

## Setting Up Enigma

*When two Enigma machines are set to the same key and their three wheels are in the same positions, the electrical connections through their steckerboards and scramblers will produce the same thirteen pairings of the twenty-six letters of the alphabet. . . . Thus, if pressing letter-key K on one of the machines causes lamp P to be lit, then pressing letter-key P on the other machine will cause lamp K to be lit. [27, p. 45]*

Two Enigma operators could communicate only if their Enigma machines were set up using the same key. Daily keys were provided to the operators in a book, for example, for a month at a time. There were several settings which made up the Enigma key. In 1932, the following made up the key.

**Plugboard:** The key specified which 6 pairs of letters were to be connected on the plugboard. For example, CO DI FR HU JW LS.

**Rotor order:** The key specified the order in which the rotors were placed in the rotor system (from left to right). For example, I III II.

**Ring setting:** There was a ring around the circumference of each rotor on which the letters of alphabet A, B, . . . , Z or the numbers 01, 02, . . . , 26 were engraved. This ring could be rotated around the circumference and then held in place with a pin. The ring setting of the key indicated the letter of the alphabet on the ring that corresponded to the position of the pin. For example, P K M. The purpose of the ring setting was to set the letters on the ring with respect to the internal wiring of the rotor. The permutations that were given in Section 3 for each rotor assume that the ring setting for each is A. Another effect was to position the turnover notch. The notch was in a fixed position on the left side of each rotor. Changing the ring setting changed the position of the turnover with respect to the internal wiring of the rotors.

**Groundsetting:** This portion of the key specified the position of each rotor at the beginning of sending or receiving a transmission. The groundsetting indicated which letter on each ring should be visible in the windows above the three rotors, for example, N K U. These settings made up the key.

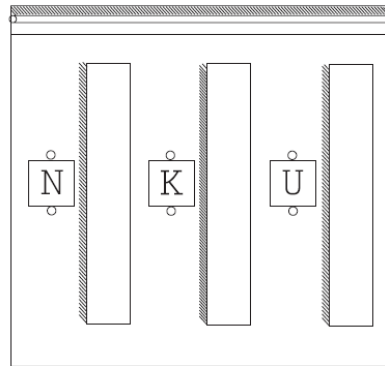


Figure 3 Enigma Rotor Cover closed with setting at NKU

## The Number of Enigma Keys

*[If] a man were able to adjust, day and night, a new key at every minute, it would take him 4000 years to try all those possibilities through on[e] after another.*

Mid-1920s Enigma sales brochure reprinted in the  
July 2001 *Cryptologia*. See [28, p. 252].

The security of Enigma depends on its having a large key space. The size of the keyspace equals the number of possible plugboard settings  $\times$  the number of possible rotor orders  $\times$  the number of possible ring settings  $\times$  the number of possible ground settings.

The number of possible plugboard settings: Assume that  $n$  plugs are being used. There are

$$\frac{[26 \times 25] \times [24 \times 23] \times [22 \times 21] \times \cdots \times [(26 - 2n + 2) \times (26 - 2n + 1)]}{2^n \times n!}$$

ways to connect  $n$  plugs into the plugboard. Here is a table which shows the number of connections for each of the possible number of plugs.

$n$	Number of connections	$n$	Number of connections
0	1	7	1,305,093,289,500
1	325	8	10,767,019,638,375
2	44,850	9	53,835,098,191,875
3	3,453,450	10	150,738,274,937,250
4	164,038,875	11	205,552,193,096,250
5	5,019,589,575	12	102,776,096,548,125
6	100,391,791,500	13	7,905,853,580,625

When the Poles began to attack Enigma, six plugs were in use. So, there were 100,391,791,500 ways to connect the six plugs into the plugboard. Later the Germans used ten plugs.

The number of possible rotor orders: There are six ways to arrange the three rotors in order in the rotor system.

The number of possible ring settings: Only the positions of the notches on the right-hand and middle rotors contributed to the cryptographic security of Enigma. So, we will say that there are  $26^2 = 676$  possible ring settings.

The number of possible groundsettings: There are  $26^3 = 17576$  choices of the letters to appear in the windows.

So, effectively, the number of possible keys was

$$100,391,791,500 \times 6 \times 676 \times 17576 = 7,156,755,732,750,624,000$$

which would seem to be secure enough.