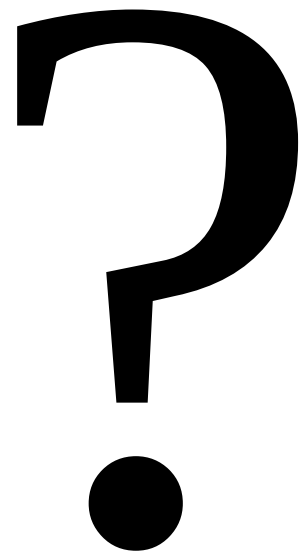
Kryha cipher machines

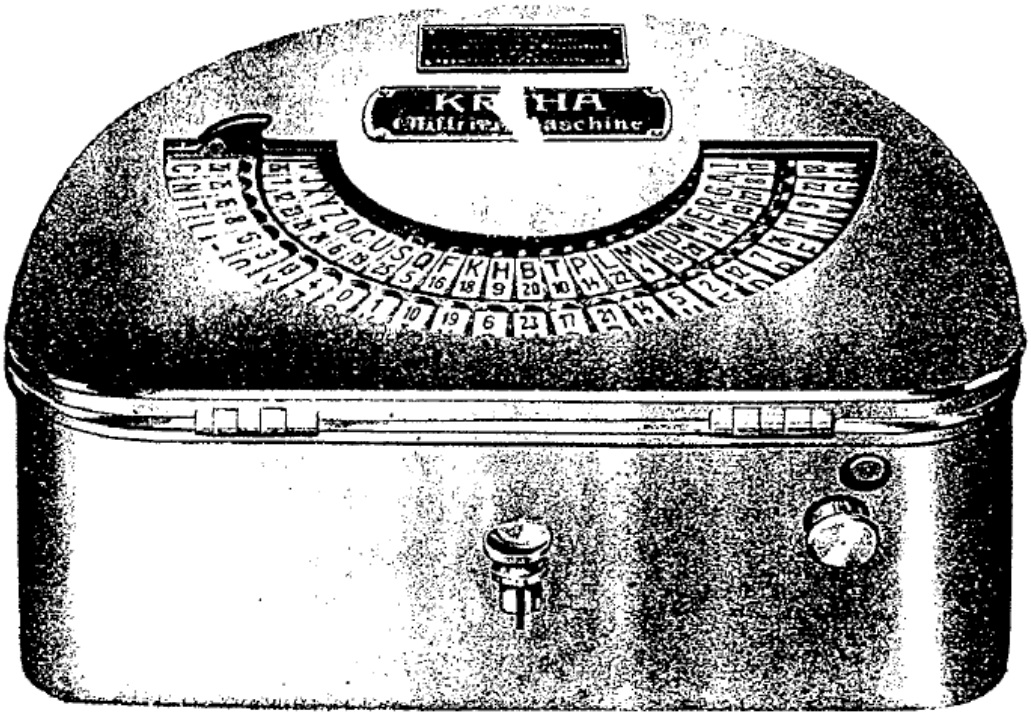


[le symbols of the Kryha society: a variety of trident]

itrnde xumylha

Mertens-Freiwald

The Kryha Encryption and Decryption Machine



Kryha-Commerce

Awarded a State Prize by the Prussian Ministry of the Interior at the Great Police Exhibition in Berlin, 1926

I.
Purpose.

Purpose

The purpose of the machine is to mechanically encrypt and decrypt documents of any kind, letters, and telegrams in such a way as to guarantee their absolute confidentiality from unauthorized persons.

II.
General.

General.

The machine's mechanism is housed in a nickel-plated brass case, which is closed by a lid. The case is semicircular, measuring 25 x 20 cm and 10 cm high. It can be stored and transported in a handy leather case.

The machine, which is made mostly of Elektron metal, weighs approximately 4.5 kg.

It is mechanically driven by a precision clockwork mechanism built into the case.

The hand-operated machine functions without a connection to an electrical current and is therefore completely independent, so that it can be carried in the field, on airplanes, while traveling, etc., and is always ready for use.

The operation can be learned quickly. With some practice, 60-70 letters can be encrypted or decrypted per minute.

III.
Brief explanation
of the mechanical process of encryption and decryption.

Mechanical Process.

