2 Mathematical Description of Rotors

Identify the alphabet Σ with $\mathbb{Z}/n\mathbb{Z}$, the integers $\bmod n$. Let ρ be the monoalphabetic substitution that the rotor performs in its initial position. Moving the rotor by one position forward the new substitution is

$$\rho^{(1)}(a) = \rho(a-1) + 1$$

Denote by τ the shift by 1 of the alphabet $\Sigma = \mathbb{Z}/n\mathbb{Z}$, that is $\tau(a) = a + 1$. Then the formula looks like this:

$$\rho^{(1)}(a) = \tau\rho\tau^{-1}(a)$$

By induction we immediately get part (i) of the following theorem:

Theorem 1 (The secondary alphabets of a rotor)

(i) *If a rotor in its initial position performs the substitution with the primary alphabet ρ, then after rotation by t positions forward it performs the substitution with the conjugate alphabet $\rho^{(t)} = \tau^t\rho\tau^{-t}$. In particular all secondary alphabets have the same cycle type.*

(ii) *The diagonals of the corresponding alphabet table each contain the standard alphabet (cyclically wrapped around).*

Proof. Assertion (i) is proved above. Assertion (ii) follows immediately by interpreting it as a formula:

$$\rho^{(i)}(j) = \tau^i\rho\tau^{-i}(j) = \rho(j-i) + i = \rho^{(i-1)}(j-1) + 1$$

$\diamond$

The definition of "cycle type" was given in Appendix A.

The formula makes it obvious why—in contrast with the cipher disk—for a rotor the (unpermuted) standard alphabet is completely useless: It corresponds to the identity permutation, therefore all its conjugates are identical.

In general the conjugate alphabet $\rho^{(t)}$ is identical with the primary alphabet ρ if and only if ρ is in the centralizer of the shift τ^t. The designer of a rotor might wish to avoid such wirings.

Examples.

1. If n is a prime number, then all the shifts τ^t for $t = 1, \ldots, n-1$ are cycles of length n. Therefore all their centralizers are identical to the cyclic group $< \tau >$ spanned by τ. If the designer avoids these n trivial wirings, then all the n conjugated alphabets are distinct.

2. If $\gcd(t,n) = d > 1$, then τ^t splits into d cycles of length $\frac{n}{d}$, $\tau^t = \pi_1 \cdots \pi_d$, and centralizes all permutations of the type $\pi_1^{s_1} \cdots \pi_d^{s_d}$. These are not in the cyclic group $< \tau >$ unless all exponents s_i are congruent mod $\frac{n}{d}$.
3. In the case $n = 26$ the shifts τ^t are cycles, if t is coprime with 26. However τ^t splits into two cycles of length 13, if t is even. All the powers τ^t, t even, $2 \leq t \leq 24$, span the same cyclic group because 13 is prime. The permutation τ^{13} splits into 13 transpositions. For example τ^2 centralizes the permutation $(ACE \ldots Y)$, and τ^{13} centralizes the transposition (AB), where we denoted the alphabet elements by the usual letters A, ..., Z. Therefore in wiring the rotors the designer should avoid the centralizers of τ^2 and of τ^{13}.