

THE GLOW-LAMP CIPHERING AND DECIPHERING MACHINE: ENIGMA FROM THE ARCHIVES

[Editor's Note: We reprint what may be the first Enigma sales brochure produced around the mid-1920s to encourage all businesses to "keep their correspondence absolutely secret" by using Enigma. The cover reads, *Chiffriermaschinen, Aktiengesellschaft, Berlin W 35, Steglitzer Str. 2. Fernspr.: Nollendorf 2899, Tel. Adr.: Chiffrier Berlin*. Measuring 20.8 cm wide by 14.5 cm high with elegantly framed text on 16 pages, this pamphlet promoted the Enigma while "educating" the reader into a need for such a device in commerce. The original brochure is from the collection of Louis Kruh, one of *Cryptologia's* founding editors. Slight grammatical cor



WHAT PERSONS IT IS CALCULATED TO SERVE AND HOW?

It is a well-known fact that, now and forever, for purposes of both war and peace, politicians and military men, industrial producers and commercial houses are compelled to keep their correspondence secret. This is a point increasing in importance from day to day. Decisive battles have been lost, by land and by water, in the air and in debating with each other, because the adversary had a better method of keeping his correspondence secret, or a good apparatus being capable of considerably quickening the speed, and multiplying the number of information sent and received. Hand-writing systems will prove insufficient in times of great excitement and hurried proceedings.

If you have no good coding system, you are always running a considerable risk. Transmitted by cable or without wire, your correspondence will always be exposed to every spy, your letters, to being opened and copied, your intended or settled contracts, your offers and important news to every inquisitive eye. Considering this state of things, it is almost inconceivable that persons interested in those circumstances should delay securing themselves better against such things.

Yet, ciphering and deciphering has been a troublesome art hitherto. Much time and expenses and experience were required to give a man that qualification. Nevertheless, the result obtained couldn't be but very imperfect, for the secret code you made use of, was always accessible to many persons, or the ciphering clerk was ill or absent for any other purpose. Thus, expenses and efforts were always of little avail only. All kinds of losses and prejudices, perhaps irreparable, always threatened everybody's and the States business and existence.

Now, we can offer you our machine "Enigma", being a universal remedy for all those inconveniences. The machine has been tried and improved in the course of many years. At the present time this machine is a perfect instrument capable of any effect desired. It is of so simple a construction that every non-expert can learn and remember the few manipulations within a few minutes. Henceforth, no especial clerk is required for ciphering and deciphering. The managers may do the work themselves or with the aid of some reliable assistants. Spending once only a trifle, you will have a whole coding office, always ready for service, entirely reliable, free of charge when out of service, and costing but a few farthings a day when working. Moreover, the life of this machine being nearly endless, the time required for amortizing the funds invested is, theoretically, likewise nearly endless.

It is generally agreed upon that not only armies, navies, air-navigation, diplomatic representations, police-departments, in a word, the whole administration of

a State, but also all commercial houses, especially those engaged in exportation, all industrial undertakings, banking establishments (for instance in order to prevent every kind of fraud in bank assignments), shipping-companies, stockbrokers, inquiry offices, press people, large political and economical associations, Chambers of Commerce, and many others must keep their correspondence absolutely secret. The correspondence of a commercial house with their representatives and branch establishments is under the same necessity. This applies not only to information, sent to distant places, in which case the trouble and the expenses for journeys, conferences and couriers are saved, but is also true in such cases when documents, production-methods, explanations of drawings and the like are to be kept secret. The natural inquisitiveness of competitors is at once checkmated by a machine which enables you to keep all your documents, or at least their important parts, entirely secret without occasioning any expenses worth mentioning. One secret, well protected, may pay the whole cost of the machine. Of course, the machine cannot make a code altogether superfluous. But you need not any longer make use of expensive private and secret codes. You may safely avail yourself of any public code, simple or voluminous, in order to obtain a ciphered document resisting to every attempt of deciphering after having passed our machine. It is, moreover, superfluous to say that in sending written news, brevity is always much less important than security against inquisitiveness. An information, ciphered by our machine, may be safely sent by an open post-card without any danger of being deciphered.

Working with our machine is much less intricate than that with a writing-machine. Every beginner can learn the few manipulations required within a few minutes. The rapidity of writing is, practically, unlimited and only depends on the degree of rapidity with which the eye can perceive the flashing-up letters. There is no searching for ciphered letters in lists, on rules or discs, the bugbear of every specialist. There is no getting fatigued, not even with long work. You only need press down a certain key of the keyboard to make appear the corresponding ciphered letter, or, in deciphering the original text. In case of clerical errors, only put back the machine, the mistake will be corrected within two seconds. Moreover, there is no preventing you from deciphering the text, even if it should have been falsified or mutilated by the telegraph,

For this triumph we are, again, indebted to electricity. Before flashing up, each letter is eight times permuted by electrical power. No purely mechanical apparatus possesses such a degree of capacity. Besides, each time each letter is taken from a different permutation alphabet. And all this may be done several millions of times without a pause.