(For detailed operating instructions, see Section VIII)

The "Commerce" model machine does not operate as a typewriter; instead, it mechanically converts any plaintext into a ciphertext that is read and written down or dictated.

Encryption.

The ciphertext is obtained by locating each letter of the plaintext on the outer (green) plaintext semicircle (Figure I f*) and replacing it with the corresponding (black) ciphertext letter.

While the (green) plaintext letters are arranged on a stationary disk, the (black) ciphertext letters are on a rotating disk (ciphertext disk, Figures I e, II a**), which is set in motion by briefly pressing a key (Figure I a). (For details, including releasing the brake, see Section VIII.) This shift of the cipher disk must be triggered after each encryption of a letter by briefly pressing the key again.

The essential point is that the rotating ciphertext disk constantly brings different ciphertext letters into contact with the plaintext letters.

Example: (For details, see Section VIII)

```
Plaintext : A s i a A m e r i c a
Ciphertext: f t h q j f u n c g w
```

The machine's unique mechanism causes such varied movement of the ciphertext letters that the periodic recurrence of encryption is extended almost indefinitely. This is achieved primarily through the unique design of the interchangeable cipherwheel (Figure II e, removed).

---

*) See page 9.

**) See page 13.

This wheel rotates inside the machine, and depending on the arrangement and number of teeth and locking holes ("stopping points" 1, 2, 3, etc.), it causes a greater or lesser rotation of the cipher wheel.

Due to the variation in these rotations, the encrypted text is completely dependent on the machine's initial position at the start of the encryption process. This initial position includes, among other things, the initial position of the letters (e.g., A=F) and the initial position of the cipher wheel (e.g., stopping point 12, recognizable by the gap – Figure I g).

Since decryption is impossible without knowing this initial position, this alone provides a simple yet secure method of decryption.

The uncontrollability of the movement of the ciphertext letters can be further increased by inserting one or more "space characters" (e.g., the dispensable "j" or a dash "-") after the end of words in the plaintext and encrypting them.

Furthermore, the agreed-upon "default position" can be refined by occasionally changing the order of the interchangeable plaintext and ciphertext letters.

Finally, a specially designed, individual cipher wheel can be used for specific recipients or groups of recipients, thereby achieving the highest degree of undecipherability. (For a detailed explanation, see Section VI.)

Decryption.

Decryption is performed analogously to encryption, with the only difference being that the letters of the ciphertext are located on the movable ciphertext wheel (black letters) and replaced with the corresponding (green) plaintext letters. At the start of the decryption process, the agreed-upon initial position (e.g., A=F, stop point 12) must be set (see Section VIII for details).

IV.
The Undecipherability of the Machine.

Decryptability.

The claim that the mechanical Kryha cipher is completely undecipherable to the untrained eye and therefore absolutely secret has been scientifically proven.

Dr. Georg Hamel, Professor at the Technical University of Berlin-Charlottenburg, provided this proof in a detailed expert opinion and considered the invention so scientifically interesting that he presented and scientifically evaluated it in a lecture at the Berlin Mathematical Society in front of a group of scholars. (See Proceedings of the Berlin Mathematical Society, Vol. XXVI.).

From the expert opinion, only the following should be mentioned:

"With 14 cipher wheel holes (stopping points), the number of possible combinations is a seventy-one-digit number, beginning with 3!" (With an increase in the number of cipher wheel holes, this number grows many times over.)

"If 10 million people buy the machine, each of them can still perform 90 billion system changes without any two people having the same system."

V.
The machine's potential uses.

Usages.
Possibilities.

For all entities that must place absolute value on the secrecy of certain messages and records (diplomats, politicians, government agencies, armies, navies, air forces, the press, trading companies, banks, etc.), the machine offers the only absolutely secure protection against espionage.

The World War proved that the previously used secret codes do not guarantee absolute protection. Their decryption is not an insurmountable problem for experts.

The ideal replacement for secret codes.

The superiority of the cipher machine over any secret code is evident from the following:

Every secret code must be printed in numerous copies and sent to all points of contact. The printing process alone carries the risk of betrayal. (Furthermore, military and diplomatic agencies must maintain mobilization stocks, which in wartime are sent to the operational area and carried on journeys.)

If even a single copy of the code is lost or stolen, its secrecy is no longer guaranteed, the entire print run becomes worthless, and a reprint is necessary. Experience has shown that altering a code that has once been betrayed is a rather unreliable stopgap measure.

