MIDTERM EXAM

1. (a) Describe the Caesar cipher. **(2 points)**

   (b) Alice and Bob are planning to communicate using a simple substitution cipher. They pick their key at random, with the same probability for each permutation of the alphabet. What is the probability that their simple substitution cipher will actually be a Caesar cipher? **(4 points)**

Solution. (a) In the Caesar cipher, both $\mathcal{M}$ and $\mathcal{C}$ are set of the letters of the alphabet:

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

The key set $\mathcal{K}$ is the set of positive integers not exceeding 26:

$$\mathcal{K} = \{k \in \mathbf{N} : 1 \leqslant k \leqslant 26\}.$$

Given a letter, the key k acts on it via a shift by k, where the number corresponding to each letter is its number in the alphabetical order, i.e. `a` is 1, `b` is 2, and so on, `z` is 26. We understand this order cyclically, i.e. after `z`, `a` comes again. To put this more formally,

$$e_k(m) = \text{the shift of } m \text{ by } k \text{ in the alphabetical order, understood cyclically.}$$

As for the decryption, it is a shift backwards by k, or equivalently, a shift by $26 - k$. Formally,

$$d_k(c) = e_{26-k}(c).$$

(b) The number of simple substitution ciphers is 26!, while that of Caesar ciphers is 26. Therefore

$$\mathrm{P}(\text{a randomly chosen simple substitution cipher is Caesar}) = \frac{26}{26!} = \frac{1}{25!}.$$

2. (a) State Fermat's little theorem. **(2 points)**

   (b) Alice and Bob are planning to communicate using an XOR cipher on 101 bits. To exclude trivialities, they consider only those keys which contain both 0 and 1 bits. Prove that the number of such keys is divisible by 101. **(4 points)**

Solution. (a) Fermat's little theorem says that if p is a prime number, and $a \in \mathbf{Z}$, then $a^p \equiv a \bmod p$.

(b) The number of all keys for XOR ciphers on 101 bits is 2^{101}, therefore, dropping the trivial keys, we are left with $2^{101} - 2$ keys. Applying Fermat's little theorem with $p = 101$, $a = 2$, we obtain that $2^{101} \equiv 2 \bmod 101$, that is, $101 \mid (2^{101} - 2)$.

3. (a) Describe the Diffie-Hellman problem over the group $\mathbf{F}_p^\times$. **(2 points)**

   (b) Let p be a large prime and $1 \leqslant g \leqslant p-1$. Assume Eve has an access to a machine, which from any input (g^a, g^b), computes $g^{(a+1)(b+1)}$ in polynomial time. Prove that using this machine, Eve can solve the Diffie-Hellman problem over $\mathbf{F}_p^\times$ in polynomial time. **(4 points)**

Solution. (a) The Diffie-Hellman problem over the group $\mathbf{F}_p^\times$ is the following computational task. Given $g \in \mathbf{F}_p^\times$, $g^a, g^b \in \mathbf{F}_p^\times$ (with some unknown $a, b \in \mathbf{Z}$), compute g^{ab}.

(b) Since

$$g^{ab} = g^{(a+1)(b+1)-a-b+1} = g^{(a+1)(b+1)} g^{-a} g^{-b} g,$$

Eve can do the following. She gives (g^a, g^b) to her machine, then takes the output, multiplies it by the inverse of g^a and then by the inverse of g^b (both computable in polynomial time as we learned it in class), then by g.

4. (a) Describe the ElGamal cryptosystem over the group $\mathbf{F}_p^\times$. **(2 points)**

   (b) Alice publishes the data p, g, A (p is a large prime, $1 \leqslant g \leqslant p-1$, $A \equiv g^a \bmod p$ (with some secret $a \in \mathbf{N}$) on her homepage for an ElGamal cryptosystem. Unfortunately, her g is so bad that the order of g in $\mathbf{F}_p^\times$ is less than $\log p$. Prove that Eve can break any intercepted cipher in polynomial time. **(4 points)**

Solution. (a) Alice chooses a prime number p, and a residue class $g \in \mathbf{F}_p^\times$ (preferably of large order). She further chooses a positive integer a, and computes the residue class $A \equiv p^a \bmod p$. Then she publishes p, g, A, and keeps a in secret.

Now anyone (say, Bob) can send a message to Alice as follows. If his message is a residue class $m \in \mathbf{F}_p^\times$, then he chooses a positive integer k (an ephemeral key), and computes $c_1 \equiv g^k \bmod p$ and $c_2 \equiv mA^k \bmod p$, then sends the pair (c_1, c_2) to Alice.

Now Alice decrypts the cipher as follows: she computes $c_2 c_1^{-a} \bmod p$:

$$c_2 c_1^{-a} \equiv mA^k g^{-ak} \equiv mg^{ak} g^{-ak} \equiv m \bmod p,$$

which is just the original message.

(b) Eve can do the following. She computes $g, g^2, \ldots, g^{\lceil \log p \rceil}$ (this is an admissible number of powers, and each exponentiation can be computed in polynomial time, as we learned it in class). Since the order of g is less than $\log p$, this list contains all powers of g, in particular A. Therefore, she managed to get a value a' such that $g^a \equiv g^{a'} \bmod p$. Then for an intercepted pair (c_1, c_2), she can play the role of Alice:

$$c_2 c_1^{-a'} \equiv mA^k g^{-a'k} \equiv mg^{ak} g^{-a'k} \equiv mg^{ak} g^{-ak} \equiv m \bmod p,$$

and the cipher is decrypted.