Midterm Exam

1. (a) Let G be a finite group and $a \in G$. Define the order of a. **(2 points)**

   (b) Given G, characterize those elements of G which have order 1. **(4 points)**

   Solution. (a) The order of $a \in G$ is the smallest positive integer n which satisfies

$$a^n = \underbrace{a * \ldots * a}_{n \text{ times}} = e,$$

   where e is the unit element and $*$ is the operation of G.

   (b) We claim that the order of an element $a \in G$ is 1 if and only if a is the unit element e. First, if $a = e$, then indeed,

$$a^1 = a = e,$$

   and of course $a^n = e$ cannot hold for $\mathbf{N} \ni n < 1$, since 1 is the smallest positive integer. As for the converse, assume that the order of a is 1. Then

$$e = a^1 = a,$$

   hence a must be the unit element itself.

2. (a) Describe the XOR cipher. **(2 points)**

   (b) Alice and Bob are planning to communicate using an XOR cipher on 201 bits. They meet and choose their key at random, i.e. for each bit, they toss a fair $0-1$ coin. What is the probability of that the resulting key will contain more 1's than 0's? **(4 points)**

Solution. (a) In the XOR cipher, we fix a positive integer t, and then

$$\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0-1 \text{ sequences of length } t\}.$$

We define the $\oplus$ operation as the bitwise addition, i.e. if $a = \sum_{j=0}^{t-1} a_j 2^j$, $b = \sum_{j=0}^{t-1} b_j 2^j$ (where a_j, b_j's are binary digits, 0 or 1 each), then let

$$a \oplus b = \sum_{j=0}^{t-1} c_j 2^j,$$

where $c_j = 0$ if $a_j = b_j$, and $c_j = 1$ if $a_j \neq b_j$.

Given m and k, $e_k(m) = m \oplus k$. The decryption function is the same: $d_k = e_k$, i.e. $d_k(c) = c \oplus k$.

(b) We claim that the probability in question is $1/2$. First observe that any particular $0-1$ sequence will be the chosen key with probability 2^{-101}. Therefore, to verify our claim, it suffices to show that exactly half of the $0-1$ sequences contain more 1's than 0's. In any sequence, replace the 0's with 1's and the 1's with 0's. Since 201 is odd, this is a bijection between the sets

$$A = \{0-1 \text{ sequences of length 201 with more 1's than 0's}\}$$

and

$$B = \{0-1 \text{ sequences of length 201 with more 0's than 1's}\}.$$

That is,

$$\Pr(\text{the chosen key contains more 1's than 0's}) = \frac{\#A}{\#(A \cup B)} = \frac{\#A}{\#A + \#B} = \frac{\#A}{2\#A} = \frac{1}{2}.$$

3. (a) Describe the discrete logarithm problem in the group $\mathbf{F}_p^\times$. **(2 points)**

   (b) What are those integers $n \in \mathbf{Z}$ which are solutions to the discrete logarithm problem $2^x \equiv 16 \bmod 31$? **(4 points)**

Solution. (a) Assume p is a prime number and g is a nonzero residue class modulo p. Assume that for some $1 \leqslant x \leqslant p-1$, $g^x \equiv a \bmod p$, again a residue class modulo p. The discrete logarithm problem is to compute the smallest such positive integer x, if g and a are given.

(b) **Typo in the problem: n is the same as x.** The computations $2^1 \equiv 2 \bmod 31$, $2^2 \equiv 4 \bmod 31$, $2^3 \equiv 8 \bmod 31$, $2^4 \equiv 8 \bmod 16$, $2^5 \equiv 1 \bmod 31$ show that the order of 2 modulo 31 is 5, and also that $2^4 \equiv 16 \bmod 31$.

We claim that integers n which satisfy $2^n \equiv 16 \bmod 31$ are exactly those which satisfy $n \equiv 4 \bmod 5$. First, if $n \equiv 4 \bmod 5$, then $n = 5k + 4$ for some $k \in \mathbf{Z}$, and then

$$2^n \equiv 2^{5k+4} \equiv (2^5)^k \cdot 16 \equiv 16 \bmod 31.$$

As for the converse assume $2^n \equiv 16 \bmod 31$. Then $2^{n+1} \equiv 1 \bmod 31$, therefore, by our considerations on the order in the class tells us that $n + 1$ is divisible by 5. Hence $n \equiv 4 \bmod 5$.

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. When choosing a, she was so careless that she picked $a = p-1$. 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) First, by Euler-Fermat, if $a = p-1$, then $A \equiv g^{p-1} \equiv 1 \bmod p$. When Eve learns that $A \equiv 1 \bmod p$ has been publshed, and intercepts the cipher (c_1, c_2), she computes $c_2 c_1^{-(p-1)} \bmod p$. This is possible in polynomial time, since it is just modular multiplication, modular exponentiation and taking modular inverse, in the class we learned all of these can be done in polynomial time. Since her computation is the same as that of Alice, she also gets m.

We remark that not only $p-1$, but any multiple of the order of g leads to the same collapse of the cryptosystem.