MIDTERM EXAM

1. (a) Define groups. **(2 points)**

   (b) Let G be the group of isometries of a regular triangle. Prove that if $a \in G$ is an isometry, and N is a positive integer, then a^N can be computed in polynomial time. **(4 points)**

Solution. (a) We say that a set G together with a binary operation $*$ is a group, if the following three axioms hold:

- for any $x, y, z \in G$, $(x * y) * z = x * (y * z)$;
- there exists $e \in G$ such that for any $x \in G$, $x * e = e * x = e$;
- for any $x \in G$, there exists $y \in G$ such that $x * y = y * x = e$.

(b) We learned in class that $\#G = 6$. By Lagrange's theorem, the order of any element divides the order of the group, therefore $o(a) \mid \#G$. This means that if $M \equiv N \bmod 6$, then

$$a^M = a^N.$$

Indeed, assume $M > N$, then we may write $M - N = 6k = o(a)l$ for some $k, l \in \mathbf{N}$. Then

$$a^M = a^{N+o(a)l} = a^N \mathrm{id}^l = a^N.$$

Therefore, a^N in the original question depends only on the residue class of N modulo 6. This can be computed by the euclidean division which we learned to be done in polynomial time, i.e.

$$N = 6n + d,$$

where $0 \leqslant d < 5$, and this value d can be computed from N in polynomial time. Now compute a^d which takes only a constant time, and is equal to a^N.

2. (a) Describe the simple substitution cipher. **(2 points)**

   (b) Alice and Bob communicate using the simple substitution cipher. Eve constructs a computer which tries 10 million possible keys per second. Can this computer break the cipher in a lifetime? (To break the cipher, assume the computer has to try all possible keys.) **(4 points)**

Solution. (a) In the simple substitution cipher, both $\mathscr{M}$ and $\mathscr{C}$ are set of the letters of the alphabet $\mathfrak{A}$:

$$\mathscr{M} = \mathscr{C} = \mathfrak{A} = \{\mathtt{a},\mathtt{b},\mathtt{c},\mathtt{d},\mathtt{e},\mathtt{f},\mathtt{g},\mathtt{h},\mathtt{i},\mathtt{j},\mathtt{k},\mathtt{l},\mathtt{m},\mathtt{n},\mathtt{o},\mathtt{p},\mathtt{q},\mathtt{r},\mathtt{s},\mathtt{t},\mathtt{u},\mathtt{v},\mathtt{w},\mathtt{x},\mathtt{y},\mathtt{z}\}.$$

The key set $\mathscr{K}$ is the group of permutations of $\mathfrak{A}$:

$$\mathscr{K} = \{k : k \in \text{Perm}(\mathfrak{A})\}.$$

Given a letter, the key k acts on it via the permutation, i.e.

$$e_k(m) = k(m).$$

As for the decryption, it is given by the inverse permutation. Formally,

$$d_k(c) = k^{-1}(c).$$

(b) The number of possible keys is 26!. The number of operations is

$$10^7/\text{sec} < 10^9/\text{minute} < 10^{11}/\text{hour} < 10^{13}\text{day} < 10^{16}/\text{year},$$

which is less than 10^{19} in 1000 years, which is safe to say to be longer than a lifetime.

In 26!, there are 17 factors not smaller than 10 (namely, the numbers $10, 11, \ldots, 26$). Also, $2 \cdot 9$ and $3 \cdot 8$ are both bigger than 10, so

$$26! > 10^{19},$$

therefore the computer cannot try all keys in a lifetime.

3. (a) Describe the pseudorandom number generators. **(2 points)**

   (b) Assume that there exists a pseudorandom number generator R. Prove then that there exists another pseudorandom number generator R'. (By another, we mean that for any $k \in \mathscr{K}$, there exists at least one $n \in \mathbf{N}$ such that $R'(k,n) \neq R(k,n)$.) **(4 points)**

Solution. (a) A pseudorandom number generator is a function $R : \mathscr{K} \times \mathbf{N} \to \{0,1\}$ satisfying the conditions:

- for any $k \in \mathscr{K}$, $j \in \mathbf{N}$, it is easy to compute $R(k, j)$;
- from any $j_1, \ldots, j_n$ and corresponding $R(k, j_1), \ldots, R(k, j_n)$, it is hard to figure out k;
- from any $j_1, \ldots, j_n$ and corresponding $R(k, j_1), \ldots, R(k, j_n)$, it is hard to guess the value of $R(k, j)$ with better than a 50% chance of success, if $j \notin \{j_1, \ldots, j_n\}$,

(b) Assume $R(k,n)$ is a pseudorandom number generator. Consider the function $R'(k,n) = 1 - R(k,n)$. Then clearly $R' : \mathscr{K} \times \mathbf{N} \to \{0,1\}$, and we see that all requirements are fulfilled. Indeed, the easy computability of $R'(k,n)$ from k and n is just the same as that of $R(k,n)$, we only have to compute $R(k,n)$ (which is easy by assumption), then alter the resulting bit. Also, if there were a fast algorithm to figure out k from $R'(k, j_1), \ldots, R'(k, j_n)$, then this is nothing else but computing k easily from $1 - R(k, j_1), \ldots, 1 - R(k, j_n)$, that is, from $R(k, j_1), \ldots, R(k, j_n)$. Finally, a guess from $R(k', j_1), \ldots, R(k', j_n)$ to $R(k', j)$ with better than a 50% chance can be translated to R: take the values $R(k, j_1), \ldots, R(k, j_n)$ alter each bit, apply the 'good guess' algorithm of R', then alter the resulting bit again.

On the other hand, it is easy to see that R' is other than R: $R'(k,n) \neq R(k,n)$ for any $k \in \mathscr{K}$ and any $n \in \mathbf{N}$.

4. (a) Describe the chosen plaintext attack. **(2 points)**

   (b) For a prime p, let $\mathscr{M}, \mathscr{C} = \mathbf{F}_p$, $\mathscr{K} = (\mathbf{F}_p^\times, \mathbf{F}_p)$, and for $m \in \mathscr{M}, k = (k_\times, k_+) \in \mathscr{K}$ (i.e. $k_\times \in \mathbf{F}_p^\times$ and $k_+ \in \mathbf{F}_p$), let $e_k(m) = k_\times m + k_+$. Prove that this cryptosystem is vulnerable against the chosen plaintext attack. How many pairs $(m, e_k(m))$ are needed to reveal k? **(4 points)**

Solution. (a) In the chosen plaintext attack, Eve convinces Alice to encrypt a few messages $m_1, \dots, m_n$. Then, knowing the pairs $(m_1, e_k(m_1)), \dots, (m_1, e_k(m_1))$, she may try to figure out what the key k can be, or at least to decrypt any cipher $c = e_k(m)$.

(b) In the given example, we prove that the given cryptosystem is vulnerable against the chosen plaintext attack in the sense that if Eve learns two pairs $(m_1, e_k(m_1)), (m_2, e_k(m_2))$ (with $m_1 \neq m_2$), then she can figure out k. Also we prove that one pair $(m_1, e_k(m_1))$ is not enough to do so (at least for $p > 2$, in the exceptional case $p = 2$, $k_\times$ must be 1, and $k_+ = e_k(m_1) - m_1$, so in this case, one pair suffices).

First of all, two pairs give the linear system of equations

$$k_\times m_1 + k_+ = c_1,$$
$$k_\times m_2 + k_+ = c_2.$$

Taking their difference, then dividing by $m_1 - m_2$ (which is not zero, since $m_1 \neq m_2$), we obtain

$$k_\times = \frac{c_1 - c_2}{m_1 - m_2}.$$

Then it is clear that

$$k_+ = c_1 - \frac{c_1 - c_2}{m_1 - m_2} m_1 = c_2 - \frac{c_1 - c_2}{m_1 - m_2} m_2.$$

Checking back, this is indeed a solution, therefore two pairs indeed give the key.

On the other hand, one pair is not enough (at least when $p > 2$), since the equation

$$k_\times m_1 + k_+ = c_1$$

has $p - 1$ solutions:

$$\{(k_\times, c_1 - k_\times m_1) : k_\times \in \mathbf{F}_p^\times\},$$

which means that if Eve knows a single pair $(m_1, e_k(m_1))$, there are still $p - 1$ possible keys k which map m_1 to $e_k(m_1)$.