In contrast, the loss of a cipher machine does not jeopardize secrecy.

If necessary, simply replacing the cipher wheel and rearranging the letters is sufficient to eliminate any risk of betrayal. Furthermore, it is advisable to keep the cipher wheel, and possibly also the letter rings of the plaintext and ciphertext wheels, locked away from the machine. This allows the machine to be left open in the office.

The cipher machine thus offers the ideal mechanical replacement for all secret code communication, avoiding all the disadvantages of a cipher system.

As already mentioned, telegrams can be pre-encrypted with abbreviation codes to shorten the text. These codes can be used openly and do not need to be kept secret. This significantly simplifies the entire encryption process and renders all secret codes superfluous.

Free choice of key.

The machine is so easy to operate that it can be learned in a short time. On the other hand, the selection of keys to be agreed upon results in so many combinations that the ingenuity of the head of the relevant cipher department in this area is rendered insufficient by the machine's peculiar design.

The current demand for "rationalization of the economy" must not stop short of organizing office operations. Just as the calculating machine overcame mental arithmetic despite the initial resistance of some employees, the task of the cipher machine is to mechanize encryption, protect against errors, and simplify it while ensuring absolute security.

Among the numerous applications, the following should be highlighted in particular:

Eliminates travel.

Whereas previously it was often necessary to convey particularly important and confidential messages—especially for branches abroad—orally or by courier, the cipher machine offers the possibility of entrusting not only telegraphic instructions but also detailed written explanations to the postal service with a guarantee of absolute confidentiality.

The purchase of the machine,

which initially might only be used to equip the most important seats, will pay for itself in a short time, among other things, through savings in travel costs.

Secure communication with foreign countries.

The threat of espionage, particularly in international trade, especially overseas, should not be underestimated, so foreign representatives will especially welcome the machine as an invaluable advancement.

Encryption options for travel.

Since the machine, due to its light weight and practical, inconspicuous case, can be taken on trips (including by plane), it also offers the advantage of protecting highly confidential documents and preventing the loss of folders or wallets. At the same time, it allows for encrypted communication (telegraphically or by letter) with headquarters from any location while traveling, without having to carry a secret code.

Secret files.

Given the extent of industrial and business espionage today, it can also be extremely advantageous to store particularly important and secret documents in Kryha script.

All the aforementioned aspects naturally become more important in times of internal unrest or the threat of war, so it is always advisable to possess a certain "mobilization reserve."

Apart from maintaining secrecy, the machine fulfills an important function in

Payment transactions.

Protection of payment transactions against counterfeiting.

Using the machine offers the only truly secure protection against the forgery of any type of payment order.

For telegraphic payment orders, the encryption of the order (name of the recipient) and the amount renders the previously used keying method superfluous and surpasses it in simplicity and security.

For written payment orders and letters of credit, a notation containing the order and amount in Kryha cipher is sufficient to prevent any forgery or to detect it immediately.

Even in check transactions—at least when large sums are involved—the cipher machine is designed to make forgery impossible through an encrypted control note.

(The recently reported check forgery, which defrauded a major New York bank of $150,000, proves that the previously used punching machine is insufficient when a check form is obtained and the signature skillfully forged.)

Numerous simple combinations arise for encryption in payment transactions, for example, in conjunction with the letters of the recipient's name and their number.

Security of documents of all kinds.

Generally speaking, markings using Kryha encryption (possibly discreetly placed) are the best means of certifying the authenticity of documents of any kind and protecting them against forgery.

For example,

Identity cards

can also be secured against signature forgery by discreet markings.

Kryha Electro Writer.

For central agencies that need to perform extensive encryption services in the shortest possible time, an electrotype cipher machine of the same system is available, capable of up to 300 characters per minute. (Image on envelope.)

Since both models correspond to each other in operation and use, they can be used simultaneously in communication between main stations (electronic) and branch stations (Model "Commerce").

Keying options.

VI.
Detailed explanation of the keying options.

The simplest keying (arranging the initial position) consists of the following two elements:

1. "Holding point" of the cipher wheel, e.g., 12,

2. Initial position of the plaintext and ciphertext letters relative to each other,

e.g., A=F. (See also the operating instructions, Section VIII.)

