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)**

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)**

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)**

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)**