MA080G Cryptography Summary of Block 0 Theory

Viktor Rosvall

April 8, 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 plaintext. 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: *monoalphabetic* (letters are always encrypted the same) and *polyalphabetic* (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.

Counting

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 $S_n \quad \forall n \in Z_+$.

The number of permutations of type $[1^{\alpha_1}2^{\alpha_2}...n^{\alpha_n}]$ can be calculated as:

$$\frac{n!}{1^{\alpha_1}2^{\alpha_2}...n^{\alpha_n}\alpha_1\alpha_2...\alpha_n}$$

Where the base is the loop size, and α is the number of loops

Example: The number of permutations of type $[2^3 3^2]$ on S_{12} can be calculated as:

$$\frac{12!}{2^3 3^2 3!2!}$$

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

Relations

Main Theorem 12.5 in [Biggs]
Two permutations in S_n are conjugate if and only if they have the same type.

The *conjugacy relation* $\sim$ is an *equivalence relation* on S_n, is defined by $\alpha \sim \beta$ if α, β are conjugate permutations in S_n.

The *transposition* T is always of type 2: $[2^1]$. It can be used to split cycles or combine them. When you apply a transposition, you always get one more or less cycles.

Theorem 12.6.2
Let $n > 2$ be an integer. Half the permutations in S_n are even and half are odd.

Modulo n Arithmetic

The congruence relation (mod n):

$$\forall a, b \in Z \quad a \equiv b(mod\ n) \quad \iff \quad n|(a-b)$$

$\forall x \in Z$ there is a *unique* $r \in \{0, 1, ..., n-1\}$ such that

$$x \equiv r(mod\ n)$$

MOD n definition:
For any positive integer n define a function called MOD n (% operator):

$$MOD\ n : Z \rightarrow \{0, 1, ..., n-1\}$$

is given by the rule

$$x\ MOD\ n = r$$

if $r \in \{0, 1, ..., n-1\}$ and $x \equiv r(mod\ n)$

Euclid's algorithm

We can use Euclid's algorithm to find the *greatest common divider*, (gcd) of two integers. The gcd can be calculated by using the Division Theorem on successive remainders, covered in Discrete Mathematics block 3, or by a recursive one-line program [Cameron 2.7]:

$$\textbf{if } b = 0 \textbf{ then } gcd(a, b) = a \textbf{ else } gcd(a, b) = gcd(b, a\ MOD\ b) \textbf{ fi}$$

For example:

$$gcd(30, 8) = gcd(8, 6) = gcd(6, 2) = gcd(2, 0) = 2$$

By running the algorithm from block 3 backwards we can find the linear combination of 2 integers.

Euler's function

Only elements $[a] \in Z_n$ with $gcd(a, n) = 1$ has a multiplicative inverse.

φ definition:
Euler's φ function is the function on the natural numbers $n \geq 2$ given by:

$$\varphi(n) = \#\text{ congruence classes } [a] \in Z_n \text{ such that } gcd(a, n = 1)$$

So φ counts the number of invertible elements of Z_n.

Theorem
Let $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$ where $p_1, p_2, ..., p_r$ are distinct primes and $a_1, a_2, ..., a_r > 0$. Then:

$$\varphi(n) = p_1^{a_1-1}(p_1 - 1)p_2^{a_2-1}(p_2 - 1)...p_r^{a_r-1}(p_r - 1)$$

Example:

$$20 = 2^2 * 5 \quad \text{so} \quad \varphi(20) = 2^{2-1}(2 - 1)5^{1-1}(5 - 1) = 2 * 1 * 4 = 8$$

Monoalphabetic Substitution ciphers

We permute the plaintext, substituting each letter to a number. In the English alphabet we have a key-space of 26!.

This key-space is too large for a brute force attack, but it's still possible to easily break a monoalphabetic cipher by looking at the *letter frequencies* in the ciphertext. By replacing the letters of digrams and trigrams in the ciphertext, to letters that's common in the English alphabet, we can break the cipher.