive Stifte aufweisen, so wird hier also die Schrittzahl 40 betragen. Die Alphabetenscheibe macht eine volle Umdrehung [26 Schritte] und noch 14 zusätzliche Schritte dazu. Wenn alle Schlüsselräder in einem Arbeitsmoment inaktive

Stifte tragen, so wird die Schrittzahl 0 sein, das heisst, die Alphabetenscheibe bewegt sich überhaupt nicht.
Die erzeugbaren 64 verschiedenen Möglichkeiten ergeben hier also sämtliche Schrittzahlen von 0 bis 40, wobei wichtig ist, dass einige Schrittzahlen durch verschiedene Kombinationen erreichbar sind.
Die hohe Zahl von 40 möglichen Fortschaltschritten für die Alphabetenscheibe ist kryptologisch von sehr grossem Vorteil.
Beim Verarbeiten von Texten (verschlüsseln oder entschlüsseln) wird Buchstabe um Buchstabe auf dem stillstehenden äusseren Alphabetenring abgelesen. Der jeweilen einem Buchstaben gegenüberliegende Buchstabe auf der inneren, sich drehenden Scheibe, ist der Schlüsselbuchstabe bzw. der Klarbuchstabe.
Der Schrittschaltmechanismus arbeitet auf die innere Alphabetenscheibe, dass diese nach jedem Arbeitszyklus eine der 26 Relativlagen gegenüber dem äusseren Alphabetenring einnehmen kann.

Gebrauch des Gerätes

I. Vorbereitung

Zuerst sind die Geräte, die zusammen arbeiten sollen, auf gleiche Schlüssel-

grundlagen einzustellen, das heisst, es müssen die Schlüsselelemente auf gleiche Ausgangs- und Einstellagen gesetzt werden. Diese umfassen die Stifte in den Schlüsselrädern, die Auswahl der Schlüsselräder und die Reihenfolge, in der diese in die Geräte einzusetzen sind, ausserdem die Schrittzahleinstellung beim Schrittschaltmechanismus und die Wahl der Alphabete.
Es wird hierzu wie folgt vorgegangen:

a) Schlüsselräder

1. Zähler vor- oder rückwärts auf Null drehen durch Einführen der Kurbel (8) in das Loch (13) des Hauptlagers (9). Der Bedienungshebel (1) muss dabei in eingeschobener, eingerasteter Stellung stehen (Fig. 1).
2. Gerät offen durch Drehen des Knopfes (81) am Deckel. (Bei gewissen Geräten ist der Knopf zu drücken.) (Fig. 2).
3. Bügel (51) leicht anheben und herausdrehen (Fig. 3).
4. Gerät wenden und die Schlüsselräder in die Hand fallen lassen, eventuell leicht nachhelfen.
5. Schlüsselräder mit Stiften nach oben auf Tisch oder ebene Fläche legen (Fig. 3).

6. Stifte mit Fingernagel oder hinterem Ende der Hilfskurbel (8) nach Sondervorschrift einstellen. Darauf achten, dass alle Stifte sauber nach innen oder aussen gekippt sind.
7. Räder in Reihenfolge der Sondervorschrift, mit Stiftenseite nach unten in das Gerät einsetzen. Dabei wird jedes Rad, sobald es über das zentrale Hauptlager gestülpt ist, von Hand vor- oder rückwärts rastend verdreht, bis beim Stab (58) der Kennbuchstabe der Ausgangslage nach Sondervorschrift erscheint. Das Verdrehen der Räder ist so leichter, als wenn es erst durchgeführt würde, wenn alle Räder eingesetzt sind.
8. Räder kontrollieren auf sauberen Sitz und eventuell vorstehende Stifte, hierauf Bügel (51) schliessen (Fig. 2).

b) Umstellmechanismus

Mit dem hinteren Schlitz der Hilfskurbel wird der unterste Anschlag (31) leicht angehoben und in diejenige Kerbe gedreht, die über der, nach Sondervorschrift angegebenen Einstellzahl (32) liegt (Fig. 4). Hierauf wird der zweitunterste Anschlag eingestellt usw.

Es ist zu beachten, dass die Summe der Zahlen, die diesen Einstellungen zugeordnet sind, nie 40 überschreitet. (Wenn zwei Anschläge auf die gleiche Zeit fallen, so ist diese doppelt zu rechnen. Jeder Anschlag ist einer Zahl zugeordnet.)

c) Alphabete

(Falls andere Ringe verwendet werden.)