With sufficiently frequent changes, this keying, in conjunction with the characteristics of the cipher wheel, practically guarantees far greater protection against decryption than the previously common encryption methods.

In the event of a particular threat, and to also meet the scientific requirement of undecipherability, i.e., In addition to the possibility of a period recurring indefinitely, the machine offers four further encryption options.

Unchangeable plaintext characters.

3. Rearranging the letters on the plaintext disk.

According to the instructions in Section VIII, all letters on the plaintext disk can be rearranged in numerous other sequences, which can be agreed upon at will.

To save time by avoiding the need to replace individual letter tiles, the metal ring bearing the plaintext letters can be exchanged for another ring bearing the plaintext letters in a different order. Such metal rings can be kept in any quantity and specially marked. The key would then be, for example: 12, A=F, Plaintext "June".

Changeable ciphertext characters.

4. Rearranging the letters on the ciphertext disk.

Similar to the arrangement of the plaintext letters, the ciphertext letters can also be rearranged at will. Likewise, the metal ring bearing the ciphertext letters is interchangeable. It is important to note that within the two cipher alphabets, the letter sequence of one alphabet must exactly match that of the other.

Key example: 12, A=F, Plaintext "June", Cipher III.

Custom cipher wheel.

5. The Cipher Wheel's Variations.

The cipher wheel is the "soul" of the cipher machine. Driven by the clockwork mechanism, it rotates, as soon as the lever is released by pressing the key, by the distance between two stopping points, until the lever's nose engages again at the next hole (stopping point), bringing the cipher wheel to a standstill.

Simultaneously, the cipher disk is also set in motion by the gear train, rotating by as many letters as the gear set of the cipher wheel, which was just rotating past gear (II i), has teeth. The type of teeth on the cipher wheel is therefore just as crucial to the movement of the cipher letters as the number and opposing spacing of the holes ("stopping points"). This results in endless variations for the construction of the cipher wheel. The wheel can, for example, be made with 15 or 21 holes and correspondingly different hole spacings.

They can be manufactured, and with the widely varying toothing patterns, simply filing away individual teeth is sufficient to make the wheel "individual."

No master key!

Therefore, the owner of the machine cannot be controlled by the inventor or manufacturer. **There is no master key!**

In practice, this allows for the possibility of keeping "individual" cipher wheels, identified by numbers or names, for communication with particularly important entities.

Key example: 12, A=F, Kl. "Juni," ch III, Wheel "Hamburg."

6. The insertion of spacers.

Space symbol.

Of the 26 plaintext letters, the least common one in the language in question (e.g., the letter "j" in German) can be inserted after the end of words as a spacer or replaced by a "-" on the plate.

This "spacer" is used to encrypt the space between individual words. Instead of words, one obtains a continuous sequence of characters, which can be divided into groups of 5 and 10 as needed, for example, in telegram communication. During decryption, the cipher of the blank space (j or "-" line) again results in a word break, so that the encrypted text mechanically reproduces the words in their original order. This method has the two advantages that, firstly, a character is added after each word—that is, irregularly and at a point not discernible to an outsider—thus altering the key, and secondly, the decryption reveals the original words in their correct order without the length of the individual words being apparent due to the grouping of the characters in the ciphertext.

Example:

```
                          (j)              (j)
Plaintext : A s i e n - A m e r i k a -
Ciphertext: f t h t q a r m a u h m d b
```

A specific agreement (key) is not strictly necessary for using this combination, as it appears automatically during decryption.

Of course, one can also change the sequence at any time—even within a ciphertext—by inserting one or more spaces. This results in countless new combinations that completely scramble the periods and make them endless.

A particular advantage of the machine, as derived from the above, is that no fixed set of instructions is needed for key selection. Instead, the owner has complete freedom in how the machine is used, i.e., in combining and applying the various encryption options.

Example of the effect of "inserting spaces" on the ciphertext.