You know that, in each language, the different letters occur with a different

frequency. Our machine makes away with this difference, which offers so many possibilities to every attempt of deciphering a text. Amongst a thousand letters the letter “e” occurs quite as many times as the letter “z”. The safety of working admits of no objection. There are many machines of ours that have been worked every day for many years without requiring any repair. The working is secured for 3 - 6 months, without any pause, by a regular little dry battery of 4 volts tension, lodged within the machine. In case of need one pocket-lamp battery is quite sufficient. The machine works almost without any noise. There is no clock mechanism making superfluous noise, needing permanent winding, and destroying the whole machine, whenever the spring is broken. Our machine “Enigma” is always ready for working.

DIMENSIONS AND WEIGHTS

The outer dimensions of the portable machine, lodged in an oakwood-box, are:

	Machine without box:	Box:
Breadth ...	25.5 cm	28.0 cm
Length ...	27.0 cm	29.0 cm
Height ...	11,5 cm	15.0 cm
Weight ...	6.77 kg	2.04 kg

Our machine is provided with a regular dry battery of 4 volts tension, which lasts about 3–4 months, if used freely every day. In case of need a common pocket-lamp battery is quite sufficient.

There are also connecting terminals for an accumulator of 4 volts tension.

Only use glow-lamps of 12.5 mm diameter and of hemispherical shape, such as are usually employed in the ordinary electric torch-lamps (3.5 volts, 0.2 amp.).

There are two spare-lamps R (II) on the right and left hand of the middle row of glow-lamps, between two white points, and ten at the inside of the lid of the box within a particular band,

WHAT CAPACITIES MUST A CIPHERING MACHINE POSSESS?

A ciphering machine must give a greater security than any handwriting system, be this ever so complicated. This is the principal condition to be fulfilled. But it must equally enable you to work more rapidly than with the list system, be this ever so simple. From these two principal conditions we may derive the following secondary ones and the following facts:

- a) From a merely practical point of view the rapidity of ciphering and deciphering may be called unlimited. Pressing down a key immediately makes appear the corresponding ciphered letter. The rapidity only depends on the degree of rapidity with which the eye can perceive the flashing-up letters. If not relieving a man from the necessity of seeking after the corresponding cipher in permutation alphabets, a machine is a failure being by no means superior to handwriting systems. This necessity of searching for things produces countless mistakes, wearies you rapidly and takes too much time, especially in case of long texts to be ciphered (for instance 500 letters).
- b) When discussing the rapidity of a machine, it would be a fault only to consider the time it takes you to transform the original text into ciphers, and vice versa. It is nearly quite as important that a machine should enable both the sender and the receiver to adjust the whole key within a minimum of time. If the very adjusting of the key for a telegram containing 10 words takes you 10 minutes, your machine is of no avail, for the hand works more rapidly with pen and list. Adjusting the whole key—(11 parts) of our machine (inside and outside) will not take you more than 70 to 80 seconds. The outside adjustment (including 450,000 possibilities), taking 10 seconds only, doesn't make you lose any time, then.
- c) In case of clerical mistakes, a machine must admit of repeating the last ten written letters, for instance. With our machine this can be done within five seconds.
- d) Errors and omissions occasioned by the telegraph must not delay the deciphering or render it impossible. With our machine, the omission of two groups of five letters will occasion a delay of 10 seconds only.
- e) Even if hidden in the text of a communication, the key must be easy to transmit. If a key be composed of 50 or 60 parts, a machine is not simple enough and liable to failure. The key of our machine consists, therefore, of eight letters and three figures only (of one digit each). Yet four letters are sufficient to give you about 450,000 possibilities, and this number will rise to 2,700,000 possibilities by employing 4 letters and 3 figures. Seven characters are easy to hide even in short communications. The other 4 letters will, moreover, offer you another series of 450,000 possibilities. There is, however, no need of them, because changing a single letter of the key, whatsoever it may be, will always change the whole system.
- f) It is a well-known fact that, in combining a number of objects in whatever manner you like, you will always obtain, besides numerous combinations

being very different from each other, a great deal showing but very slight differences and, therefore, being very similar to each other and liable to confusion. This circumstance must compel you to select your key with utmost carefulness, will make you lose considerable time and expose you to countless mistakes, not only when establishing your first key, but also in changing it in the course of your work. This annoying inconvenience is now, entirely, removed by our machine. It is so calculated that changing a single letter of a key in whatever manner you like, will always give a new system showing not the least likeness to that employed before. If, for instance, some text, for the first time, be ciphered with the aid of the outside key "ajkl", you will obtain quite a different text by employing, for the second time, the key "ajil" (the inside adjustment remaining the same). This secures you all the more from every attempt of unauthorized deciphering.

