HAGELIN-CRYPTOS
CRYPTO AG

No. 3088 B

POCKET CRYPTOGRAPHER TYPE CD-57

TECHNICAL DESCRIPTION

Postadresse 6301 Zug/Schweiz, Postfach
Adresse postale 6301 Zug/Suisse, Case postale
Post address 6301 Zug/Switzerland, P.O.Box

Telefon
Téléphone (042) 38 15 44
Phone

Telegramme
Télégrammes CRYPTO ZUG
Cables

Telex 78 702
Domizil: Steinhausen-Zug
Zugerstrasse 42

HAGELIN-CRYPTOS
CRYPTO AG

POCKET CRYPTOGRAPHER TYPE CD-57

TECHNICAL DESCRIPTION

Table of contents — Page

POCKET CRYPTOGRAPHER TYPE CD-57

Technical Description

A. FOREWORD

The growing demand for ciphering machines of reduced dimensions has led to the development of the type CD-57 pocket cryptographer. This machine is recommended for such cases, where the need for small dimensions is paramount and where direct printing of the message can be dispensed with.

In comparison with existing small of miniature ciphering machines the CD-57 offers superior security. Where printing machines of our manufacture type C-machines are also used, there exists the possibility of correspondence which should be advantageous from an organizational point of view.

The cryptological functions of the CD-57 machines are in principle the same as those of the C-4 and C-52 machines. The construction, however, differs rather extensively, with resulting reduced dimensions.

The main characteristics of the pocket machines are:

1. Small dimensions 130 x 80 x 36 mm (5 1/8" x 3 1/8" x 1 1/2") and small weight 680 g (1 1/2 lbs).

2. The same machine is used for both ciphering and deciphering.

3. Speed: As there is no printing mechanism the signs to be ciphered do not have to be indicated, the reading of the ciphered letters is direct, and can be noted down by hand, or even be dictated directly into the telephone or to the teleprinter. Operating speeds of 30 to 40 signs per minute can be obtained.

B. DEFINITIONS

The special expressions, used to explain the cryptographical functions of the CD-57 machine, are defined as follows:

1. Enciphering and deciphering. These operations are, seen while machine functions, identical. When such operations of the machine are mentioned, they will always be called ciphering, in order to avoid the repetitious use of the expression "enciphering" or "deciphering", unless specifically described.

2. Primary and secondary. As the enciphering and deciphering operations are identical, it has been found convenient to use the words "primary" and "secondary", in connection with the texts, letters and alphabets used, instead of "clear" and "cipher", as f.i. the alphabet used to encipher from is also used to decipher from, and vice versa. Therefore, texts, letters and the alphabet on which these are indicated, are primary, both when enciphering or deciphering and the alphabet on which the result is found and also the resultant texts and its letters are secondary.

3. Inverse alphabets. The alphabets on the alphabet ring and the alphabet disk are normally arranged in such manner that the letters on the ring are in their normal alphabetical order, when read clockwise, while the letters on the disk run counterclockwise; this arrangement is called "inverse alphabets" and offers the practical advantage that both, enciphering and deciphering can always be done from the ring to the disk.

It should be noted that any other sequence of letters, where the one used on the ring and that on the disk runs in opposite directions, falls under the definition of "inverse alphabets".

4. Displacement and stepping. The ciphering operation is based on causing the alphabet disk to change its position relative to the alphabet ring. When, as normally, the alphabet consists of 26 letters, the disk can take 26 different positions. The change in position is called displacement, and the number of steps made during a ciphering operation is called displacement steps. The series of displacement which follows one after another, for the ciphering of a message,is called displacement series, or substitution series. As the character of the displacement series is defined by the arrangement of the key wheels, it may in some contexts also be called key series. The key wheels are also subjected to a displacement for each operation, with one step for each key wheel. We call this movement, in order to distinguish it from movement of the alphabet disk, stepping.

