

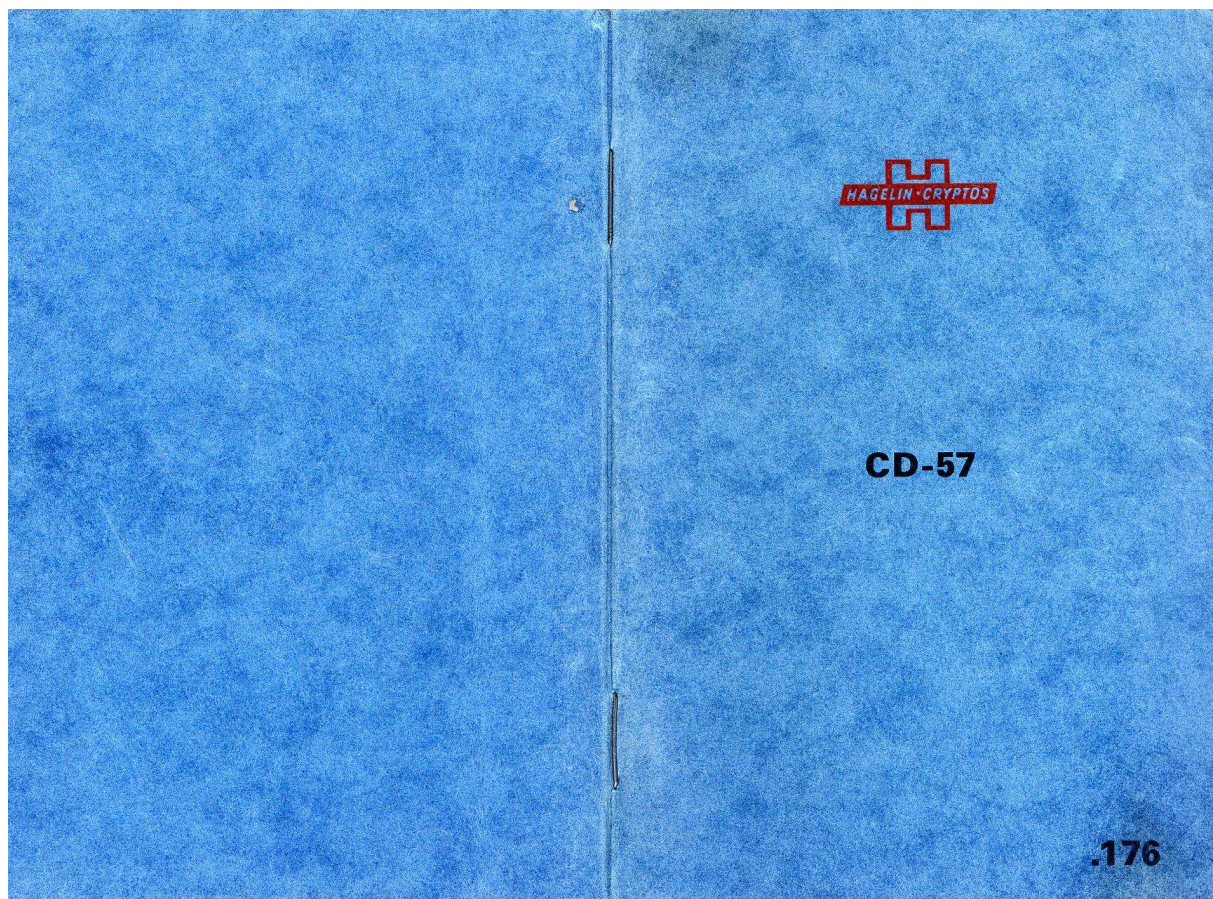
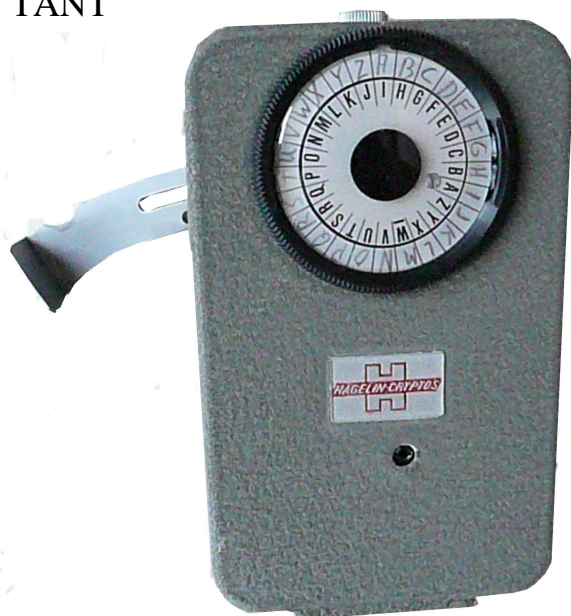


## Manuel de la CD57

Par Daniel TANT

Un problème pour le collectionneur consiste à trouver les manuels d'utilisation des machines à chiffrer, car souvent les machines se vendent seules.