Key remains 12; A=F.

```
1. Without spaces   A s i e n   A m e r i k a   A u s t r a l i e n
                    f t h t q   j f u n c g w   d p z e q m h o a x
                            (j)             (j)               (j)
2. After each word  A s i e n - A m e r i k a - A u s t r a l i e n -
a space character.  f t h t q a r m a u h m d b r d p t b x t b l l x

3. 1 Space marker   - A s i e n - A m e r i k a - - A u s t r a l i e n -
before the first    x l y o z v i y s h z n t i i p h s a e n k e p b y k
word, one before
the second, two
before the third.
```

VII. Ciphering Code Texts.

Since the machine encrypts the plaintext but does not condense it, special codes can be used for longer telegrams to reduce costs by shortening certain expressions. This code text only becomes truly secret through "over-encryption" with the cipher machine; because commercially available codes (Mosse, A.B.C., etc.) are generally known, but even special codes (private and company codes, etc.) are—as was particularly evident during the World War—decipherable by experts.

It is particularly important to note here that only abbreviation (contraction) codes are now possible, which require no secrecy whatsoever and can be used quite openly.

Every so-called secret code becomes superfluous!

When encrypting code texts in letters or numbers, the keying digit 6 (inserting spaces) cannot be used if all 26 plaintext characters are needed. It is also superfluous, since an over-encrypted code text does not provide any clues to the plaintext.

Numeric codes.

When encrypting numerical codes, the numbers of the code are replaced by the machine's cipher letters. Since the numbers 1-25 are each represented by a single cipher letter, using the machine results in significant cost savings, averaging at least 30% to 50%.

Cost savings.

Since the numerical codes are usually arranged in groups of 5, it is practical to encrypt the numbers consecutively and then group the resulting letters of the ciphertext into groups of 5. Upon decryption, consecutive numbers are obtained, which are then divided into the known groups of the numerical code. Errors regarding the grouping of the numbers are thus impossible.

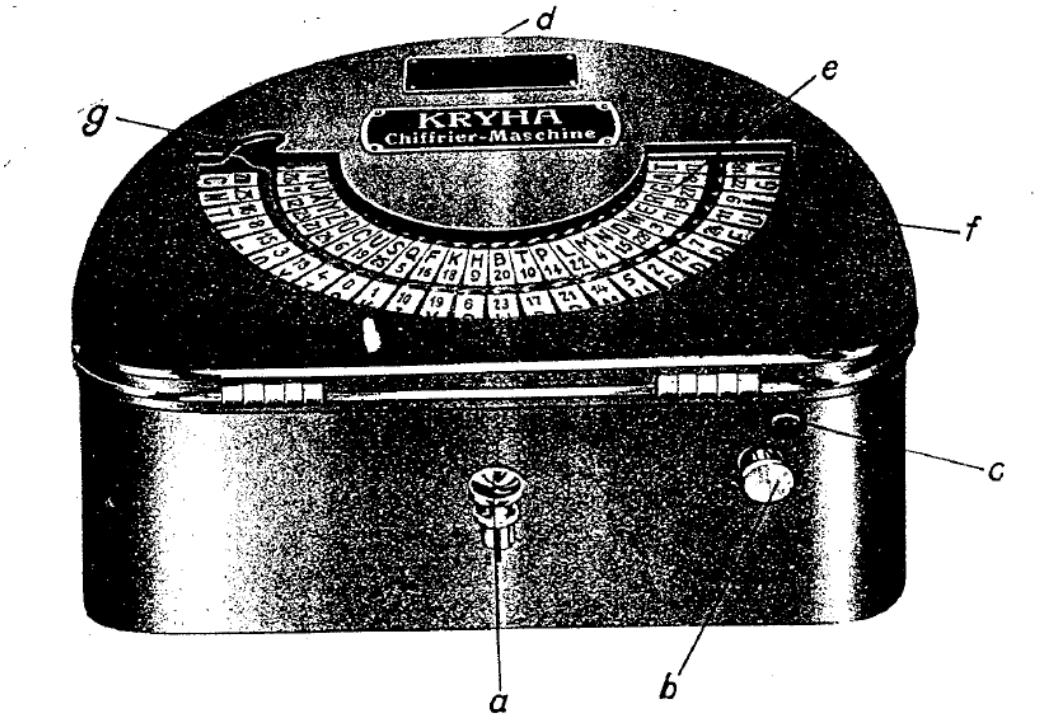


Figure I

VIII. Detailed Instructions for Use.

Instructions for use.

Preparation

Unlock the case.

Open the case lid.

Remove the winding crank, which is visible in the gap between the machine and the flat side of the case.

With your left hand, grasp the handle from below.