- g) Every exchangeable part of a machine that has to be transported independently from its body is liable to particular loss and damage. Every machine must be a coherent system. This ideal condition is entirely fulfilled by our machine. The exchangeable rollers (cylinders) are solidly joined with its body, and every exchange is exclusively effectuated by changing the path of the electric current.
- h) There are many ciphering apparatus employing the so called "letter of influence" as a particular means of increasing the "security" against deciphering. The nature of this method consists of changing the regular course of the working machine, whenever a certain letter, "n" for instance may occur in the original text, by hand, automatically, or by mental transformation of the key. This mode of producing is generally known and, from a theoretical point of view, not altogether useless. Yet, in practice, it is of no value at all. For every error of the telegraph, every omission, and every clerical mistake will render a ciphered document almost entirely undecipherable. Our machine doesn't exclude this method, but renders it superfluous, because of being, even without it, entirely protected from every inquisitiveness.

SECURITY AGAINST UNAUTHORIZED DECIPHERING

1. When discussing the security of a machine against unauthorized deciphering, you can never hope to succeed, for any length of time, in keeping secret the construction of the machine with all its accessories. It is, moreover, quite evident that you cannot change your key at every moment if it consists of 26 or 52 letters of one or two alphabets, and if a particular correspondence with

your friends, and, thus, a considerable while be needed, whenever another key is to be introduced. Our machine makes away with all that, it will take you some seconds only to change one letter of your key and, thus, to obtain an entirely different ciphered document. And it will take you no more than 30 or 40 seconds to change the whole key consisting of seven letters and figures. Even if the whole key of seven characters should become known, the remaining four letters secure the document from every attempt of deciphering. There is no difficulty whatever to change the whole key at any time.

2. To increase the security, keys can be divided, and each part entrusted to various persons. In case of the key list being lost, another key can immediately be established while writing, of you make a general stipulation. For instance, it can be agreed upon that, whenever the letter "z" occurs three times consecutively in a document to be deciphered, the next letter is to mean the outside key - letter with regard to a certain roller, or that every sixth, ninth, tenth and fourteenth letter of the text is to mean the outside position of the key. Such agreements, countless in theory, will protect you from treason as well as from the consequences of a key lost. We can never sufficiently emphasize the importance of the fact that, with our machine changing a single letter always changes the whole key without lengthening the text.
3. You are not always and everywhere in a position to put a machine in a locked-up iron-safe, when leaving a room for a moment. Nor are you able to prevent the machine being in service from being photographed inside and outside. Our machine need not be protected from photographers, even if they should take photos of the several parts. Without taking the whole machine to pieces nothing can be ascertained, and, with all that, it would still take an unauthorized person several hours to make out all connections established. But, moreover, whenever you are compelled to leave your working-room, be it for ever so short a while, you only need pass your hand slightly over the notched wheels of the ciphering rollers, thus destroying the key-adjustment in so radical a manner that nobody would be able to reconstruct it even by long years' labor and although he might possess a machine of the same kind and the same connections. With our machine, even a key discovered by treason given no fixed point to attempt of deciphering a document written with a changing key.
4. Every machine contains a certain number of fixed elements such as cog-wheels, notched wheels connection-joints etc. After having worked for a

certain time, each of these parts must return to the position it had when starting, and thus the whole machine, after having ciphered a certain number of letters, must return to its original position, the position it had before beginning to work. The time required for this return is called a "period". Now, if a machine have only a short period of about 300 letters, the original position will already reappear after every fifth line, and a clever man would be able to decipher the document on this basis, if it have any considerable length. Our machine has a "period" of about 8 or 10 typewritten pages so that even a long document will never exceed the period.

5. The security of a machine against deciphering depends by no means on gigantic figures. The "simple Caesar" (substitution of a letter for another) gives no less than 26 possibilities or a figure of 27 digits. By making use of this method four times consecutively we shall obtain fantastic figures (of more than 100 digits), which, however, are of no avail in practice, since no new combination can be secure unless giving a system that differs sufficiently from that employed before. v Our machine allows every possibility, a number which exceeds by far 100 digits. But we only speak of 2,700,000 possibilities, because these alone will give sufficiently different results. To find them out, you only need a perfect knowledge of all parts and connections of our machine.

