MOCK MIDTERM EXAM

1. (a) Define the function φ. **(2 points)**

   (b) Prove that if m, n are positive integers such that $\gcd(m,n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$. **(4 points)**

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

   (b) Bob encrypts a message using the Caesar cipher and sends it to Alice. Eve intercepts the message, but her time is limited to try only six keys. Independently, Evan also intercepts the message, but his time is also limited, and can try only four keys. What is the probability of that none of them decrypts the message? (Note that Eve and Evan do not consult, it might happen that their attempts overlap.) **(4 points)**

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

   (b) Assume we design a XOR cipher on t bits, where t is even. In order to avoid trivial keys (such as the constant zero key), we restrict to those keys, which contain exactly $t/2$ zeros and $t/2$ ones. Prove that the number of such keys is at least $2^t/t$. **(4 points)**

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

   (b) Assume that p is an odd prime number, $1 \leqslant g \leqslant p-1$, and a is a positive integer such that $a-g$ is even. Prove that if for some $1 \leqslant x \leqslant p-1$, $g^x \equiv a \bmod p$, then $g^x \equiv a \bmod 2p$. **(4 points)**