5. Keys. The machine contains a number of variable elements, which have to be set according to instructions prepared by those responsible for the cipher service. Each setting corresponds to a specific key for the element in question. Setting all the variable elements according to specified instructions corresponds to the "keying" of the machine. The purpose of the specific key is:

a) to enable the machine to produce a cipher of the highest possible qulity.

b) to permit correspondence between two or more users and

c) to set those elements, whose positions will change during the ciphering operation (the key wheels) into the positions, specified for the ciphering of a given message. These must be set before the ciphering of every separate message.
We call the two first mentioned settings: basic keys, and the keys for the starting positions: initial keys.

Basic keys. These compris the folowing elements:

a) The arrangement of the stops on the displacement disks.

b) The choice of the key wheels to be used, the arrangement of the pins in the pin disks and the sequence in which they are placed in the machine.

c) The position of the alphabet ring, as defined by the letter to register with the index on the lid of the machine.

Initial keys. These normally comprise the starting position for the key wheels, as defined by the index letters on their crowns, to register with the index pin in the machine.

Note: There is in practice no sharply defined difference between the basic and the initial keys, as in some cases some or all of the above mentioned basic settings are set anew for every separate message. The positioning of the alphabet ring, although by definition a basic key, will in practice be treated as an initial one, as it is easy to change and can be set without opening the lid of the mechanism.

C. CONSTRUCTION AND MAIN PARTS

The complete mechanism of the machine is mounted on a pressed steel platen, which is fastened with four screws in the machine housing. This and the lid are of a die-cast aluminum alloy. The machine consists of the following main parts:

Housing and lid with alphabet ring	Group No. 1
Mounting plate	" " 2
Stepping mechanism	" " 3
Group of key wheels	" " 4
Stepping mechanism	" " 5
Sensing mechanism	" " 6
Driving system	" " 7

In the following list the numbers in the ( ) brackets are not shown on the figures, but their component parts. The numbers with only one figure refer to the group number, whereas the numbers with two figures refer to the component parts of the groups, and the numbers with 3 and 4 figures refer to the subelements. The first number always indicates the number of the group to which the piece in question belongs. The list is not complete (and can therefore not be used to order the spare parts, for which a separate catalog is provided) and only those parts are mentioned which are necessary to understand the functioning of the machine.

No	Part	to see in fig.
(1)	Housing	1, 5
11	Lid	1, 5
1101	Index	1
111	Hinge pin	5
112	Lock spring	4
1121	Lock spring knob	3, 5
113	Crank holder	5
1131	Crank	5, 9, 10
114	Positioning lever for alphabet ring	4
1141	Positioning lever spring	4
(116)	Alphabet ring assembly	2
1161	Positioning ring (or crown)	2
116101	Positioning holes	4
11611	Alphabet ring	2
1162	Protecting glass	1
1163	Locking ring for protecting glass	1
12	Bottom plate	5
2	Mounting plate	5, 8
(201)	3 Cylinder head screws	
21	Spring housing	7, 9
211	Spring holder	7
(212)	Benzing clip	
22	Support	6
221	Holding spring for key wheels	6
23	Housing for Maltese cross	7
231	Guide pin for key wheels	7

No	Part	To see in fig.
24	3Supporte	7
(241)	3 Benzing clips	
242	Triangular cover plate	7
25	2 Counter supports	5
(251)	Cylinder head screw	
26	Reference numbers for positioning lugs	6
27	Reference bar (or grid)	6
28	Catch	3, 11
(281)	Flat spring	
(282)	Pin	
3	Stepping mechanism	5, 8
31	Notched displacement disks	9, 11
3102	Stop	12
311	Catch	12
(312)	Catch spring	
313	Lug	9, 12
(32)	Benzing clip	
(33)	Shaft	
(34)	Alphabet ring (carrying alphabet disk)	12
3401	Stop	12
(3402)	Pin	
341	Alphabet disk	10,11,12
(342)	Groove	
35	Pinion	11
(351)	Guide disk	
(352)	Benzing clip	
4	Key wheels (group of 6)	5, 6
41	Key wheels	7
(411)	Pin crown	
4111	Pin active	7
4112	Pin inactive	7
(412)	Disk bearing	
(4121)	Pinion	
(4122)	Detent	
(4123)	Detent spring	
5)	Advancement mechanism	
51	Maltese cross	7
5101	Slit for crank	10
(511)	Pinion	
52	Intermediate gear wheel	8
53	Counter	5, 6
531	Counter pinion	8