1. Hohle Hand über Uhrenglas (82) halten
2. Mit dem Zeigefinger von innen her das Uhrenglas herausdrücken
3. Alphabetenring (2) herausheben und nach Sondervorschrift austauschen
4. Ring einsetzen
5. Uhrenglas einsetzen und einrasten

II. Betrieb

Die Geräte sind nun in der Grundstellung. Für jede Meldung wird eine neue Ausgangslage festgelegt und wie folgt vorgegangen:

1. Alphabetenring (2) rastend verdrehen, bis Kennbuchstabe nach Sondervorschrift bei roter Marke steht.
2. Mit Hilfskurbel (8) bei geschlossenem Gerät und eingeschobenem, verriegeltem Bedienungshebel (1) durch Loch (13) hindurch Mechanismus verdrehen,

bis Zählerstand nach Sondervorschrift erreicht ist. [Beim Stab (58) ist dann das sogenannte Schlüsselwort erkennbar, das unter Umständen an Stelle des Zählerstandes dienen kann.]

3. Kurbel (8) versorgen (Fig. 2).

Zu Beginn wird das Gerät in die linke Hand genommen und der Bedienungshebel (1) [welcher zuerst durch Verschieben des kleinen Riegels (12) freigegeben werden soll] mit dem Daumen nach innen gedrückt und wieder freigelassen (Fig. 1). Nach jeder Operation wird der zu verarbeitende Buchstabe auf dem äusseren Alphabetenring (2) gesucht und der ihm gegenüberliegende Buchstabe auf der inneren Alphabetenscheibe (3) notiert. Das Notieren kann von Hand oder mit einer Schreibmaschine erfolgen, es ist auch direkte Durchgabe im Fernsprecher oder Funkgerät denkbar. Genau wie beim Verschlüsseln wird auch beim Entschlüsseln vorgegangen, wenn die beiden Alphabete in umgekehrter Anordnung vorliegen. (Sofern Ring oder Scheibe mit nicht inverser Buchstabenfolge verwendet werden, ist für das Verschlüsseln von innen nach aussen abzulesen, und für das Entschlüsseln von aussen nach innen.)

Gewicht und Abmessungen

Breite: 80 mm, Länge: 135 mm, Dicke: 40 mm. Gewicht des Gerätes mit 6 Schlüsselrädern zirka 650 g.

Abbildungen

Fig. 1: Zeigt das Gerät in der linken Hand der Bedienungsperson, wobei der Bedienungshebel (1) in der äusseren, freigelassenen Lage dargestellt wird. Das Gerät trägt hier einen äusseren Alphabetenring (2) mit geordnetem, lateinischem Alphabet. In dieser Stellung würde zum Beispiel der Buchstabe «B» auf dem äusseren Alphabetenring (2) durch den Geheimbuchstaben «I» ersetzt, der auf der inneren Alphabetenscheibe (3) abgelesen wird.
Wenn das Gerät nicht im Gebrauch ist, wird der Bedienungshebel (1) nach innen gedrückt und der kleine Riegel (12), welcher links unterhalb des Hebels im Gehäuse sichtbar ist, vorgeschoben.

Legende:
(1) Bedienungshebel
(2) Alphabetenring mit geordnetem Alphabet
(3) Innere Alphabetenscheibe
(12) Halteriegel
(13) Kurbelloch

Fig. 2: Zeigt das Gerät mit geöffnetem Gehäusedeckel. Es sind folgende Teile sichtbar:

(1) Bedienungshebel
(3) Alphabetenscheibe (über dem Schrittschaltmechanismus)
(5) Schlüsselräder auf einer zentralen Lageranordnung montiert
(6) Steuerhebelgruppe
(7) Zähler
(8) Hilfskurbel
(51) Haltebügel
(58) Bezugsmarke
(81) Verschlussknopf
(82) Uhrenglas

Die im Deckel sichbare Hilfskurbel (8) wird verwendet:

a) um die Schlüsselräder in eine bestimmte Ausgangslage zu kurbeln, wobei der Zähler als Merkzeichen verwendet wird;

b) um die Anschläge (Reiter) (31) auf dem Schrittschaltmechanismus in die gewünschte Stellung zu bringen.

Fig. 3: Zeigt ebenfalls die geöffnete Maschine. Die Schlüsselräder (5) sind herausgenommen und umgekehrt dargestellt.