6. Although gigantic figures cannot prove anything in favor of a machine, let us see which possibilities are offered by our machine!

Each one of the four ciphering cylinders can be connected in 26 ways. Thus we obtain a figure of 27 digits, or of more than 100 digits, when taking all the four cylinders together. Consequently it would be possible to provide each person in the world with several machines having the same adjustment. A key discovered by treason would be entirely useless, then. Well, but now the three cylinders on the right side can be exchanged as you like. Suppose you have only seven spare-cylinders, you would obtain about two million different keys, and would be able to cipher each text in two milliards of ways. That is to say: if a man were able to adjust, night and day, a new key at every minute, it would take him 4000 years to try all those possibilities through on after another. Do you see now that our machine can hold its ground against every attempt of this kind?

7. Yet, we must never forget that not every possible combination is at the same time a useful one. By combining the 26 keys of a typewriter, we obtain a gigantic number of possible keys, but every mathematician will tell you that no more than 60% are different enough to serve for practical purposes. It

is the greatest advantage of our machine that it excludes, from the very beginning, every useless combination, without any loss of time or labor. Changing one single letter of a key employed will always change the whole system in a radical manner.

INSTRUCTIONS FOR USE

I. KEY ADJUSTMENT

- a) Opening the lid and taking out the cylinders.

Put the switch-handle 5 (I & II) parallel to the right edge. Unscrew both lid-screws 12 (I) open the lid. Put the lever 9 (II) in a vertical position, push the reversing cylinder 11 (II) to the left, to stop, press together the three right ciphering cylinders (rollers) by the notched wheels, move them upwards, and pull them from the shaft. in order to be able to adjust the machine to the key agreed upon, the following manipulations are necessary:

- b) Selection of the cylinders and order of same.

From the existing ciphering cylinders take out those three which are required by the key agreed upon. Slide them on to the shaft in the stipulated order (collar of shaft to the left, letter-ring on left side of cylinder). Then put the cylinders in and shift the lever 9 (II) to the rear as far as stop,

- c) Adjustment of the rings upon the cylinders.

Removing the spring 7 (II) turn the letter-ring of each cylinder so far that the join of the rings upon the spring catches the hole beyond the letter which has been agreed upon. the cylinders.

- d) Outside adjustment of the letters in the windows.

the lid and turn the notched wheels till the letters agreed upon become visible in the windows.

- e) Combinations of the key

Let us take, for instance, the key (always start from left hand): II, III, I; G, X, M, Z; I, S, A, N.

1. The group II, III, I is to design the order of the cylinder, and means to say that the ciphering cylinders'4 (I & II) which bear these marks on the frontal side of the movable contacts have been put on the shaft in this order (counting from collar of shaft). If there are more than

three ciphering cylinders, the roman figures mean at the same time the cylinders to be selected.

2. The group G, X, M, Z means to say that the pin of the spring 7 (II) catches beneath the holes below these letters of the letter-rings.
3. The group Z, S, A, N means to say that these letters become visible in the windows 3 (I).

f) In round numbers 2.7 million of different and useful keys possible.

If possible, change the key so often that no more than 30 typewritten pages may be written with the same key. As nearly 3 millions of keys are given, this can easily be done and only depends on organization. Adding the possible change of letter-rings, possible you will obtain about 1000 milliards of possible keys.

g) Transmitting the key and keeping it secret.

If need be, the keys may be divided, and each part entrusted to another person.

In order to hide the key, various stipulations can be made between the correspondents. You may thus stipulate that the tenth, eleventh and twelfth letter of every communication is to mean the order of the cylinders mark them with letters) and that the eighteenth, twentieth and twenty-first letter is to mean the visible letters. If is, however, sufficient to change a single letter of the key in order to obtain a completely different text.

You may also stipulate that the number of the current month has to be added to the number of the place the transmitted key-letter occupies in the alphabet. For instance, if “B”, the second letter of the alphabet, is transmitted in the fourth month (April), you are to understand the sixth letter “F”

It is thus possible to find out many hundreds of protective measures against unauthorized use of keys which have become known. As a rule, it suffices to change every day the letters appearing in the windows, whereas the inside adjustment only need be changed every week or month.

II. CIPHERING

The switch-handle 5 (II & III) has to be set to “maximum” (hell). When the letters flash up too dimly, set it to “minimum” (dkl.). It is advisable to employ square paper for writing, The text is ciphered, letter by letter, by pressing down the keys 1 (I & II) as it is done when type-writers are being used. Each key must be sufficiently pressed down to make a lamp 2 (I & II) flash up. If intervals

between the words are desired, for instance, the key "X" may be pressed down after each word.