No	Part	to see in fig.
6	Sensing mechanism	5
61	Cradle lever	11
611	Guide roller	11
62	Sensing lever	11,12
621	Helicoidal springs	11
(7)	Driving system	
71	Operating lever	2,11
(7101)	Sectorslit	
7102	Curved slit	11
7103	Pusher	3
710	Ratchet segment	11
711	Ratchet lever	11
(7111)	Ratchet spring (detent spring)	
(713)	Feed lever	
(7131)	Lever spring	
(714)	Spiral spring	
72	Drive segment	11
7201	Gear segment	11
(7202)	Stop	
721	Lever	11
7211	Return spring	11
7212	Auxiliary lever	11
7213	" spring	11
(7203)	Benzing clip	
73	Ratchet (detent)	11
(7301)	Ratchet spring	
(7302)	Benzing clip	
74	Ratchet disk (four teeth)	11

D. ILLUSTRATIONS

Fig. 1
is a general view of the machine, specially visible are:

Lid	11
Index	1101
Protecting glass	1162
Locking ring	1163

Fig. 2
shows the machine ready for use:

Operating lever	71
Positioning ring	1161
Alphabet ring	11611

Fig. 3

Slide view:

Pusher	7103
Catch	28
Lock spring knob	1121

Fig. 4

View of the lid with:

Positioning lever	114
Positioning lever spring	1141
Positioning holes	116101
Lock spring	112

Fig. 5

Machine with opened lid:

Mounting plate	2
Stepping mechanism	3
Key wheels (group of 6)	4
Sensing mechanism	6
Lid	11
Bottom	12
Counter support	25
Counter	53
Hinge pin	111
Lock spring knob	1121
Auxiliary lever	1131
Crank holder	113

Fig. 6

Key wheels (group of 6)	4
Reference bar (or grid)	27
Counter	53
Reference numbers for lug positioning	26
Support	22
Holding spring for key wheels	221

Fig. 7

Key wheels (divisions:)	41
25,26,34,38,42,46,	(25/46)
29,31,37,41,43,47,	(29/47)
Maltese cross	51
Housing for Maltese cross	23
Guide pin for key wheels	231
Spring housing	21
Supports	24
Spring holder	211
Triangular cover plate	242
Pin active	4111
Pin inactive	4112

Fig. 8

Mounting plate	2
Displacement disk ass.	3
Intermediate gear eheel	52
Counter pinion	531

Fig. 9

Spring housing	21
Notched disk displacement	31
Lug	313
Crank	1131

Fig. 10

Crank	1131
Maltese cross slit	5101
Alphabet disk	341

Fig. 11a

Bottom view of the mounting plate

Operating lever	71
Curved slit	7102
Catch	28
Drive segment	72
Ratchet	711
Lever	721

Return spring	7211
Ratchet	73
Ratchet disk	74
Auxiliary lever	7212
Auxiliary spring	7213

Fig. 11b

Top view of the mounting plate

Notched disk displacement	31
Alphabet ring	341
Cradle lever	61
Sensing lever	62
Helicoidal springs	621

Fig.12

Sensing lever	62
Lug	313
Catch	311
Stop	3102
Stop	3401

E. GENERAL DESCRIPTION

1) Housing. The housing (1) consists of two parts, of diecast aluminum alloy, inside which the complete machine is mounted.In the lid (11) the alphabet ring assembly (116) is placed. It is held by the two positioning levers (114), which press against the sides of the alphabet ring and hold it in any of 26 different positions. By turning the positioning ring (or crown) (1161) by hand, the letter on the alphabet ring, which is chosen for the keying (see page 3/4) can be brought to register with the index (1101).