Bei diesen ist ersichtlich, dass sie aus zwei Untergruppen bestehen:

a) einem äusseren Ring (55), der die Stifte trägt;

b) einer inneren feststehenden Scheibe (52), welche als Bezeichnungsnummer die Teilungszahl trägt, und die im Inneren ein Ritzel besitzt, welches für den Antrieb der Schlüsselräder dient.

Das zentrale Hauptlager (9) ist hohl und besitzt eine Öffnung, durch die das darin liegende Hochkant-Malteserkreuz (10) sichtbar wird. Dieses besitzt 4 Antriebszähne, welche die Schlüsselradscheiben über die Ritzel antreiben. Wenn der Betätigungshebel (1) hineingedrückt wird, wird jeweils das Malteserkreuz um eine Viertelsumdrehung weitergedreht.
Ein Übertragungszahnrad (11) liegt zwischen der Zentralwelle und dem Zähler, der für jede Operation um eine Einheit weiterdreht.

Legende:
(5) Schlüsselräder
(9) Zentrales Hauptlager
(10) Antriebs-Malteserkreuz
(11) Übertragungszahnrad
(51) Haltebügel
(52) Schlüsselradscheibe

(53) Aktiver Stift
(54) Inaktiver Stift
(55) Schlüsselradring

Fig. 4: Zeigt das Vorgehen beim Einstellen der Anschläge (31) des Umstellmechanismus und die festen Einstellzahlen (32).

Einstellungen nach Sondervorschrift

Grundeinstellungen

Auswahl und Reihenfolge der Schlüsselräder, Lage der Stifte, Anschläge
Alphabet auf Ring (eventuell)

Sprucheinstellungen

Schlüsselwort (Zählerstand)
Kennbuchstabe – rote Marke

CRYPTO AG
ZUG
Suiza

CRIPTOGRAFO DE BOLSILLO TIPO CD-57

Instrucciones para el uso

El criptógrafo de bolsillo CD-57 ha sido creado para casos que exigen el empleo de un aparato ligero y en los que se puede renunciar al texto escrito.
Desde el punto de vista criptológico, el aparato funciona según el principio de desplazamiento irregular del alfabeto, formando la clave mecánicamente.
Entre las 12 ruedas claves diferentes a disposición se pueden escoger libremente 6 de ellas para meterlas en el aparato. Según las claves escogidas, se pueden producir series de clave con períodos de 7×10^8 hasta 6×10^9 pasos de avance. Se puede, pues, obtener una gran seguridad del mensaje secreto si la puesta en clave se ha efectuado cuidadosamente. (Ver más abajo).

ESPANOL

Las ruedas claves son disponibles en las 12 distintas divisiones siguientes: 25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46 y 47. Seis ruedas claves están incluídas en el precio de la máquina.

Estas ruedas claves están provistas de espuelas de mando que pueden ser colocadas en posición activa o pasiva. El numero de espuelas es igual al número de división de la rueda clave.

La influencia de estas espuelas activas de cada rueda clave es transformada sobre un sistema de avance para producir la cifra. Se pueden obtener de 0 a 16 pasos de avance por rueda clave, pero el número total de pasos no ha de superar los 40. Son posibles muchas combinaciones: la rueda núm. 1, producirá 1 paso; la núm.2, 2 pasos; la núm.3, 4; la núm.4, 8; la núm.5, 10 y la núm. 6, 15. Total, 40 pasos.

Si todas las ruedas claves tienen una espuela activa en cierto ciclo de operación, se tendrán en total 40 pasos. El disco-alfabeto dará una vuelta completa (26 pasos) y 14 pasos suplementarios. Si todas las ruedas claves tienen una espuela pasiva en un ciclo de operaciones, no se tendrá ningún avance. En este caso el disco-alfabeto no se desplazará.

Existen 64 posibilidades para producir un número de pasos de avance. Es evidente que pueden ser introducidos todos los números entre 0 y 40, y es importante saber que cierto número de pasos de avance puede a menudo ser obtenido por medio de varias combinaciones, lo que significa una ventaja desde el punto de vista criptográfico.
Para tratar un texto (cifrar o descifrar) se debe leer letra por letra sobre el anillo-alfabeto fijo exterior La letra que se encuentra justo enfrente sobre el disco-alfabeto móvil es la cifrada o descifrada. El sistema de avance actúa sobre el disco móvil de manera que este último pueda tomar una de las 26 posiciones relativas con el anillo-alfabeto. En cada ciclo de operación, la probabilidad es prácticamente igual para las 26 posiciones relativas, y depende de la colocación de la clave interna.

