2 Mathematical Description

Here we give a mathematical description of the Enigma I ("Wehrmachts-Enigma") with 5 selectable rotors denoted by the roman numerals I to V (whereas the arabic numerals 1 to 3 denote the order in which three rotors are mounted). For a bit of mathematical background on permutations we refer to Appendix A.

The Key Space

The key of an Enigma message has several components:

- The operator choses 3 rotors from a set of 5 and mounts them in a certain order. This gives $\frac{5!}{2!} = 60$ different options ("Walzenlage").
- He adjusts each of the 3 alphabet rings to one of 26 possible positions. This gives another $26^3 = 17576$ options. Since the alphabet ring of the slow rotor has no effect on the encryption, only $26^2 = 676$ of these options contribute to the key space.
- He inserts 10 plugs into the plugboard. Each plug connects 2 letters. He has $\frac{26!}{(2^{10}\cdot 10!\cdot 6!)} = 150{,}738{,}274{,}937{,}250 \approx 1.5 \cdot 10^{14} \approx 2^{47}$ different choices. This formula is derived in Appendix A. If the operator is allowed to use also less than the maximum 10 plugs this number grows to about $2.1 \cdot 10^{14}$.
- Finally he sets the rotors to their initial positions, another $26^3 = 17576$ possibilities.

Multiplied together these numbers make up a key space of

$$60 \cdot 676 \cdot 150{,}738{,}274{,}937{,}250 \cdot 17576 = 107{,}458{,}687{,}327{,}250{,}619{,}360{,}000$$
$$\approx 10^{23} \approx 1.4 \times 2^{76}$$

or a key length of 76 bits (in modern language). However it is not clear at all (and even hardly likely) that all keys define different substitutions. Therefore we can conclude only that the effective key length is *at most* 76 bits. And 47 of these bits are due to the plug-board.

The Control Logic

The current flows through the three movable rotors first from right to left. Accordingly we denote the fast rotor by 1, the middle one by 2, and the slow one by 3. Taking the irregularity in the stepping of rotor 2 into account, and denoting the position of the notch that moves the next rotor by m_i, the formula for the state transition function is

$$g(z_1, z_2, z_3) = (z_1, z_2 + \lambda_1(z_1) + \lambda_1(z_1)\lambda_2(z_2), z_3 + \lambda_1(z_1)\lambda_2(z_2))$$

where $\lambda_i(x) = \delta_{x,m_i}$ is the KRONECKER symbol.

Due to the direction of the labeling of the rotors and the corresponding wiring between input keys or output bulbs and rotors, the substitution by a single rotor in step i is $\rho^{(i)} = \tau^{-i} \circ \rho \circ \tau^i$ where ρ is the rotor substitution and τ the alphabet shift, as explained in Chapter 5.1.

The Enigma Substitution

The rotors being in the state $z = (z_1, z_2, z_3)$ the rotor substitution describes the effect of transversing them from right to left:

$$\sigma_z := \rho_3^{(z_3)} \circ \rho_2^{(z_2)} \circ \rho_1^{(z_1)}$$

The effect of the reflecting rotor is a proper involution π, no element is mapped to itself. The plug-board also provides an involution, η. Together this gives the **Enigma substitution** in state z:

$$\rho_z = \eta^{-1} \circ \sigma_z^{-1} \circ \pi \circ \sigma_z \circ \eta$$

or, with more details, the **Enigma equation** for encryption

$$c_i = \eta^{-1}\tau^{-z_1}\rho_1^{-1}\tau^{z_1-z_2}\rho_2^{-1}\tau^{z_2-z_3}\rho_3^{-1}\tau^{z_3}\pi\tau^{-z_3}\rho_3\tau^{z_3-z_2}\rho_2\tau^{z_2-z_1}\rho_1\tau^{z_1}\eta\,(a_i)$$

Theorem 1 *The Enigma substitution ρ_z in state z is a proper involution.*

Proof. a) Involution:

$$\rho_z^{-1} = \eta^{-1} \circ \sigma_z^{-1} \circ \pi^{-1} \circ \sigma_z \circ \eta = \rho_z$$

since $\pi^{-1} = \pi$.

b) Proper: Assume $\rho_z(s) = s$ for a letter $s \in \Sigma$. Then

$$\sigma_z\eta(s) = \sigma_z\eta\rho_z(s) = \pi\sigma_z\eta(s)$$

hence $\pi(t) = t$ for $t = \sigma_z\eta(s) \in \Sigma$. This contradicts the fact that π is a proper involution. $\diamond$

Note. The proof didn't use the fact that η is an involution. This limitation of the plug-board had purely practical reasons: It reduced errors in operation. Variable plugs between the keyboard or light-bulbs and the first rotor would give more degrees of freedom. But this would require 26 cables instead of the 10 double-plug cables.