Homework 4

Due date: Friday, April 7th 11:30 AM

Question 1 (20 points)

Find all of the points on the elliptic curve $E: \ y^2 = x^3 + 2x + 1$ over $\mathbb{Z}_{11}$. How many points are on this curve? (Don't forget about the identity!)

Question 2 (20 points)

a. Show how to compute discrete logarithms efficiently in the group $(\mathbb{Z}_N, +)$ if the base g is a generator of $\mathbb{Z}_N$. (Note: in the group $(\mathbb{Z}_N, +)$ the identity is 0 and $g^4 = g+g+g+g \mod N$. Recall that g is a generator of $\mathbb{Z}_N$ if and only if $\mathbf{gcd}(g, N) = 1$.).

b. Show that if $ab = c \mod N$ and $\mathbf{gcd}(b, N) = d$, then

   i. d divides c (written $d|c$);

   ii. $a \cdot (b/d) = (c/d) \mod (N/d)$; and

   iii. $\mathbf{gcd}(b/d, N/d) = 1$.

c. Using the above operations show how to compute discrete logarithms efficiently in the group $\mathbb{Z}_N$ even if the base g is not a generator of $\mathbb{Z}_N$.

Question 3 (10 points)

Consider the following key-exchange protocol Π:

a. Alice chooses uniformly random strings $k, r \in \{0,1\}^n$, and sends $s := k \oplus r$ to Bob.

b. Bob chooses uniform $t \in \{0,1\}^n$ and sends $u := s \oplus t$ to Alice.

c. Alice computes $w := u \oplus r$ and sends w to Bob.

d. Alice outputs k and Bob outputs $w \oplus t$.

Show that Alice and Bob output the same key. Is Π secure? Justify your answer with a security proof or by providing a concrete attack.

Question 4 (25 points)

Show that for any CPA-secure public-key encryption scheme for single-bit messages, the length of the ciphertext must be super logarithmic in the security parameter. **Hint:** Suppose that the length of a ciphertext was $|c| = k \log n$ for some constant k. What is the size of the ciphertext space $\mathcal{C}$?

Question 5 (25 points)

Prove formally that the El Gamal encryption scheme is *not* CCA-secure.