If the positioning levers (114) are pulled apart, as shown in fig. 4, the alphabet ring unit can be removed. Normally the unit is provided with an alphabet ring (11611) with letters in their normal sequence. In case rings are to be used, the protecting glass (1163) is easily removed to allow this.

In the bottom plate (12) of the housing the mounting plate (2) is fastened at four points by screws. The platen carries the complete ciphering mechanism (with the exception of the alphabet ring assembly.)

The lid (11) is kept closed by the lock spring (112). To open the lid, press the lock spring knob (1121). (Turn the knurled knob in other models).

2. Mounting plate. On the upper side of the mounting plate, the following main parts are mounted:

a) A group of six key wheels (4), which are kept in place, when the led is open, by the hoding spring (221), and which are otherwise kept in their proper position by the key wheel guide (231).

b) The sensing mechanism (6).

c) The key wheel advancement mechanism (5) with the Maltese cross (51) in its housing (23) and

d) the stepping mechanism (3) with its six notched disks on top of which the alphabet disk (341) is mounted.

On the under side of the mounting plate the drive mechanism is located. Its parts are described in a following paragraph.

To remove the key wheels, in order to rearrage them, or the pins in them, lift the holding spring (221) slightly and turn it to the side: the key wheels can now be taken out of the machine. The mounting plate (2) with the mechanism as per b, c and d above, can be separated from the bottom plate (12) by removing the three screws (201) and the support (22). The mounting plate, however, is normally removed only when the machine has to be serviced.

F. FUNCTIONING

For the purpose of explaining the functioning of the machine, we will following consider the mounting plate with the mechanism mounted on same, removed from the housing, and the key wheels from the mounting plate.

When the catch (28) is pulled downward, the operation lever (71) is given free, and it will, under the combined tensions from the springs (7211) which are found on the under side of the mounting plate (2) and in the spring-housing (21), be pulled outward. It can now be pushed in by hand. It should be noted that the two movements: outward and inward, can take place only after the

lever (71) has reached the inner, or the outer end positions respectively. A ratchet lever (711) acts to control this.

When the operation lever (71) is operated then on the one hand the ratchet disk (74) will turn 90° and on the other the drive segment (72) will be moved to its innermost position, against the tension of the spiral spring (714). The ratchet (73) which presses against the disk (74) will assure that it will not turn more than 90° for every operation, and will also keep it in its correct position, when at rest. Furthermore, the curved slit (7102) in the operation lever (71) will, acting on the guide roller (611), cause the cradle lever (61) of the sensing mechanism (upper side of mounting plate) to move upwards.

The cradle lever will, when moved upwards, lift the sensing levers (62) away from the pins in the key wheels, against the tension of the springs (621). The movements are timed in such a way that the 90° movement of the ratchet disk (74) - which is dowelled to the shaft of the Maltese cross (key wheel drive) - will take place only when the sensing levers have been withdrawn, so that the key wheel-feed will not be hindered by these levers.

The Maltese cross, which extends over the combined height of the six key wheels, will for each operation advance these by one step by engaging their pinions (4121).

The key wheels can take individually the same number of positions as the number of their pins, and there is a detent inside each key wheel which assures that for each of the positions the key wheels can take, one of their pins will always be found exactly opposite the end of the respective sensing arm. Assuming that the key wheels have been removed from the machine - as described on page 13 - we can now put them back, taking care that the side, on which the pins are placed will face downwards. The pins are journalled on a closewound spring ring in such a way that the hole in the pin will be closed to one end so that the long ends of the pins can, by turning them over, point either towards the center of the key wheel or outwards. In the first mentioned position the pin is inactive (4112), and in the second active (4111). It must be taken care, when the pins have been arranged in the manner desired, and the keywheel put back into the machine, that all the pins remain in their proper position and that the operation lever (71) is pushed in and locked with the catch (28).

