FINAL EXAM

1. (a) Describe the simple substitution cipher. **(2 points)**

   (b) In Bergengócia (a country in Hungarian fairy tales), people use an alphabet on four characters. How many simple substitution cipher keys k exist for this alphabet which satisfy $e_k = d_k$? **(4 points)**

2. (a) Describe the Miller-Rabin primality test. **(2 points)**

   (b) We all know that $15 = 3 \cdot 5$ is not a prime number. Find a *witness*: an integer which is on the one hand coprime to 15, and on the other hand, shows the compositeness of 15 in the Miller-Rabin test. **(4 points)**

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

   (b) Let E be the elliptic curve over the field $\mathbf{F}_5$ given by the equation

$$y^2 = x^3 + x + 1$$

   and let $P = (4, 2)$ and $Q = (0, 1)$ be points on E. Compute the point $P + Q$ on E (under the elliptic curve addition). **(4 points)**

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

   (b) Prove that the problem of breaking the RSA is polynomially reducible to the discrete logarithm problem in the following sense. Let N be the modulus of an RSA cryptosystem, and assume that there is an algorithm which works as follows: for an input (g, a) satisfying $\gcd(g, N) = \gcd(a, N) = 1$, it computes in polynomial time the output x, where x is the smallest positive integer satisfying $g^x \equiv a \bmod N$ if there is such an x at all, while if there is no such positive integer, $x = \texttt{error}$. Show that using such a hypothetical algorithm, the eavesdropper can decrypt any intercepted cipher in polynomial time. **(4 points)**