

TOP SECRET

DIE LUECKENFUELLERWALZE (THE NOTCH FILLER WHEEL) (Knowledge of the Enigma Principle is Assumed)

The counter-like drive system of the three cipher wheels, the invariable, internal wiring of the wheels, the fixed assignment of the letters to the 26 keys and lamps, and the reciprocal effect of the reversing wheel - which results in the reciprocal structure of the cipher alphabets, have disadvantageous results for the security of the cryptograms.

Due to the fixed internal wiring of the wheels, 17,576 basic cipher alphabets can be derived with each wheel position and their sequence is fixed by the rigid, counter-like drive of the cipher wheels. The variable ring settings on the three wheels have only an insignificant influence on the change of this sequence. (Cyclic displacement.)

The plug connections merely have the effect of a substitution table on the derivation of the basic cipher alphabets, i. e. the characteristics of the cipher alphabets with respect to one another are preserved.

The drive of the three wheels is by three pawls and three ratchet wheels, one associated to each cipher wheel. On the settable rings of the cipher wheels there is in each case one notch. The settable ring of the right wheel in connection with the ratchet wheel of the middle wheel controls the stepping [of the middle wheel] and the ring of the middle wheel in connection with the ratchet wheel of the left wheel controls the stepping [of the latter]. The ring of the left wheel has no effect on the stepping. After 26 steps by the right wheel the middle wheel takes one step, after 26 steps by the middle wheel the left wheel and the middle wheel take one step independent of the function of the right wheel. This function causes the middle and right wheel to have a period of 650 steps instead of 676 possible steps.

1. Actually the order is reversed. The left drives the center, and the left and center drive the right. /Editor's note/

TOP SECRET

TOP SECRET

The machine constants (wheel wiring, drive notches, etc.) were included as security factors in the assessment of the machine when it was put into use. Assuming a knowledge of the machine, it did not satisfy present day security demands. The reconstruction of the entire daily key was possible by mechanical means provided 15 to 20 letters of enciphered X-text were given. (The letter X had to be enciphered 20 times as plain letter.)

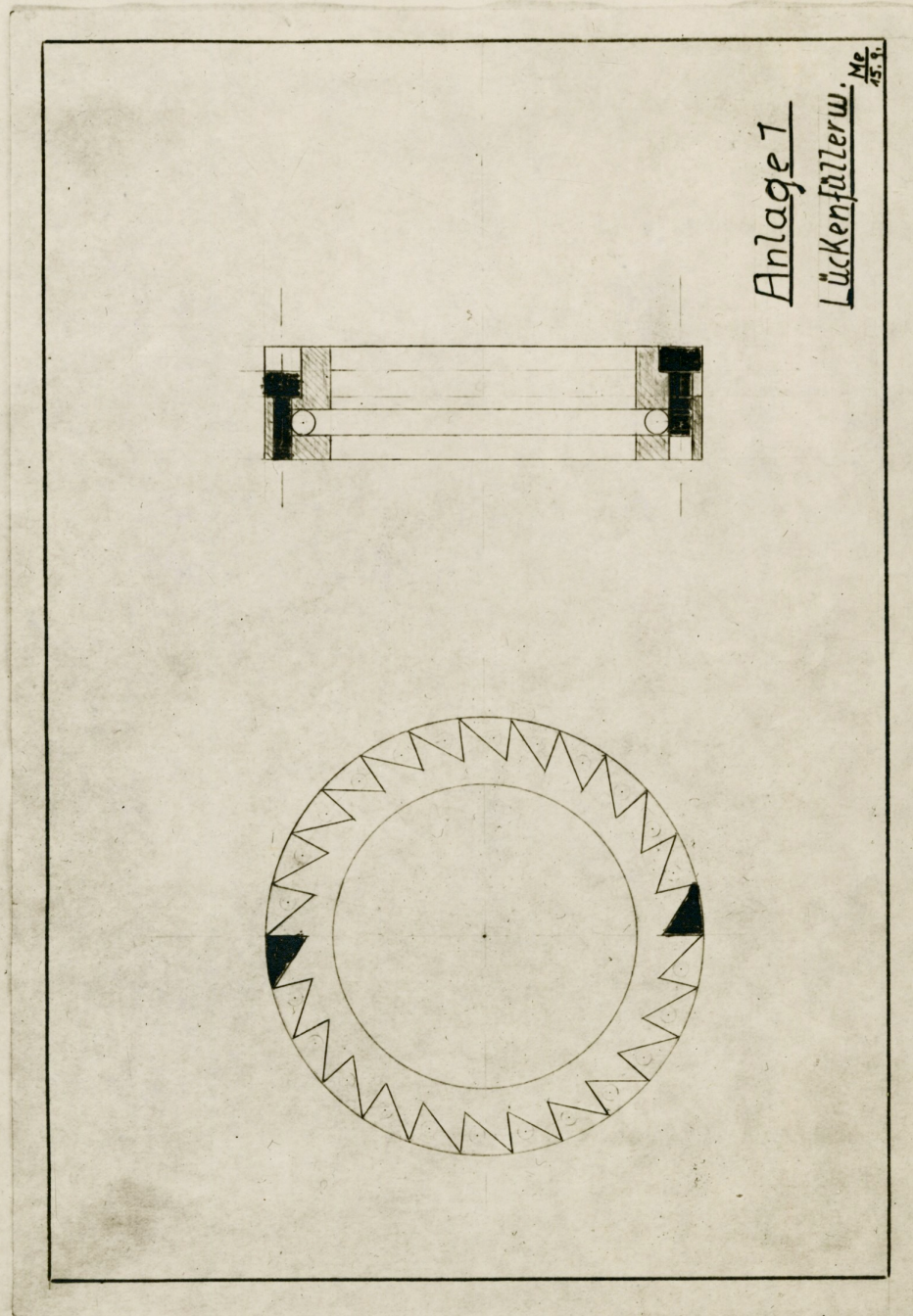
Recognition of this fact led to the development of the Lückenfüllerwalze. Lücke and Antriebskerbe (drive notch) are synonymous. Since the drive notch could be opened in the form of a pin at each of the 26 positions and could be filled again, this cipher wheel was given the name Lückenfüllerwalze. Since the construction is carried out only on the settable ring, only the ring with the notch fillers is represented in the supplement. In the case of the Lückenfüllerwalze, however, the ring is rigidly attached to the wheel.

When the Lückenfüllerwalze was put into use it was intended to have these drive notches effective daily in different arrangements. This measure involves a further shortening of the period by some 2000 steps but has a decided influence on the security of the resulting cryptograms.

Moreover other combinations on the Lückenfüllerwalze with respect to the number of effective notches can be employed. In this connection it should be remembered that the number of open notches shall not be a multiple of 2 or 13 and by increasing the number of effective notches the period is correspondingly shortened. It is also possible to subdivide the entire daily key, which in general is valid for 24 hours, by using different arrangements of the notch fillers.

TOP SECRET

TOP SECRET



TOP SECRET