Modo de empleo

I. Preparativos

Antes de poner en funcionamientes el aparato, todos los elementos que deben colaborar entre sí han de estar en la misma clave, es decir, los elementos de clave

diferentes deben ser colocados en claves iguales.
Los elementos de clave básicos son: las espuelas da las ruedas, la elección de las seis ruedas claves, su orden y posición en el aparato, y, por fin, la colocación de las espuelas para el número de pasos que cada rueda clave podrá producir en el sistema de avance, y la elección eventual de los alfabetos.

Se procederá como sigue:

a) Ruedas claves

1. Girar el contador a 0, introduciendo la manivela (8) en el agujero (13) del cojinete central (9). Cuídese de que la manivela de mando (1) esté en posición cerrada.
2. Abrir el aparato, girando el botón (81) de la tapa (fig. 2). En ciertos modelos hay que apretar el botón.
3. Levantar ligeramente y volver la palanca (51) que retiene las ruedas claves fig. 3).
4. Voltear el aparato y dejar caer las seis ruedas en la mano, o sacarlas una a una.
5. Colocar las seis ruedas sobre una mesa, con la cara de las espuelas hacia arriba (véase fig. 3).

6. Colocar las espuelas en posición activa o pasiva, según instrucciones especiales. Esto se lleva a cabo con la uña de un dedo o con la parte posterior de la palanca (8). Cuídese de que todas las espuelas estén debidamente colocadas, es decir, en posición activa o pasiva. Ninguna ha de estar en posición intermedia.
7. Volver a poner las seis ruedas en el aparato, una a una, según el orden precisado en las instrucciones especiales. Se hace resbalar las ruedas sobre el cojinete central (9), el lado de las espuelas hacia abajo. Antes de encajarlas, gírese hasta que la letra de comienzo prevista para la próxima operación se encuentre junto a la barra de referencia (58), (fig. 2). (Será más difícil girar las ruedas si se encuentran ya dentro del aparato.)
8. Comprobar que las seis ruedas claves estén bien colocadas y pueden girar bien. Cuídese de que ninguna espuela esté en posición intermedia. Cerrar seguidamente la palanca (51), que retiene las ruedas claves (fig. 2).

b) Mecanismo de avance

Para desplazar las espuelas del sistema de avance (31), se las alza ligeramente

con la hendidura posterior de la manivela (8). Se comienza por la espuela más baja y se la pone frente a la hendidura numerada (32) que ha sido prescrita por las instrucciones especiales (fig. 4). Obsérvese que el número de hendiduras a emplear no debe pasar de 40. Si se colocan dos espuelas sobre la misma hendidura hay que contar dos veces, ya que ese número será tocado por dos ruedas.

c) Alfabetos

(si hay que cambiarlos)

1. Poner la mano sobre el cristal de protección (82).
2. Empujar el cristal de protección hacia atrás con el índice de la otra mano.
3. Quitar el anillo-alfabeto (2) y colocarlo según las instrucciones especiales.
4. Volver a colocar el anillo-alfabeto.
5. Volver a colocar el cristal de protección y verificar si está debidamente sostenido por las dos cuñas.

II. Puesta en servicio

Los aparatos están ahora en su posición base. Para cada mensaje, los elementos claves deben colocarse de manera distinta. Esto se realiza de la siguiente manera:

1. Girar el anillo-alfabeto exterior (2) en una de las 26 posiciones, de modo que la letra relativa prescrita en las instrucciones se encuentre frente a la marca roja.
2. Al aparato cerrado [la manivela de mando (1) está introducida, posición cerrada] se la aplica la palanca (8) en el agujero (13) y se gira esta palanca hasta que el contador se encuentre en la posición señalada en las instrucciones especiales. [En la barra (58) se podrá señalar el «código» de partida.]
3. Volver a colocar la palanca (8) en la tapa como indica la fig. 2.

Para ello se coge el aparato con la mano izquierda como indica la fig. 1. Resbalando el cerrojillo de contención (12), que se encuentra al lado de la manivela (1), se librará esta y saltará hacia atrás. Hay que apretar otra vez esta manivela y soltarla de nuevo, lo que constituye una función del aparato.

Después de cada operación se verá la letra a tratar en el anillo-alfabeto exterior (2), y la letra correspondiente que se encuentra frente a ella en el disco alfabeto interior (3) debe ser anotada o puede ser transmitida por teléfono o radio.

Para el cifrado y descifrado se procede de la misma manera, es decir: se busca siem-

pre la letra a tratar en el anillo-alfabeto exterior y la letra cifrada y descifrada aparecerá en el disco móvil.

