Summary of Block 0 Theory

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: $\alpha : N_n \to N_n$

Permutations can be written in both **matrix notation**:

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

and **cycle notation**, also called *disjoint cycle notation*:

$$\alpha = (1\ 2)\ (3\ 5\ 4)$$

The product of two permutations $\alpha, \beta : N_n \to N_n$ is the composite function $\alpha \bullet \beta$, defined as:

$$\alpha \bullet \beta(x) = \alpha(\beta(x)) \quad \forall x \in N_n$$

The *inverse* of α^{-1} can be found by swapping the rows in a matrix notation and ordering them. The product of α and α^{-1} is the *identity* permutation i of N_n.

S_n is the set of all permutations of N_n. S_n is called the *symmetric group of degree n*. The number of permutations can be counted as $n!$ which is the order of $S_n \quad \forall n \in Z_+$.

A **k-cycle** in S_n is a permutation which moves k element of N_n in a cycle and does nothing to the remaining elements os N_n.