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 3

Due date: Thursday, November 1st$^{\text{nd}}$ 3:00 PM

Question 1 (20 points)

Let $e = 3$, $\langle N, e\rangle$ be an RSA public key, and $m_1 \neq m_2 \in \mathbb{Z}_N^*$ satisfy the condition that $m_2 = 2m_1 + 1 \mod N$.

Show that: given $\langle N, e = 3, c_1 = m_1^e, c_2 = m_2^e\rangle$ and the fact that $m_2 = 2m_1 + 1 \mod N$, one can construct a PPT adversary $\mathcal{A}$ that can recover both m_1 and m_2

Question 2 (20 points)

Let $p \geq 5$ be prime and let E be the elliptic curve given by $y^2 = x^3 + Ax + B \bmod p$ where $4A^3 + 27B^2 \neq 0 \bmod p$. Let $P_1, P_2 \neq \mathcal{O}$ be the points on E, with $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$. Prove the following statements:
If $P_1 = P_2$ and $y_1 \neq 0$ then $P_1 + P_2 = 2P_1 = (x_3, y_3)$ with

$$\begin{aligned} x_3 &= \left[m^2 - 2x_1 \mod p\right] \\ y_3 &= \left[m \cdot (x_1 - x_3) - y_1 \mod p\right] \end{aligned} \tag{1}$$

where $m = \left[\dfrac{3x_1^2 + A}{2y_1}\right]$

Question 3 (15 points)

Consider a specific cyclic group $\mathbb{G}$ of prime order q generated by $g \in \mathbb{G}$. Let $\mathcal{A}$ be an efficient algorithm with the following property:

$$\Pr[u \xleftarrow{\$} \mathbb{G}, x \leftarrow \mathcal{A}(\mathbb{G}, g, u) : g^x = u] = \epsilon$$

Then we can construct an efficient algorithm $\mathcal{B}$ with the following property:

$$\forall u \in \mathbb{G} \quad \Pr[x \leftarrow \mathcal{B}(\mathbb{G}, g, u) : g^x = u] = \epsilon$$

where the probability is over the random choices made by $\mathcal{B}$

Question 4 (25 points)

Fix $N \in \mathbb{N}$ such that $N, e \geq 1$ and $\texttt{gcd}\,(e, \phi(N)) = 1$. Assume that there is an adversary $\mathcal{A}$ running in time t such that

$$\Pr\left[\mathcal{A}\left([x^e \mod N]\right) = x\right] \geq 0.01$$

where the probability is taken over the uniform choice of $x \in \mathbb{Z}_N^*$. Show how to construct an adversary $\mathcal{A}'$ with running time $t' = O\left(poly\left(t, \log_2 N\right)\right)$ such that

$$\Pr\left[\mathcal{A}'\left([x^e \mod N]\right) = x\right] \geq 0.99 \ .$$

Hint: Use the fact that $y^{1/e} \cdot r = (y \cdot r^e)^{1/e} \mod N$. Here, $y^{1/e} = y^d \in \mathbb{Z}_N^*$ where d is a (secret) number such that $ed \equiv 1 \mod \phi(N)$. Also use the fact that, given $r \in \mathbb{Z}_N^*$, we can find a number r^{-1} such that $rr^{-1} = 1 \mod N$.

Question 5 (20 points)

Define a fixed-length hash function (Gen, H) as follows:

(a) Gen : on input 1^n, run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, h_1)$ and selects $h_2, \cdots, h_t \leftarrow \mathbb{G}$. Output $s := \langle \mathbb{G}, q, (h_1, \cdots, h_t) \rangle$ as the key.

(b) H : given a key $s := \langle \mathbb{G}, q, (h_1, \cdots, h_t) \rangle$ and input $(x_1, \cdots, x_t)$ with $x_i \in \mathbb{Z}_q$, output $H^s(x_1, \cdots, x_t) = \prod_i h_i^{x_i}$

Prove that if the discrete-logarithm problem is hard relative to $\mathcal{G}$ and q is prime, then for any $t = \mathsf{poly}(n)$ this construction is a fixed length collision-resistant hash function