3 Mathematical Description of Cylinder Ciphers

This section assumes knowledge of the mathematical excursion to permutations in the Appendix to the Chapter on monoalphabetic ciphers.

Parameters

A cylinder cipher depends on the following parameters:

- The number $n = \#\Sigma$ of letters in the alphabet Σ
- The number q of disks, where $q \geq 1$. If all disks are different, then $q \leq (n-1)!$. [See below for an explanation why we don't need to take $n!$ for the upper bound.]
  - Each disk is characterized by a permutation $\tau \in \mathcal{S}(\Sigma)$.
  - Therefore the collection of disks can be described as a q-tuple $(T_1, \ldots, T_q) \in \mathcal{S}(\Sigma)^q$.

  Assume the disks are numbered from 1 to q.
- The number l of selected disks, where $1 \leq l \leq q$
  - The key is a sequence $(\tau_0, \ldots, \tau_{l-1})$ consisting of different members of the q-tuple $(T_1, \ldots, T_q)$, and described by the corresponding sequence of numbers in $[1 \ldots q]$.
  - The number of choices for the key is

    $$\#K = q \cdot (q-1) \cdots (q-l+1) = \frac{q!}{(q-l)!}$$

    some of which could coincide if some of the disks have identical alphabets.

Examples

Jefferson **cylinder:** $l = q = 36$, $\#K = 36!$, effective key length ≈ 138.

Bazeries **cylinder:** $l = q = 20$, $\#K = 20!$, effective key length ≈ 61.

M-94: $l = q = 25$, $\#K = 25!$, effective key length ≈ 84.

M-138-A: $l = 30$, $q = 100$, $\#K = 100!/70!$, effective key length ≈ 190.

Encryption and Decryption

The cylinder cipher is polyalphabetic with period l, the number of disks on the cylinder.

Attention: Don't confuse the permutation $\tau \in \mathcal{S}(\Sigma)$ written on the circumference of the disk with the permutation $\sigma \in \mathcal{S}(\Sigma)$ that defines the substitution alphabet realized by the disk. We subsequently examine the relationship between these two permutations.

As usual identify the alphabet Σ (in a fixed order) with $\mathbb{Z}/n\mathbb{Z}$, the integers mod n. Then, using the first generatrix, encrypting a plaintext block $(a_0, \ldots, a_{l-1})$ looks like this:

a_0	$\ldots$	a_i	$\ldots$	a_{l-1}
		$\tau_i(0)$		
		$\vdots$		
Search entry x such that		$\tau_i(x)$	$= a_i$	
		$\tau_i(x+1)$	$= c_i$	corresponding cipher letter
		$\vdots$		
		$\tau_i(n-1)$		

where the center column $\tau_i(0), \ldots, \tau_i(n-1)$ represents the marking of the i-th disk. Therefore

$$c_i = \tau_i(x+1) = \tau_i(\tau_i^{-1} a_i + 1)$$

The corresponding decryption function is

$$a_i = \tau_i(\tau_i^{-1} c_i - 1)$$

This derivation proves:

Theorem 1 (Cylinder Cipher Theorem) *The relation between the permutation $\tau \in \mathcal{S}(\Sigma)$ written on the circumference of the disk and the permutation $\sigma \in \mathcal{S}(\Sigma)$ that defines the substitution alphabet realized by the disk using the first generatrix is given by the formulas*

$$\begin{aligned} \sigma(a) &= \tau(\tau^{-1} a + 1) \\ \sigma^{-1}(c) &= \tau(\tau^{-1} c - 1) \end{aligned}$$

Or in other words: σ is a cyclic permutation and τ is the cycle representation of σ.

There are $(n-1)!$ different cycles of length n. As n different disk definitions τ result in the same cyclic permutation σ we could make the restriction $q \leq (n-1)!$ for the number of possible different disks.

Corollary 1 *Using the j-th generatrix the formulas become*

$$\begin{aligned} \sigma_j(a) &= \tau(\tau^{-1}a + j) \\ \sigma_j^{-1}(c) &= \tau(\tau^{-1}c - j) \end{aligned}$$

if we denote by σ_j the substitution by the j-th generatrix.

Example: Let $\Sigma = \{\mathrm{A}, \ldots, \mathrm{Z}\}$, and let the disk inscription be

$$\tau = \text{QWERTZUIOPASDFGHJKLYXCVBNM}$$

Then σ is the permutation

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
S N V F R G H J O K L Y Q M P A W T D Z I B E C X U
```