With all six key wheels in place, then, when the operation lever (71) is released and concurrently the six sensing levers, some of them may encounter active pins and remain in their active positions, while the other will be free to move into the spaces unencumbered by the inactive pins, and thus take their inactive positions. Suppose now that a key wheel has been placed into the machine in such a position, that an active pin (4111) is found opposite its sensing lever. When we now release the operating lever (71) slowly, we will find that when this lever has moved about 10 mm (3/8") outwards, the cradle lever (61) will descend sufficiently to release the sensing arms, and the arm which corresponds to the above mentioned active pin will be stopped by this, so it will move very little, and will remain in its active position, while the other five sensing arms which do not encounter any pins, will make their full movement.

Now looking back to the under side of the mounting plate (2), it will be seen that the lever (721) which had been subjected to the pressure of the spring (7211) will be given free, and will in its turn transmit the tension of the spring (714) in the housing (21) to the drive segment (72). This has a gear segment (7201) which meshes with the pinion (35), which is dowelled to a vertical shaft inside a hollow shaft, on which the displacement disk assembly (or stepping mechanism) (3) is mounted. This vertical shaft is keyed to a disk at the top of the assembly which carries the alphabet disks (341). Under the top disk there are five notched disks which are mounted loose on the hollow shaft, and at the bottom a sixth notched disk which is revited to the mounting plate (2). The number of notches in the six last mentioned disks is 16, and the numbers 1 to to 16 ate engraved on the mounting plate in a semicircle, with one number below each notch, whereby these can be identified. The notches are placed so that the distance betweeen successive notches is 1/26 of the complete circle.

The top disk has a stop (3401) which points downwards and reaches a little below the topmost notched disk. This disk in its turn has a stop (3102) going down to the next notched disk below and so on, that the stop of the last loose disk will reach to the bottom fixed notched disk. Each of the six notched disks carries on its upper side a small catch (311) which when not acted on will engage the stop of the next disk above, so that the catch of the sixth notched disk will engage the stop of the top disk which carries the alphabet disk. Each of the notched disks also carries a lug (313) which can be placed in anyone of the sixteen notches.

As mentioned earlier, the top alphabet disk is subjected to a torque from the spring-loaded segment (72) which tends to turn it in a clockwise direction, but no movement will take place even when the operation lever (71) is released as long as the catches stay in their locking positions: the catch of the stationary bottom disk engages the stop of the next disk and so on up to the top. Now, if any one of the catches (341) is released, the disk immediately above the one carrying the catch will turn clockwise and will be arrested only when its stop will strike the lug of the disk carrying the released catch. If the lug is placed in the notch No. 1, the movement between the two disks and of all the disks above the release disk, including the alphabet disk, will be equal to 1/26 of a revolution, i.e. the distance between two letlers on the alphabet disk. The amount of movement of the displacement disk assembly for each operation will depend on one hand on the position of the lugs on the notched disks, and on the other hand on which of the catches are released. The release of the catches is directed by the key wheels and executed over the sensing levers, the lower arms of which will encounter active or inactive pins in the key wheels.

