MOCK FINAL EXAM

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

   (b) Let $p > 2$ be a prime number, and g be a primitive root modulo p, i.e. the discrete logarithm problem $g^x \equiv a \bmod p$ has a solution $1 \leqslant x \leqslant p-1$ for all $1 \leqslant a \leqslant p-1$. Assume there is a machine which solves the discrete logarithm problem for any input $1 \leqslant a \leqslant (p-1)/2$ in polynomial time. Prove that using this machine, the discrete logarithm problem can be solved for any input $1 \leqslant a \leqslant p-1$ in polynomial time. **(4 points)**

2. (a) Describe the elliptic curve ElGamal public key cryptosystem. **(2 points)**

   (b) Let $\mathbf{F}_7$ be the base field. How many points does the elliptic curve

$$\{[X,Y,Z] \in \mathbf{PF}_7^2 : Y^2Z = X^3 - XZ^2\}$$

   have? **(4 points)**

3. (a) Describe perfect secrecy. **(2 points)**

   (b) Let X, Y be random variables. Prove that

$$H(X,Y) \leqslant H(X) + H(Y).$$

   (4 points)

4. (a) Define key equivocation. **(2 points)**

   (b) Alice and Bob use the XOR cipher on t bits. Assuming that M and K are independent and uniformly distributed, compute the key equivocation. **(4 points)**