NAME:

I pledge my honor that I will not discuss any information, any details of this exam with anyone until Thursday, Dec 15th.

signature

FINAL EXAM

1. (a) Describe the RSA public key cryptosystem. **(2 points)**

   (b) Alice establishes an RSA cryptosystem. Prove that if Eve knows that p, q are twin primes (i.e. $q = p + 2$), then she can easily break the cryptosystem, namely she can decrypt any cipher in polynomial time. **(4 points)**

2. (a) Describe the elliptic curve discrete logarithm problem. **(2 points)**

   (b) Let $\mathbf{R}$ be the base field. Prove that the affine elliptic curve

$$\{(x,y) \in \mathbf{R}^2 : y^2 = x^3 + Ax\}$$

   has exactly three intersection points with the x axis if and only if $A < 0$. **(4 points)**

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

   (b) Let $p_1, \ldots, p_n$ be positive real numbers such that $p_1 + \ldots + p_n = 1$. Let q and r be further positive real numbers such that $p_n = q + r$. Prove that

$$H(p_1, \ldots, p_n) < H(p_1, \ldots, p_{n-1}, q, r).$$

   (4 points)

4. (a) State the Euler-Fermat theorem. **(2 points)**

   (b) Let $p > 2$ be a prime number such that $p \equiv 3 \mod 4$. Assume a is a further integer, which is coprime to p. Assuming that a has a square-root modulo p, prove that $a^{(p+1)/4}$ is a square-root of a modulo p. **(4 points)**