# 4 Mathematical Description of Periodic Polyalphabetic Substitution

## The General Case

In general a periodic polyalphabetic cipher has a key space $K \subseteq \mathcal{S}(\Sigma)^l$, consisting of sequences of $l$ permutations of the alphabet $\Sigma$. The key $k = (\sigma_0, \ldots, \sigma_{l-1})$ defines the encryption function $f_k\colon \Sigma^r \longrightarrow \Sigma^r$ given by

$$\begin{array}{cccccccccc}
a_0 & a_1 & \ldots & a_{l-1} & a_l & \ldots & a_i & & \ldots & a_{r-1} \\
\downarrow & \downarrow & & \downarrow & \downarrow & & \downarrow & & & \\
\sigma_0 a_0 & \sigma_1 a_1 & \ldots & \sigma_{l-1} a_{l-1} & \sigma_0 a_l & \ldots & \sigma_{i \bmod l} a_i & \ldots & \ldots &
\end{array}$$

The componentwise encryption formula for $c = f_k(a) \in \Sigma^r$ is

$$c_i = \sigma_{i \bmod l}(a_i),$$

and the formula for decryption

$$a_i = \sigma_{i \bmod l}^{-1}(c_i).$$

## Effective Key Length

### Bellaso Cipher

The primary alphabet is the standard alphabet, and we assume the cryptanalyst knows it. The key is chosen as word (or passphrase) $\in \Sigma^l$. Therefore

$$\begin{aligned}
\#K &= n^l, \\
d(F) &= l \cdot \log_2(n).
\end{aligned}$$

For $n = 26$ this amounts to $\approx 4.70 \cdot l$. To avoid exhaustion $l$ should be about 10 (pre-computer age), or about 20 (computer age). However there are far more efficient attacks against this cipher than exhaustion, making these proposals for the key lengths obsolete.

### Disk Cipher

The key consists of two parts: a permutation $\in \mathcal{S}(\Sigma)$ as primary alphabet, and a keyword $\in \Sigma^l$. Therefore

$$\begin{aligned}
\#K &= n! \cdot n^l, \\
d(F) &= \log_2(n!) + l \cdot \log_2(n) \approx (n + l) \cdot \log_2(n)
\end{aligned}$$

For $n = 26$ this amounts to $\approx 4.70 \cdot l + 88.38$.

If the enemy knows the primary alphabet, say be capturing a cipher disk, the effective key length reduces to that of the Bellaso cipher.

### A More General Case

For a periodic polyalphabetic cipher that uses $l$ independent alphabets,

$$\begin{aligned} K &= \mathcal{S}(\Sigma)^l, \\ d(F) &= \log_2((n!)^l) \approx nl \cdot \log_2(n). \end{aligned}$$

For $n = 26$ this is about $88.38 \cdot l$.

## Another View

An $l$-periodic polyalphabetic substitution is an $l$-gram substitution, or block cipher of length $l$, given by the product map

$$(\sigma_0, \ldots, \sigma_{l-1})\colon \Sigma^l = \Sigma \times \cdots \times \Sigma \longrightarrow \Sigma \times \cdots \times \Sigma = \Sigma^l,$$

that is, a monoalphabetic substitution over the alphabet $\Sigma^l$. In particular the BELLASO cipher is the shift cipher over $\Sigma^l$, identified with $(\mathbb{Z}/n\mathbb{Z})^l$.

For $\Sigma = \mathbb{F}_2$ the BELLASO cipher degenerates to the simple XOR on $\mathbb{F}_2^l$.