Final Exam

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

   (b) Alice and Bob are planning to use a simple substitution cipher. They want a key which encrypts vowels to vowels, consonants to consonants and (to avoid debates) `Y` to `Y`. How many choices do they have? **(4 points)**

2. (a) Describe the elliptic curve Diffie-Hellman key exchange. **(2 points)**

   (b) Let the base field be $\mathbf{F}_7$, and consider the elliptic curve E given by the equation $X^3 + XZ^2 = Y^2Z$. How many points lie on E? **(4 points)**

3. (a) Describe the RSA crpytosystem. **(2 points)**

   (b) Alice uses an RSA, but Eve learns that the prime numbers are chosen in the unfortunate way that $p = a + 1$, $q = a^2 + 1$ for some $a \in \mathbf{N}$. How can Eve break the cryptosystem in polynomial time? (Clarification: Eve does not know what a is, she only knows that there is such a positive integer a.) **(4 points)**

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

   (b) Can the entropy be infinite? (Clarification: in view of that for finitely many probabilities, the answer is obviously no, your task is to decide in the infinite setup. That is, are there nonnegative numbers $p_1, p_2, \ldots$ summing up to 1 such that the calculated entropy sums up to infinity?) **(4 points)**