Examples:

Original Text:

' 'Bieten Sie bei Zwangsversteigerung bis vierzigtausend."

Ciphered Text:

afmuz pglae rillz lfiep mgrsa basti vwbac mxgyi noffe pbluo arl.

If figures are to be written, the first ten letters may, for instance, be employed instead of same in pressing down, in the same time, the key "Y". When passing from figures to letters, press the key "Y" down once more. In short: insert "X" before letters, "Y" before figures and other signs.

III. DECIPHERING

Every machine is available for deciphering as well as ciphering. Adjust the machine to the stipulated key, connect the current by turning the switch-handle 5 (I & III), and copy the ciphered document letter by letter, by pressing down the corresponding keys. Then the flashing-up letter will show the original text.

Examples:

Ciphered Text:

afmuz pglae rillz lfiep mgrsa basti vwbac mxgyi noffe pbluo arl.

Deciphered Text:

bieten x sie x bei x zwangsversteigerung x bis x vierzigtausend.

IV. CLERICAL ERRORS

Having pressed down, by mistake, a wrong key, put back, by two steps, the ciphering cylinder on the right side. Try the last correct letter once again, then, in order to see whether one of the other cylinders has moved together with the right one.

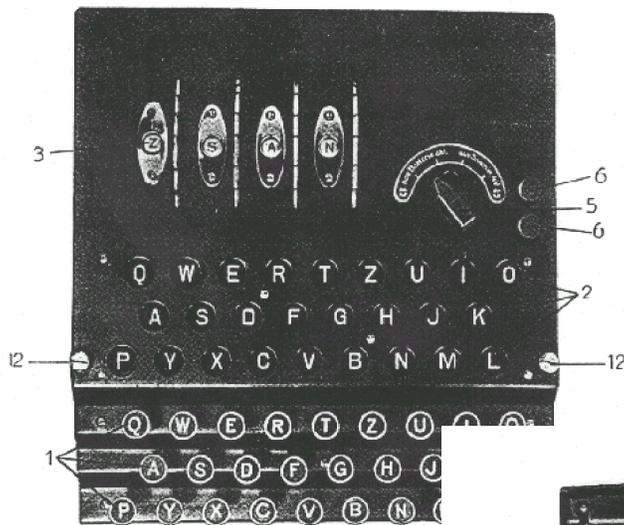
Having written but a few letters, you may, in order to repeat the twenty-third letter, for instance, press down any key you please twenty-two times, and then repeat the desired letter.

V. THE MACHINE TESTED IN PRACTICE

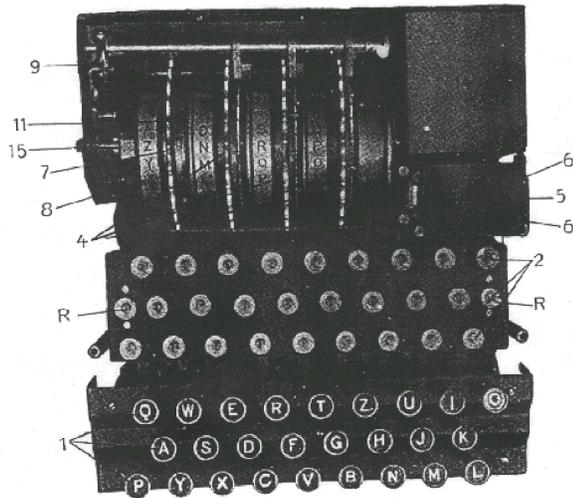
Being the result of many years' labor, our machine has been the object of countless trials and experiments under most unfavorable circumstances. If you treat the machine carefully, interruptions can scarcely take place, and, when occurring, easy to remove (see particular directions to be delivered with each machine.)

I

Ciphering and Deciphering Machine



II



- Illustration I, 11: 1. Key-board.
 " I, II: 2. Glow lamp board.
 " I: 3. Windows.
 " I, II: 4. Cipheryng cylinders (rollers).
 " I, II: 5. Switch-handle.
 " I, II: 6. Connecting terminals for accumulator working.
 " II: 7. Spring for adjusting the letter-ring.
 " II: 8. Letter-ring.
 " II: 9. Lever.
 " II: 11. Reversing cylinder.
 " II: 12. Lid screws.
 " II: 14. Dry battery.
 " II: 15. Guide pin.
 " II: R. Spare-lamps.

Explanation of the Illustrations I & II