Voici donc en reproduction dans les pages ci-après la copie du texte en français du manuel fourni d'ordinaire avec la machine CD57.







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  $7 \times 10^8$  jusqu'à  $6 \times 10^9$  pas d'avancement.

FRANCAIS

DEUTSCH

ESPAÑOL

14

2176

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-

2176

15

ment. Dans ce cas le disque-alphabet ne se déplacera pas.

On a 64 possibilités pour produire le nombre de pas d'avancement. Il est évident 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-

DEUTSCH

ESPAÑOL



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° Renserver 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 côté 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

DEUTSCH

ESPAÑOL

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 prescrite 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 prescrite 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

DEUTSCH

ESPAÑOL



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 où l'on emploiera 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 mécanisme 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 reconnaît 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

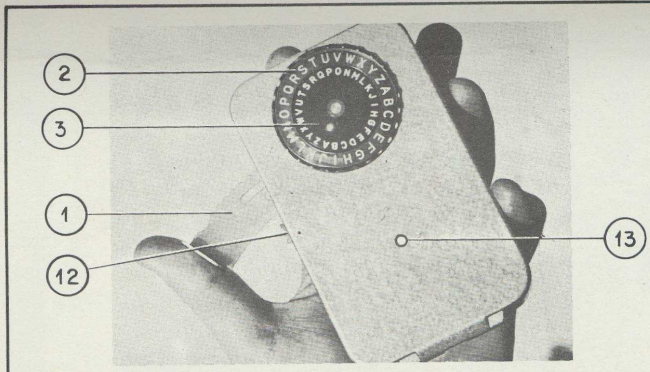
Ergots, choix et suite des roues-clés, position des arrêts du système d'avancement. (Eventuellement: anneau-alphabet.)

##### Position de départ

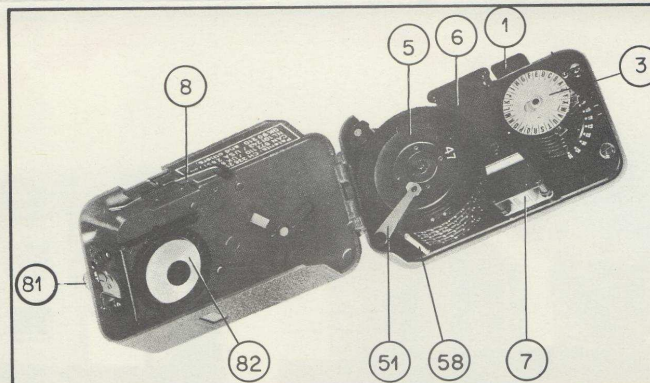
Numéro du compteur («code» de départ des roues-clés).

Lettre de repère sur la marque rouge.

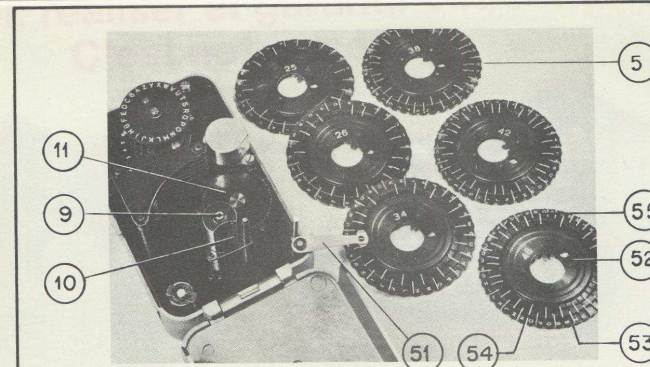




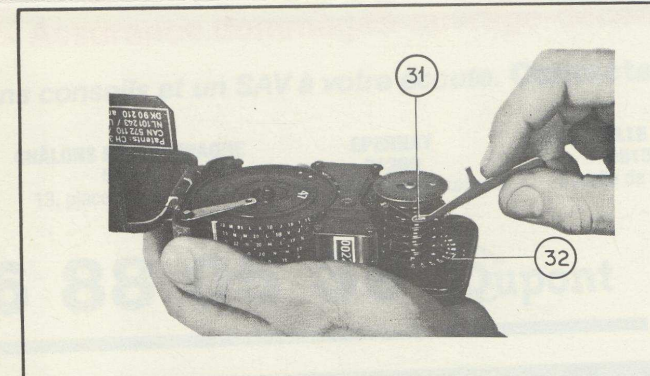
Taschengerät Pocket machine Machine de poche Fig. 1



Taschengerät Pocket machine Machine de poche Fig. 2



Taschengerät Pocket machine Machine de poche Fig. 3



Taschengerät Pocket machine Machine de poche Fig. 4