Homework 4

Due date: Thursday, November 16 at 9:00 AM

Question 1 (20 points)

Find all of the points on the elliptic curve $E: y^2 = x^3 + 5x + 1$ over $\mathbb{Z}_{11}$. How many points are on this curve? (Don't forget about the identity!)

Question 2 (20 points)

Given a prime $p > 2$ we say that $x \in \mathbb{Z}_p^*$ is a quadratic residue if $x = y^2 \mod p$ for some $y \in \mathbb{Z}_p^*$. Assume that $g \in \mathbb{Z}_p^*$ is a generator such that $\langle g \rangle = \mathbb{Z}_p^*$. Let $QR_p = \{x \in \mathbb{Z}_p^* : \exists y \text{ s.t. } y^2 = x \mod p\}$.

a. Show that QR_p is a subgroup of $\mathbb{Z}_p^*$.

b. Show that $g \notin QR_p$, but that $g^{2i} \in QR_p$ for every $i \geq 0$.

c. Show that $|QR_p| = \frac{p-1}{2}$ (Hint: Look at Lemma 8.37).

d. Show that $y \in QR_p$ if and only if $y^{\frac{p-1}{2}} = 1$. In particular, this means that there is a polynomial time algorithm to test if $y \in QR_p$.

Question 3 (20 points)

Show that the Decisional Diffie-Hellman Problem does not hold over the cyclic group $\mathbb{Z}_p^*$ (although the computational Diffie-Hellman Assumption is believed to hold). Hint: Use the properties you proved in the last question about quadratic residues. As in the previous question before you may assume $g \in \mathbb{Z}_p^*$ is a generator such that $\langle g \rangle = \mathbb{Z}_p^*$.

Question 4 (20 points)

In class we proved that the Diffie-Hellman Key Exchange Protocol was secure if the DDH assumption holds. In this problem we will develop a secure key exchange protocol based on the weaker CDH assumption. Let $\mathcal{G}(1^n)$ be a PPT algorithm which outputs a cyclic group $\langle g \rangle$ along with the generator g and the size $m = |\langle g \rangle|$ of the cyclic group. Consider the following variant of the Diffie-Hellman Key Exchange Protocol: (1) Alice selects $r_A \in \mathbb{Z}_m$ at random and sends g^{r_A} to Bob. (2) Bob selects $r_B \in \mathbb{Z}_m$ at random and sends g^{r_B} to Alice. (3) Alice and Bob both compute $g^{r_A r_B}$ and set $K_{A,B} = H(g^{r_A r_B})$ where $H: \{0,1\}^* \to \{0,1\}^n$ is a random oracle. Assuming that the Computational Diffie Hellman Assumption holds with respect to the group generator $\mathcal{G}$ show that the modified Diffie-Hellman Key Exchange Protocol (above) is secure against a passive eavesdropping adversary in the random oracle model.

Question 5 (20 points)

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

Bonus Question 1 (5 Points)

Suppose that $N_1 = p_1q_1, N_2 = p_2q_2, N_3 = p_3q_3$ where the secret p_i's and q_i's are distinct prime numbers[1]. Suppose that we have three distinct RSA public keys $pk_i = (e_i = 3, N_i)$ for each i and that Bob generates three ciphertexts $c_i = m^3 \mod N_i$ encrypting the *same* message m under each of these keys. Explain how an attacker can recover m from c_1, c_2 and c_3.

Bonus 2 (5 points)

We encrypted a secret message $m \in \mathbb{Z}_N^*$ under 7 RSA keys. The public keys are (e_i, N_i) for $i \leq 7$ and we have $e_i = 7$ for each i. The values N_i and $c_i = m^7 \mod N_i$ for each $i \leq 7$ are given in a Mathematica Notebook file. Your task is to decrypt the secret message m.

[1]Note that if N_i and N_j share a prime factor and $N_i \neq N_j$ then $gcd(N_i, N_j)$ exposes the shared prime factor.