Peso y dimensiones

Anchura: 80 mm. Longitud: 135 mm. Espesor: 40 mm. Peso del aparato con seis ruedas claves, aprox. 650 grs.

Ilustraciones

Fig. 1: Esta figura muestra el aparato en la mano izquierda de un operador. La manivela de mando (1) se encuentra en posición exterior, presta a la operación.
En la posición presentada, la letra «B» del anillo exterior (2) será reemplazada por la cifrada «I», que se ve en el disco interior (3), o bien, la «U» daría la letra cifrada «P».
Si el aparato no se utiliza, se aprieta la palanca (1) hacia adentro y se la fija corriendo el cerrojo de contención (12) que se encuentra al lado.

Leyenda:
(1) Manivela (o palanca) de mando
(2) Anillo-alfabeto
(3) Disco-alfabeto móvil
(12) Cerrojo de contención
(13) Agujero para la palanca

Fig. 2: Aquí se ha abierto la tapa del aparato. Se ve:

(1) Palanca de mando
(3) Disco-alfabeto
(5) Ruedas claves
(6) Grupo de palancas de mando
(7) Contador
(8) Manivela
(51) Palanca (para sujetar las ruedas claves)
(58) Barra de referencia para la posición de partida de las ruedas claves
(81) Botón para abrir la tapa
(82) Cristal de protección

La palanca (8) visible en la tapa sirve para:

a) Girar el mecanismo de avance hasta alcanzar la posición deseada. Esta posición viene marcada por el contador.
b) Colocar las espuelas (31) del sistema de avance.

Fig. 3: Muestra asimismo el aparato abierto. Las ruedas claves (5) se han quitado y dado vuelta, el lado de las espuelas hacia arriba. Se ve que la rueda clave está compuesta de dos partes:

a) Una corona (55) que lleva las espuelas y

b) Un disco interno (52) que queda inmóvil y que lleva el número de división. En el centro de este disco se encuentra el piñón de engranaje de la rueda clave.

El cojinete central (9) es cóncavo y en él se encuentra la Cruz de Malta (10) para el engranaje de las ruedas claves. La Cruz de Malta tiene cuatro dientes de engranaje, los cuales, por medio de los piñones, hacen avanzar las ruedas claves. Por cada operación de la palanca de mando (1), la Cruz de Malta avanza un cuarto de vuelta. Una rueda dentada (11) avanza el contador en una unidad después de cada operación.

Leyenda:
(5) Ruedas claves
(9) Cojinete central
(10) Cruz de Malta para el engranaje
(11) Rueda dentada para el contador
(51) Palanca para retener las ruedas claves
(52) Disco interno de la rueda clave
(53) Espuela activa
(54) Espuela pasiva
(55) Corona de la rueda clave

Fig. 4: En esta ilustración se ve cómo se debe proceder para desplazar las piezas de detención del sistema de avance.

(31) Espuela del sistema de avance
(32) Muesca numerada (hendidura)

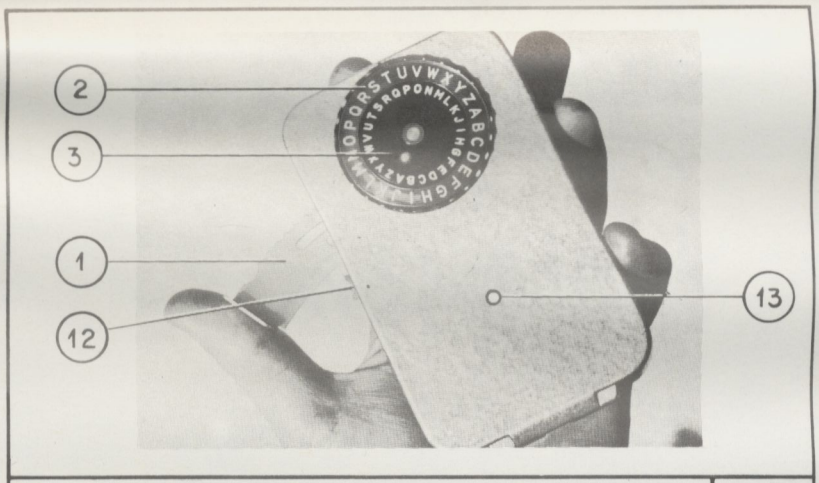
Instrucciones especiales

Posición base:

