Name:

Purdue E-mail:

*I collaborated with (...). I affirm that I wrote the solutions in my own words and that I understand the solutions I am submitting.*

# Homework 4

**Due date: Thursday, November 15th$^{\text{nd}}$ 3:00 PM**

## Question 1 (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 2 (20 points)

Here we show how to solve the discrete-logarithm problem in a cyclic group of order $q = p^e$ in time $\mathcal{O}(\mathsf{polylog}(q) \cdot \sqrt{p})$. Given as input a generator $g$ of order $q = p^e$ and value $h$, we want to compute $x = \log_g h$. You may assume that $p > 2$ is a prime number.

(a) Show how to compute $[x \mod p]$ in time $\mathcal{O}(\mathsf{polylog}(q) \cdot \sqrt{p})$. **Hint:** Consider the equation $\left(g^{p^{e-1}}\right)^{x_0} = h^{p^{e-1}}$ as well as the ideas from the Pohlig-Hellman algorithm.

(b) Say $x = x_0 + x_1 \cdot p + \cdots + x_{e-1} \cdot p^{e-1}$ with $0 \leq x_i < p$. In the previous step we determined $x_0$. Show how to compute in $\mathsf{polylog}(q)$ times a value $h_1$ such that $(g^p)^{x_1 + \cdots + x_{e-1} \cdot p^{e-2}} = h_1$

(c) Use recursion to obtain the claimed running time for the original problem. (Note that $e = \mathcal{O}(\log q)$)

## 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 question 1 about quadratic residues. You may assume $g \in \mathbb{Z}_p^*$ is a generator such that $\langle g \rangle = \mathbb{Z}_p^*$ and that $p > 3$ is a prime number.

## 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 in the random oracle model.

## Question 5 (20 points)

Consider the following protocol for two parties $A$ and $B$ to flip a fair coin.

1. A trusted party $T$ publishes her public key $pk$;
2. Then $A$ chooses a uniform bit $b_A$, encrypts it using $pk$, an announces the ciphertext $c_A$ to $B$ and $T$;
3. Next, $B$ acts symmetrically and announces a ciphertext $c_B \neq c_A$;
4. $T$ decrypts both $c_A$ and $c_B$ to obtain $b_A$ and $b_B$ and sends bits to A and B. Both parties XOR the results to obtain the value of the coin $b_A \oplus b_B$.

a) Argue that even if $A$ is dishonest (but B is honest), the final value of the coin is uniformly distributed.

b) Assume the parties use EI Gamal encryption (where the bit $b$ is encoded as the group element $g^b$ before being encrypted — note that efficient decryption is still possible ). Show how a dishonest $B$ can bias the coin to any values he likes.

c) Suggest what type of encryption scheme would be appropriate to use here. Can you define an appropriate notion of security for a fair coin flipping and prove that the above coin flipping protocol achieves this definition when using an appropriate encryption scheme?

## Bonus Question 1 (5 Points)

Let $q$ have prime factorization $q = \prod_{i=1}^{k} p_i^{e_i}$. Using the result from problem 2, show a modification of the Pohlig-Hellman algorithm that solves the discrete-logarithm problem in a group of order $q$ in time $\mathcal{O}\big(\mathsf{polylog}(q) \cdot \sum_{i=1}^{k} e_i \sqrt{p_i}\big) = \mathcal{O}(\mathsf{polylog}(q) \cdot \max_i\{\sqrt{p_i}\})$

## Bonus Question 2 (5 Points)

In the attached Mathematica Notebook file we have generated RSA keys

$$(N_i = p_i q_i, e_i, d_i) \text{ for } i = 1, \ldots, 11$$

for eleven different kings. Each king used the same public parameter $e_i = 11$ for each $i = 1, \ldots, 11$ though the secret prime factors $p_i, q_i$ are all distinct. Archimedes had an important message

$$m \leq \min_i N_i$$

that he wanted to share will all eleven kings so he sent the ciphertext

$$c_i = m^{e_i} \mod N_i$$

to each king $i$. An eavesdropping attacker intercepted all of the ciphertexts and placed them in the Mathematica Notebook file. He needs your help to recover the secret message $m$ that Archimedes sent to the eleven kings.