Quiz 2

Full Name: _____ **Student ID:** _____

Question	1	2	3	Total
Score				

Question 1 (Authenticated Encryption) [20 points]: Let (E, D) be a CPA-secure cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ and let $H_0 : \mathcal{M} \to \mathcal{C}$ and $H_1 : \mathcal{C} \to \mathcal{T}$ be collision resistant hash functions.
(a) Define (E_0, D_0) to be the following cipher:

- $E_0(k, m) := \{c \leftarrow \$E(k, m),\ \text{output } (c, H_0(m))\}$,
- $D_0(k, (c_0, c_1)) := \begin{cases} D(k, c_0) & \text{if } H_0(D_0(k, c_0)) = c_1, \\ \text{reject} & \text{otherwise} \end{cases}$.

Show that (E_0, D_0) is not AE-secure. [10 points]

We show (E_0, D_0) is not CPA-secure (therefore, not AE-secure). The adversary generates messages m_0 and m_1 such that $m_0 \neq m_1$ and sends them to the challenger. The adversary receives (c_0, c_1) as a ciphertext of one of the messages. The adversary checks if $c_1 = H_0(m_0)$, if so, it returns 0; else it returns 1.

(b) Define (E_1, D_1) to be the following cipher:

- $E_1(k, m) := \{c \leftarrow \$E(k, m),\ \text{output } (c, H_1(c))\}$,
- $D_1(k, (c_0, c_1)) := \begin{cases} D(k, c_0) & \text{if } H_1(c_0) = c_1, \\ \text{reject} & \text{otherwise} \end{cases}$.

Show that (E_1, D_1) is not AE-secure.
Hint: Use a concrete CPA-secure (E, D) and show that the resulting (E_1, D_1) is not AE-secure. [10 points]

We show (E_1, D_1) does not achieve ciphertext integrity (therefore, not AE-secure). We pick AES-\$CTR as a concrete instance of (E, D). For simplicity, we consider the encryption of a message that is one block long (128-bit if we use AES-128). The adversary sends a random message m to the challenger. The challenger responds with (c_0, c_1) where $c_0 = (ctr, c)$ and $c_1 = H_1(c_0)$ for some counter ctr. We note that AES-\$CTR is malleable, so $c_0' = (ctr, c \oplus \Delta)$ for any Δ is also a valid AES-\$CTR ciphertext. Therefore, the adversary can forge a ciphertext as $(c_0', H_1(c_0'))$ for $\Delta \neq \mathbf{0}$ and wins the ciphertext integrity game.

Question 2 (PRG from DDH) [20 points]:
(a) State the decisional Diffie-Hellman assumption. [5 points]

Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. For a given adversary $\mathcal{A}$, we define two experiments:
Experiment b ($b = 0, 1$):

- The challenger and the adversary $\mathcal{A}$ take a description of $\mathbb{G}$ as input.
- The challenger computes

$$\alpha, \beta, \gamma \xleftarrow{\$} \mathbb{Z}_q,\ u \xleftarrow{\$} g^{\alpha},\ v \xleftarrow{\$} g^{\beta},\ w_0 \xleftarrow{\$} g^{\alpha}\beta,\ w_1 \xleftarrow{\$} g^{\gamma},$$

  and sends the triple (u, v, w_b) to the adversary.
- The adversary outputs a bit $\hat{b} \in \{0, 1\}$.

The decisional Diffie-Hellman assumption states that the advantage of any PPT adversary in the experiments (the absolute difference of the probability that the adversary outputs 1 in Experiment b) above is negligible.

(b) Let $\mathbb{G}$ be a cyclic group of prime order q generated by $g \in \mathbb{G}$. Consider the following PRG defined over $(\mathbb{Z}_q^2, \mathbb{G}^3)$:

$$G(\alpha, \beta) := (g^{\alpha}, g^{\beta}, g^{\alpha\beta}).$$

Show that G is a secure PRG assuming DDH holds in $\mathbb{G}$. [15 points]

We show that if G is not a secure PRG, the DDH assumption does not hold.
Let $\mathcal{C}$ be a challenger for the DDH experiments, $\mathcal{A}$ be an adversary against the DDH assumption and $\mathcal{B}$ be a PRG adversary against G. $\mathcal{A}$ receives (u, v, w_b) from the DDH. It passes (u, v, w_b) to $\mathcal{B}$. $\mathcal{B}$ outputs a bit $\hat{b}$, which $\mathcal{A}$ forwards to $\mathcal{C}$. $\mathcal{A}$ can distinguish (u, v, w_0) and (u, v, w_1) as often as $\mathcal{B}$ can distinguish PRG G from a random output from $\mathbb{G}^3$. This completes the proof. $\square$

Question 3 (Public-key encryption) [20 points]: Suppose t users publish their public keys $pk_0, \ldots, pk_{t-1}$. Alice wants to send an encrypted message to one of them, say user 1 (with pk_1). But she does not want any other user or an eavesdropper to learn that the intended recipient of the message is user 1.
Alice does this by encrypting the message under user 1's public key and sends the ciphertext to all users. You can assume that only user 1 can decrypt the ciphertext correctly. Every other user obtain fail when attempting to decrypt the ciphertext using their own secret key.

(a) (Informally) Show that the ElGamal public-key encryption scheme is anonymous.
Hint: It is helpful to give a description of the key generation and the encryption algorithms of ElGamal. [10 points]

Recall that an ElGamal ciphertext for message m has the shape $(g^\beta, \text{Enc}_S(k, m))$ where g^β is a uniformly randomly picked element in a group $\mathbb{G}$ where discrete logarithm is hard, and $\text{Enc}_S()$ is a private key encryption scheme. As a result, the ciphertext follows the same distribution regardless of the recipient. Therefore, ElGamal is anonymous.

(b) (Informally) Show that the RSA public-key encryption scheme (not the vanilla RSA) is not anonymous. Assume that all t public keys are generated using the same RSA parameters l and e.
Hint: It is helpful to give a description of the key generation and the encryption algorithms of the RSA public-key encryption scheme. [10 points]

Recall that an RSA ciphertext for message m has the shape $(x^{e_i} \bmod n_i, \text{Enc}_S(k, m))$, where (n_i, e_i) is the public key of user i. Critically, $n_i \neq n_j$ with overwhelming probability (as each user generates their own prime numbers to derive n_i). n_i can also be significantly different from n_j as we only require them to be equally long (in terms of the number of bits). Without loss of generality, assume that $n_1 < n_2$ and suppose Alice is sending a message to user 2. There is a non-negligible probability that $x^{e_2} \bmod n_2 > n_1$ so any passive observer can learn that the message is not for user 1. This breaks anonymity.