4 Monoalphabetic Substitution

Introductory Example

The key of a monoalphabetic substition is a permutation of the alphabet, for example:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
UNIVERSTABCDFGHJKLMOPQWXYZ
```

For encryption locate each letter of the plaintext in the first row of this table, and replace it by the letter below it. In our example this becomes:

```
ENGLI SHAST RONOM ERWIL LIAML ASSEL LDISC OVERE DTRIT ON
EGSDA MTUMO LHGHF ELWAD DAUFD UMMED DVAMI HQELE VOLAO HG
```

For decryption we use the inverse permutation, given by the table

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
IJKLEMNOCPQRSBTUVFGHADWXYZ
```

Mathematical Description

Let $\mathcal{S}(\Sigma)$ be the group of permutations of the alphabet Σ, that is the full symmetric group. See Appendix A for an introduction to permutations.

A monoalphabetic substitution consists of the elementwise application of a permutation $\sigma \in \mathcal{S}(\Sigma)$ to texts:

$$f_\sigma(a_1, \ldots, a_r) := (\sigma a_1, \ldots, \sigma a_r) \quad \text{for } (a_1, \ldots, a_r) \in \Sigma^r.$$

Definition A **monoalphabetic cipher** over the alphabet Σ with keyspace $K \subseteq \mathcal{S}(\Sigma)$ is a family $(f_\sigma)_{\sigma \in K}$ of monoalphabetic substitutions.

Examples 1. The shift cipher where $K =$ the set of right translations.

2. The general monoalphabetic cipher where $K = \mathcal{S}(\Sigma)$. Here $\#K = n!$ with $n = \#\Sigma$.

The Effective Key Length

The general monoalphabetic cipher F defeats the exhaustion attack, even with computer help. The $n!$ different keys define $n!$ different encryption functions. Therefore

$$d(F) = \log_2(n!) \geq n \cdot [\log_2(n) - \log_2(e)] \approx n \cdot \log_2(n)$$

by Stirling's formula, see Appendix B. For $n = 26$ we have for example

$$n! \approx 4 \cdot 10^{26}, \quad d(F) \approx \log_2(26!) \approx 88.38.$$

Note that for a ciphertext that doesn't contain all letters of the alphabet the search is somewhat faster because the attacker doesn't need to determine the entire key.