Midterm Exam

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

   (b) Alice and Bob are students of the BSM. They would like to use a simple substitution cipher on the English alphabet with the restriction that $\{\mathtt{a}, \mathtt{e}, \mathtt{i}\}$ is mapped to itself, and also $\{\mathtt{o}, \mathtt{u}\}$ is mapped to itself. (This is important for them, because occasionally they want to use Hungarian accents and dots, and this is the simplest if they encrypt accented and dotted characters to others which may have the same accents and dots.) How many possible keys are there, if they do not impose further conditions? **(4 points)**

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

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

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

$$\mathcal{K} = \{k : k \in \mathrm{Perm}(\mathfrak{A})\}.$$

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) Such a key is a permutation of $\{\mathtt{a}, \mathtt{e}, \mathtt{i}\}$, one of $\{\mathtt{o}, \mathtt{u}\}$, and one of the remaining 21 characters, considered together. These are independently chosen, and their numbers are 3!, 2! and 21! respectively. Therefore, the number of possible keys is $3! \cdot 2! \cdot 21!$.

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

   (b) What are the subgroups of the multiplicative group $\mathbf{Z}_8^\times$? **(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 use representatives to write $\mathbf{Z}_8^\times = \{1, 3, 5, 7\}$. Obviously $\{1\}$ and $\mathbf{Z}_8^\times$ are subgroups. Since $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$, we see that $\{1, 3\}$, $\{1, 5\}$ and $\{1, 7\}$ are also subgroups. We claim that there is no more. To see this, assume that two of $3, 5, 7$ are in a subgroup H. Then since

$$3 \cdot 5 \equiv 7, \qquad 5 \cdot 7 \equiv 3, \qquad 7 \cdot 3 \equiv 5, \qquad \mod 8,$$

we see that the third of them is also in H, that is, $H = \mathbf{Z}_8^\times$.

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

   (b) Alice, Bob and Charles choose publicly a large prime p. They would like to agree on a residue class modulo p, but they know that their communication is monitored by an eavesdropper. How could they do that in spirit of Diffie-Hellman? **(4 points)**

Solution. (a) Alice and Bob would like to agree on a residue class modulo p such that even though their whole communication is monitored by an eavesdropper, they can consider this residue class to be their secret. They publicly agree on the prime p and a coprime residue class g modulo p (preferably a primitive root, but this is not absolutely necessary).

In the first step Alice chooses $a \in \mathbf{N}$ and computes $A \equiv g^a \bmod p$; while Bob chooses $b \in \mathbf{N}$ and computes $B \equiv g^b \bmod p$. Then Alice sends A to Bob, and Bob sends B to Alice.

In the next step, Alice raises the incoming residue class B to power a modulo p; while Bob raises the incoming residue class A to power b modulo p. The point is that they get the same residue class:

$$B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \bmod p.$$

(b) Alice, Bob and Charles chooses the positive integers $a, b, c \in \mathbf{N}$, respectively, and they keep these numbers in secret all along. Now in the first round Alice computes and sends g^a to Bob, Bob computes and sends g^b to Charles, Charles g^c to Alice. Then in the second round Alice raises the incoming g^c to power a, and sends her result to Bob, Bob raises the incoming g^a to power b, and sends her result to Charles, Charles raises the incoming g^b to power c, and sends her result to Alice. In the third round, Alice raises the incoming number to power a, Bob raises the incoming number to power b, and Charles raises the incoming number to power c. Of course, all along, they do the computations modulo p. In the end, each of them arrives at the residue class g^{abc}. Everything is computable here in polynomial time.

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

   (b) Consider the following symmetric cryptosystem: fix a large prime number p, and let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbf{F}_p$, $e_k(m) \equiv km \bmod p$. Prove that this cryptosystem is vulnerable to the chosen plaintext attack. **(4 points)**

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

   (b) Assume Eve learns a pair (m_1, c_1), where $c_1 = e_k(m_1)$. Then, since $c_1 \equiv km_1 \bmod p$, we know that $k \equiv c_1 m_1^{-1} \bmod p$. Here, m_1^{-1} is computable in polynomial time, so is k. After learning k, Eve can decrypt any intercepted cipher.