Final Exam

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

   (b) Prove that the number of those keys in the 23-bit XOR cipher which contain at least 7 and at most 16 zeros is divisble by 23. **(4 points)**

2. (a) Describe the RSA cryptosystem. **(2 points)**

   (b) Assume Eve has a machine which, for any input (a, b, N) (with positive integers a, b, N), returns in polynomial time

$$\begin{cases} 1, \text{ if there exists } d \mid N \text{ such that } a < d < b, \\ 0, \text{ if there is no } d \mid N \text{ satisfying } a < d < b. \end{cases}$$

   Prove that using this machine, Eve can break the RSA in polynomial time. **(4 points)**

3. (a) Define entropy. **(2 points)**

   (b) Alice and Bob use an XOR cipher on t bits, and they choose the message and the key independently and uniformly (i.e. for each t-bit sequences m and k, $P(M = m) = 2^{-t}$, $P(K = k) = 2^{-t}$, $P(M = m, K = k) = 2^{-2t}$). Compute the key equivocation $H(K \mid C)$. **(4 points)**

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

   (b) Let E be the elliptic curve given by the equation $y^2 = x^3 + x + 1$ over the field $\mathbf{F}_5$. Show that the points $P = (4, 2)$ and $Q = (3, 4)$ lie on E, and solve the elliptic curve discrete logarithm problem $nP = Q$. (It is enough to give one such n, you don't have to compute all of them.) **(4 points)**