We have already noted that the sensing arms which encounter active pins will remain in their upper positions, when their upper portions press against the detents of their corresponding notched disks. Now when the operating lever (71) is released and begins to move outwards, the active sensing arms will keep the corresponding catches released, while the inactive sensing arms will descend at such an early moment that the previously released catches will return to their locked positions. Thus, for instance active pins in the first, third and fifth key wheels (counted from the bottom) in position to act on their sensing arms will release the catch on the first, third and fifth notched disks. If their lugs have been placed in the notches 1, 5 and 7 respectively the disk No. 2 will move one step (1/26 of a revolution) in relation to disk No. 1, disk No.4 will turn 5 steps in relation to the disksbelow, and disk No. 6 (and also the alphabet disk above) will turn 7 steps in relation to disk No. 5. All in all the displacement for the alphabet disk will be 1+5+7 or 13 steps. Theoretically the alphabet disk could be made to turn up to about 120 steps, but the number of possible steps has been limited to 40, from practical reasons (a larger number of steps would have required very strong operating springs, which would be very hard on the operator). As the total movement of the alphabet disk has been limited to the above mentioned 40 steps, it is necessary to choose such lug combinations, total of which will not exceed 40.

From the above discription it has been seen that for every operation

1. the key wheels will be advanced one step each, and

2. the alphabet disk will turn a certain number of steps (= distance between two letters) clockwise, from its initial position. This number of steps is the sum of the movements which can take place between these pairs of disks, which have been desengaged through the action from the key wheels on the catches.

As each of the six sensing levers, depending on the position of the pins in the key wheels (active or inactive) can take two positions, there will be $2^6 = 64$ possibilities, through which to achieve from 0 to 40 displacement steps for the alphabet disk, combined from six partial displacements of minimum 0 and maximum 16 steps.

The counter (53) is connected over the gearwheel (52) with the pinion (511) and advances one step for each operation. When the operating lever is locked in its inner position, the counter can be set to any desired position by turning the gear wheel (52) with the tnumb by hand forwards or backwards. When the key wheels are in the machine, it will be more convenient to use the crank (shown on fig. 10). This is also used, when one wishes to move the key wheels to a desired position, such as starting position. The key wheels can also be turned individually by hand, when the operating lever is in the inner locked position.

G. OPERATION

The machine CD-57 is normally supplied with six key wheels which can be chosen from the following twelve sizes (number of divisions = number of pins): 25, 26, 29, 31, 34, 37, 38, 41, 42, 43, 46, and 47.,They are provided with letters and numbers on their peripheries, in order to allow the definition of the positions during use, and numbers at the pins, to define the pin settings.

In case the CD-57 is used to correspond with machines of the C types, then the instructions as per notice No. 3092 have to be followed, as to which key wheels can be used. Otherwise the choice is free. To prepare the machine for use, the following procedure has be followed:

1. Remove the key wheels from the machine, and put them on a table with the side with the pins uppermost (see fig.7). Turn over the pins, by hand or using the free end of the crank, in accordance with keying instructions in force.

2. The mobile lugs (313) on the displacement disks are placed in the prescribed notches, with the aid of the crank (fig. 9), the free end of which is provided with a slot which fits over the lug. Check that the total number of displacement steps will not exceed 40.

3. Check that the operating lever has been pressed in and locked with the catch, (28), (fig. 3).

4. Set the counter to show at least the two last zeros, (see fig. 8).

5. Place the key wheels into the machine, in the pescribed sequence, with the pins facing down. Take care that the pins remain in their proper positions, then slode the holding spring (221) over the top key wheel, until it locks over the guiding pin (231).

6. Turn the key wheels individually by hand until the prescribed starting position has been obtained. This is defined by a letter combination, with the letters chosen on the key wheels registering with the index pin (27). In fig. 6, key wheel positions are: A A A A A A.

7. Close the lid (11) of the machine, after having put the crank (1131) in its place inside the lid (see fig. 5).

8. Turn the alphabet ring assembly (116) so that the chosen key letter registers with the index in the lid.

The machine is now ready to be used.

To cipher a message, the operating lever (71) has to be unlatched so that it can take its outer position; after this, it is pressed inwards once, and then allowed to move outwards again, after which the first letter of the text (primary letter) is sought out on the alphabet ring (116) and the corresponding secondary letter read off the alphabet disk (341) and noted. This operation is repaated for each of the following letters in the text. For the ciphering of further messages, then, depending on the instructions in force, some or all of the settings are changed (see 1 to 8 above) or key wheels are simply moved forward to the next starting position using the crank. (For further information see leaflet No. 176).