With your right hand, reach into the aforementioned gap and, while your left hand lifts the case and places it on the flat side, carefully remove the machine.

After inserting the key, located against the flat side of the case, into the keyhole visible on the curved side of the machine, place the machine horizontally on a table so that the flat side is flush with the edge of the table.

On this side, you will see (Fig. I):

the button (a)

the brake button (b)

the winding hole (c)

Then insert the winding crank into the winding hole. Gently turn the crank back and forth until the notch engages.

Wind the clockwork mechanism – like a gramophone. Approximately 80 turns are sufficient when the clockwork is completely wound down. Stop winding when you encounter significant resistance. Do not overwind.

Pull the brake knob out as far as it will go.

Now, if you press the key very briefly and with a springy motion (as when typing on a typewriter), the inner row of black letters will rotate slightly to the right, while the outer row of green letters remains stationary.

Opening the cover (unlocking and grasping the cover by the small tab above the keyhole, I d), you will see that by pressing the key again very lightly and briefly, the inner row of letters rotates on a disc. This is the ciphertext disc (Figures I e, II a).

The outer row of numbers remains stationary; this is the plaintext disc (Figure I f).

You can also rotate the ciphertext disc from left to right by gently pressing it with your finger. The letters (cipher letters) are attached to a ring, which in turn is held in place on the cipher disk by three retaining springs (II b). The cipher letters must be directly opposite the letters on the plaintext disk (plaintext letters). If this is not the case, grasp the cipher letter ring with both hands (thumb and forefinger) and correct the position of the letters by rotating them slightly from right to left.

The cover can now be closed again.

Looking through the gap (I g, on the left at the top edge of the glass pane) into the machine, you will see a number that changes when the key is pressed. This number indicates the "stopping point" of the rotating cipher wheel (see below for details).

Encryption.

After understanding these steps, you can begin encrypting. The process involves spelling out the plaintext, but instead of a plaintext letter, taking (writing down or dictating) the corresponding ciphertext letter brought forward by the ciphertext disk.

Since the ciphertext disk always displays new letters opposite the plaintext letters when the key is pressed, you must remember the initial position of the ciphertext disk relative to the plaintext disk. It suffices to note any pair of letters (plaintext and ciphertext letters), e.g., A=F.

Furthermore, since the rotation of the ciphertext disk depends on the rotation of the aforementioned cipher wheel, you must also note the initial position of the cipher wheel, i.e., the "stopping point" visible through the gap (number 1, 2, 3, etc.).

The initial position of the letters and the stopping point of the cipher wheel are the simplest elements of the "home position."

Example:

Ciphering the words

A s i e n - Am e r i k a.

Write this text (clear letters, ideally with small spaces between them initially) on a piece of paper, and don't forget to also note the starting position (e.g., 12, A=F).

Then write the cipher letter F below the clear letter A. (Dictating will increase your speed later!)

After writing each letter, the key must be pressed briefly and lightly, and of course, only once.

If, during the initial exercises, you interrupt the encryption process by pressing the key repeatedly or incorrectly—for example, by pressing it hard for a long time so that the cipher wheel skips several stops at once—and start again, you must remember to reset the noted starting position. First, reset the stop (12) by repeatedly pressing the key briefly, and then reset the letters (A=F) by opening the cover and rotating the cipher wheel accordingly from left to right. The best way to do this is to lightly press the cipher letter (F) with your index finger and move it towards the written plaintext letter (A).

Decipher.

By alternately writing the cipher letters and lightly pressing the key, you get the following text:

A s i e n A m e r i k a (plaintext)
f t h t q j f u n c g w (ciphertext).

You can see here that the letters in the plaintext that occur multiple times (a, i, e) are each encrypted by different letters, while at the same time the recurring letters in the ciphertext (f, t) each correspond to a different letter in the plaintext.*)

Decryption

is now very simple:

First: Set the "default setting" (12, A=F). (This "default setting" is therefore the simplest form of a "key" agreed upon between sender and receiver.)

Then you proceed as with encryption, except that when reading the ciphertext, you replace the (black) cipher letters with the (green) plaintext letters. (Reading from the inside out, whereas previously it was from the outside in.)

---

*) The recurrence of the same letter pairs in longer ciphertexts is random, but by no means periodic.

So: you write down f - a, then press the key briefly and lightly, write t - s, continue in this way, and easily obtain the plaintext

Numbers.

a s i e n a m e r i k a.

