Summary of Theory for Block 0

Viktor Rosvall

Mars 2019

The main types of encryption

In **Transportation ciphers** encryption is done by changing the ordering of letters in plaintext systematically. A **Substitution cipher** is done by scrambling the letters of a plain-text. An example of this is the *Caesar cipher*, which encrypts plaintext by shifting the letters of the alphabet 3 times to the right (the key), and decrypts by shifting 3 times to the left. This is called a *Shift cipher* and isn't very secure due to the low key-space. There are 2 kinds of Substitution ciphers: *mono-alphabetic* (letters are always encrypted the same) and *poly-alphabetic* (a latter may be encrypted differently depending on it's position in the plaintext). There are 3 kinds of attacks on ciphers: *ciphertext-only*, *known-plaintext* and chosen-plaintext. A cipher must be able to withstand a chosen-plaintext attack.

Permutations

Let $N_n = \{1, 2, 3, ..., n\}$ be an alphabet with n letter. A permutation of plaintext can be seen as a bijective function: $\alpha : N_n \to N_n$

Notation

Permutations can be written in both **matrix notation** and **disjoint cycle notation**:

$$N_n = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 2 & 5 & 3 & 4 \end{pmatrix}$$