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)**

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)**

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)**

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)**