Numbers appearing in the plaintext can be encrypted in exactly the same way as the letters, since the plaintext letters are assigned the numbers 0-25. You can replace each plaintext number with its opposite ciphertext number, but it's better to use the corresponding ciphertext letter. This automatically shortens the text, since the plaintext numbers 10-25 are each represented by a single ciphertext letter (see Section VII).

If you are interrupted during encryption—for example, by a phone call—and have to stop, it is advisable to underline the last letter written and note the corresponding stop point. For example, in Asia, a break at "n=q": at n=q, you note the stopping point 16, ensuring that you continue in the correct position. Beginners can also occasionally note a stopping point at a letter pair to reliably avoid having to start over. Similarly, a very long cipher can be divided into several sections by inserting a pre-arranged word (e.g., "stop," "new," or any rarely occurring syllable). At the beginning of each new section (i.e., after "stop," etc.), the starting position (e.g., 12, A=F) is reset.

To return the machine to its case after use,

first, press in the brake button, close the machine, remove the key, carefully place the machine in the case with both hands, and then stow the winding handle and key in the empty space on the flat side of the case.

If you do not intend to use the machine for an extended period, it is recommended to let it run down to preserve the clockwork mechanism. (Instructions for this can be found at the end of this section.)

Explanation of other features of the machine and the necessary steps involved in its use.

Principle: When not encrypting, the machine must always be braked. (Brake button engaged.)

Plain text disc.

The plaintext disc.

Opening the machine cover reveals the fixed plaintext disc (green letters), embedded in a light metal plate. This plate can be opened to the right by sliding the button located on the left side of the cover slightly to the right and lifting it. You will then see that the plaintext letters are attached to a semicircular metal disc, which can be removed. To do this, lift the plate slightly with your left hand and hold it firmly, while simultaneously reaching under the plaintext disc with your right hand and pressing firmly on the protrusions on both sides of the button protruding from the back (II c). You then hold the plaintext disc in your hand. If you grasp a letter, i.e., one of the metal plates into which the letters and numbers are engraved, with your thumb and forefinger, you can easily pull it out sideways and insert it again.

When reattaching the plaintext disc, first ensure that all letter tiles are fully inserted and do not protrude beyond the edge. Then, slide the slightly flattened ends of the disc into the grooves protruding from the plate cutout and press the plaintext disc into the plate so that the knob protruding on the underside is once again held in place by the small spring.

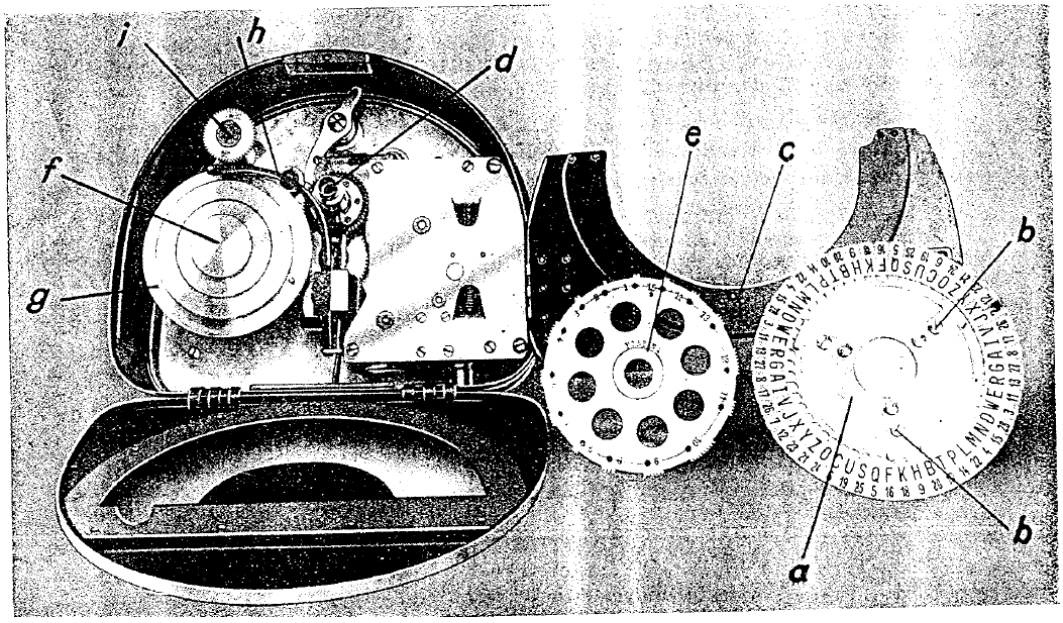


Figure II

Cipher text disk.