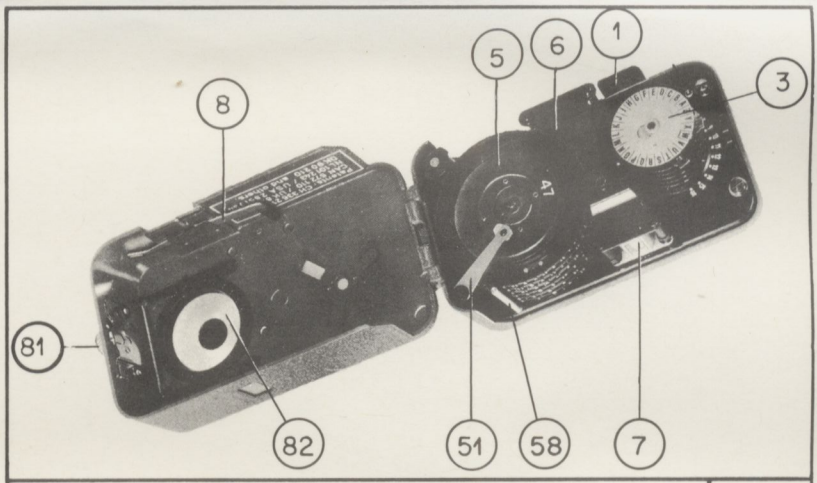
Espuelas, elección y ordenación de las ruedas claves, puesta de las piezas de paro del sistema de avance (a veces anillo-alfabeto).

Posición de partida:

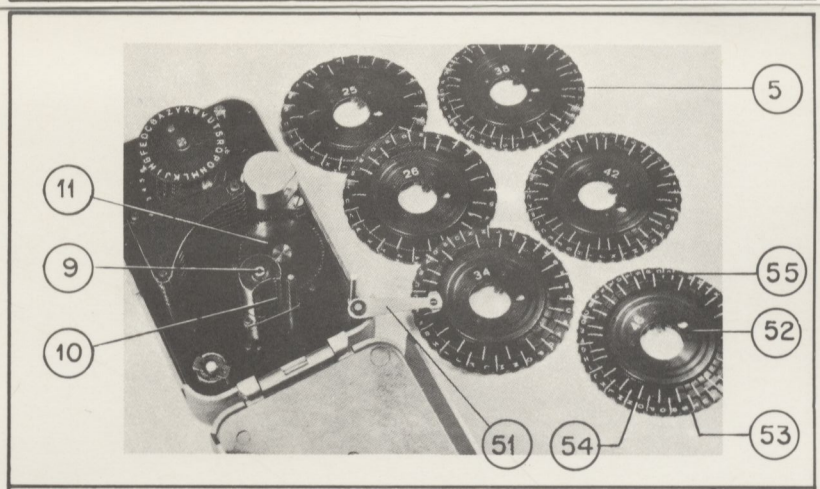
Número del contador («código de partida de las ruedas claves).
Letra de referencia sobre la marca roja.



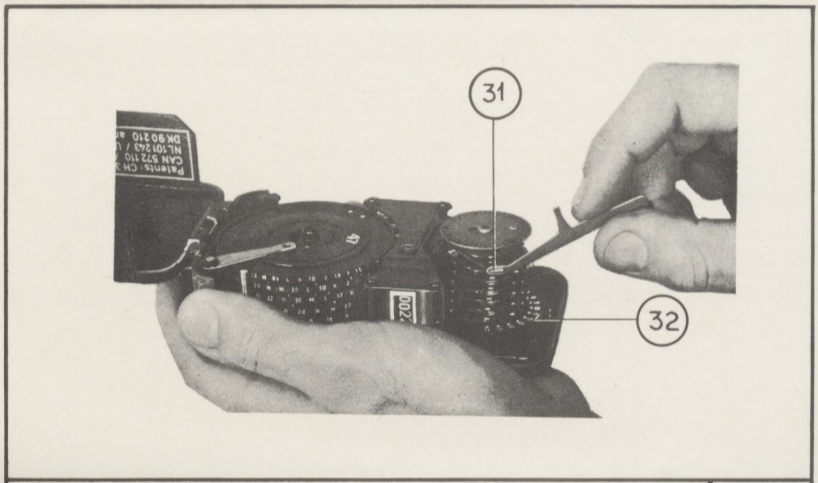
Taschengerät Pocket machine Machine de poche | Fig. 1



Taschengerät Pocket machine Machine de poche | Fig. 2



Taschengerät Pocket machine Machine de poche | Fig. 3



Taschengerät Pocket machine Machine de poche | Fig. 4