H. CRYPTOLOGICAL CONSIDERATIONS

The safety of the ciphers, produced on the CD-57, depends as far as the possibilities built into the machines allow, on the proper arrangement and use of the following organs:

a) Stepping mechanism (displacement disk assembly). The arrangement of the lugs gives the number of displacement steps, contributed by each of the disks, and these should be chosen in such a way that when they are combined in the 64 possible arragements ($2^6 = 64$) each of the steps from 0 to 25 (where the steps from 26 up to the maximum of 40 will act as repetitions of the steps 0 to 14) should appear as closely as possible with the same frequency. As the number of letters in the normal alphabet is 26, and the number of step combinations is 64, the closest one can come to the ideal, is for parts of the step combinations to appear twice and for the rest three times. The example shown below for a good distribution of the 26 steps is based on the following positions for lugs on the disks:

Disk	No.	1	=	1 step
"	"	2	=	2 steps
"	"	3	=	4 steps
"	"	4	=	7 steps
"	"	5	=	8 steps
"	"	6	=	10 steps

d) Starting positions for the key wheels.

As the length of the priod for the normal set of key wheels is about $2{,}8 \times 10^9$ letters, and as the normal length of a message will exceed 500, there would theoretically be possible to cipher about 6×10^6 messages with the same pin arrangement in the key wheels without using the same part of the period twice. In practice this should, however, be avoided and only irregularly spaced portions of the period used, and care taken that the same parts of the period should not be used twice. The distance between the parts of the period used should be at least about twice the average length of the messages to be ciphered.

e) The alphabet ring can take 26 different positions, and although in itself has little cryptographical value, its use should not be disdained as it shows up the cryptoanalysis.

The machine is normally supplied with an alphabet ring having the 26-letter alphabet in its usual sequence A...Z and an alphabet disk with inverse sequence Z...A.

In the foregoing it has been mentioned that the same part of the period should not be used twice.

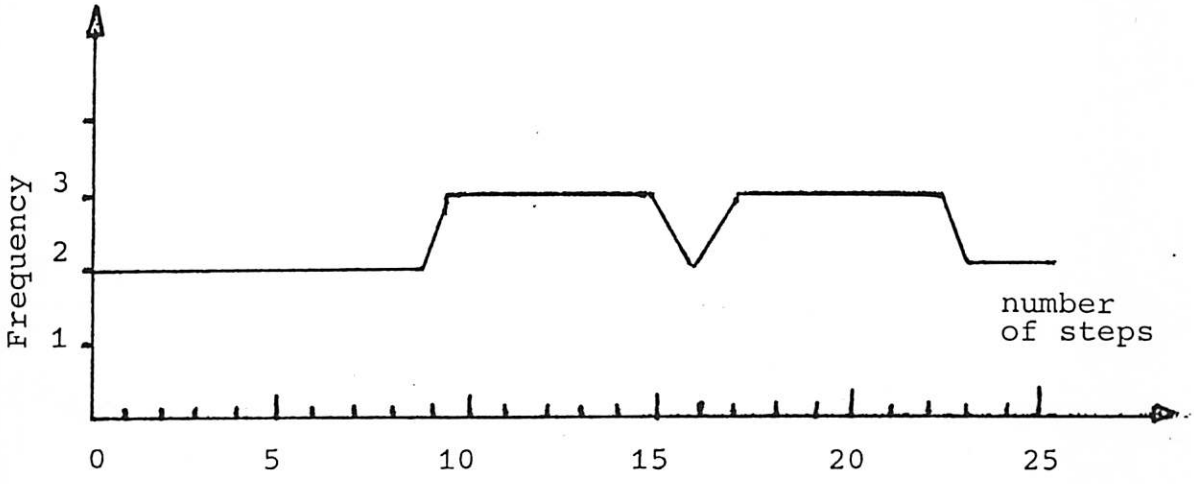
It should be useful to note that decrypting of messages produced with even the most complicated substitution series will always be possible under the following conditions:

1. If the alphabets are known when messages are enciphered with the same part of the period (substitution series).

2. If the alphabets are unknown, but inverse: about 5 messages.

It is here supposed that substitution series are unknown in both cases mentioned.