The ciphertext disc.

With the plaintext disc folded out to the side, the ciphertext disc is exposed. By placing both hands under the disc (not under the letter ring) and gently pushing upwards, you can lift it off the rotating axle on which it is mounted (II d). Do not use force or bend anything!

The letter tiles of the two cipher alphabets can also be removed as needed. Furthermore, the metal ring to which the letters are attached can be lifted off the disc once the three retaining springs (II b) have been turned to the side. When reattaching the metal ring, the retaining springs must be turned back to their resting position until they click into place.

Before reinserting the cipher wheel, ensure that all letters are properly inserted. Then, place the base of the wheel onto the rotating axle and gently rock the wheel back and forth until the base snaps into the axle's recess. (Do not use force!)

The cipher wheel:

With the cipher wheel removed, the cipher wheel is exposed (II e removed).

Cipher wheel.

The cipher wheel is screwed onto a mounting disc (II g) by means of a nut (II f). It is also held in place by a lever (II h), the lug of which snaps into the small holes drilled at the numbers (stopping points).

Before lifting this lever, ensure that the brake button is depressed; otherwise, the clockwork mechanism will run away.

After lifting the lever and unscrewing the nut, the cipher wheel can be removed.

The large holes drilled into the wheel serve only to reduce its weight. The medium-sized hole at position 0, however, acts as a detent for the pin attached to the mounting disc.

When reinserting the cipher wheel, first align the aforementioned hole with the pin, screw on the nut, and gently lower the lever.

When removing and replacing the cipher wheel, the teeth of the drive gear (II i) must be positioned in a gap between two sets of teeth on the cipher wheel. If this is exceptionally not the case (then the hole cannot be aligned with the pin when replacing the wheel), the cipher wheel or the mounting disc is given a short rotation by carefully loosening the brake (slightly pulling out the brake knob). This is repeated if necessary until the correct position is found.

Releasing the clockwork mechanism.

Remove the cipher disk and cipher wheel (with the machine braked, of course) and carefully release the brake. The clockwork will then run down, with the movement being slowed as much as possible using the brake and interrupted occasionally.

Examples of some complex keys:

Key symbol	Cipher wheel	Starting position	Letter sequence for plaintext and ciphertext wheels
Badso	Olexa H.P.5	B=A	Plain Text : acxptmbvrkedlqzh-fgyiosuwn ---------- Cipher Text: bljqignocufawsmydetxhpkrzv
Kariio	Berlin H.P.6	Z=O	Plain Text : wdms-lcraitpkefqxzbovgnuyh ---------- Cipher Text: yunbzqfigyapskwjdcmtehrvlo
45619	Sipo H.P.2	A=A	Plain Text : uqlravbohtzmkc-eydwixfsgpn ---------- Cipher Text: vcpzsnwyulbgdxemhoajftqkri
Robert	Norma H.P.15	N=K	Plain Text : xiftaqh-vycqgnewzusomdblrk ---------- Cipher Text: abcdefghijklmnopqrstuvwxyz
Malta	Thomas H.P.11	O=O	Plain Text : qaurminoxvbywcz-sltdfhegkp ---------- Cipher Text: abcdefghijklmnopqrstuvwxyz

*) H. P. = Stop point.

State Prize

KRYHA Encrypting Machines

guarantee absolute secrecy of ciphertexts
and eliminate all espionage

Indispensable
for all government agencies and banks, industry and commerce,
for all economic and political associations,
as well as for the press and all news agencies

World Patents

[photo of the electric kryha]

For telephone and telegraph
For letters and radio

KRYHA Electro-Typing Machines

encrypts, decrypts, and writes over 300 characters per minute simultaneously

Infinite key number!

BERLIN-CHARLOTTENBURG 2, SCHILLER STREET 109
TELEPHONE: STEINPLATZ 11070 * TELEGRAM ADDRESS: ERFINDKRYHA