From the above enumeration of the variable factors, entering into the ciphering procedure for the CD-57, it will be seen which in diagram form shows the 64 possible step combinations distributed as follows:



It will be seen that the steps 0 to 9, 16 and 23 to 25 will appear twice, while the steps 10 to 15 and 17 to 22 will appear three timees. It will usually not be possible to find good lug arrangements through calculations. The most suitable way is to try out a number of combinations and file them for future use. It is of course not necessary to have the sum of the steps produced by each of the six disks to total 40, one may use different totals which increase the number of suitable lug combinations.

b) Key wheels.
If only six key wheels, which are necessary for the proper use of the machine, are available for the user, these can be placed in the machine in 6! = 720 different sequences. With all the 12 key wheels available to the user, there will be about 6×10^5 different ways to place the key wheels.

c) Key wheel pins.
For each key wheel there are n pins, which as each pin can take two positions (active or inactive), allow a total of 2^n pin combinations per wheel. As normally the number of active pins should not be less than 40 % and not more than 60 % of the total number of pins and as there should also not be more than 5 active or inactive pins in a row and as the average number of pins per wheel is about 37, the average number of suitable pin combinations per key wheel will be about 10^{36}.

d) Starting positions for the key wheels.
As the length of the period for the normal set of key wheels is about $2{,}8 \times 10^9$ letters, and as the normal length of a message will rarely exceed 500, there would theoretically be possible to cipher about 6×10^6 messages with the same pin arrangement in the key wheels without using the same part of the period twice. In practice this should, however, be avoided and only irregularly spaced portions of the period used, and care taken that the same parts of the period should not be used twice. The distance between the parts of the period used should be at least about twice the average length of the messages to be ciphered.

e) The alphabet ring can take 26 different positions, and although in itself has little cryptographical value, its use should not be disdained as it shows up the cryptoanalysis.

The machine is normally supplied with an alphabet ring having the 26-letter alphabet in its usual sequence A...Z and an alphabet disk with inverse sequence Z...A.

In the foregoing it has been mentioned that the same part of the period should not be used twice.

It should be useful to note that decrypting of messages produced with even the most complicated substitution series will always be possible under the following conditions:

1) If the alphabets are known when messages are enciphered with the same part of the period (substitution series).

2) If the alphabets are unknown, but inverse: about 5 messages.

It is here supposed that substitution series are unknown in both cases mentioned.

From the above enumeration of the variable factors, entering into the ciphering procedure for the CD-57, it will be seen that they offer far more possibilities than can ever be utilized in practice, and will also exclude any chance of different users employing the same combinations, even if the machines were used universally.

The ideal way of using the CD-57 (and for that matter any other good ciphering machine) would be to use different combinations throughout, including that of different alphabets, for every new message, but this is clearly not generally possible. The user will have to strike a judicious medium between the possibilities offered by the machine, and the practical exigencies of the service in question. He will then be able to obtain with the pocket cryptographer type CD-57 the security demanded by that service with a minimum of operating rules.

Encl. : 12 figures
1 table

Zug, August 1966
OSt/iz

HAGELIN-CRYPTOS
CRYPTO AG

Example

Table I

Position No.	Stop No.
1	1
2	2
3	4
4	7
5	8
10	10

This gives a total of 32 steps. The single sum of steps (totally 64 combinations) is obtainable as below:

Combinations	Number of steps	Combinations	Number of steps
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	136	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