The deadline is **today, 18:15**.
You are **not** allowed to collaborate with each other, or use the textbook or lecture notes.
Please submit your solutions as a pdf with **"Final_StudentID"** as its name.

30 1. 5 (a) Give the formal definition of DDH assumption.

5 (b) Explain the ElGamal Cryptosystem.

10 (c) Prove that under the DDH assumption it (ElGamal cryptosystem) is CPA-secure.

10 (d) Show that it (ElGamal cryptosystem) is not CCA-secure.

20 2. 10 (a) Describe the Merkle-Damgård construction and show that if the underlying compression function is collision-resistant, so is the Merkle-Damgård construction.

10 (b) Show that $\mathsf{Mac}_k(m) = \mathsf{H}(k||m)$ may not be a secure MAC when H is a Merkle-Damgård-based hash function.

۳ 3. Let $\mathsf{H} : M \to \{0,1\}^{128}$ be a collision resistant hash function known to the adversary. Does the function $f(k,m) = \mathsf{H}(m) \oplus k$ give a secure MAC? If so explain why. If not, describe an attack.

4. Let $(\mathsf{Enc}_{\mathsf{CBC}}, \mathsf{Dec}_{\mathsf{CBC}})$ be a randomized CBC-mode encryption scheme built from a block cipher $F : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$. Let $\mathsf{H} : \mathcal{X}^{\leq L} \to \mathcal{X}$ be a collision resistant hash function. Define the following candidate authenticated encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$:

- $\mathsf{Enc}(k,m)$: Output $c \leftarrow \mathsf{Enc}_{\mathsf{CBC}}(k, \mathsf{H}(m)||m)$.
- $\mathsf{Dec}(k,c)$: Compute $(t,m) \leftarrow \mathsf{Dec}_{\mathsf{CBC}}(k,c)$ and output m if $t = \mathsf{H}(m)$ and $\perp$ otherwise.

۳ (a) Show that $(\mathsf{Enc}, \mathsf{Dec})$ does not provide ciphertext integrity.

۱۰ (b) Show that $(\mathsf{Enc}, \mathsf{Dec})$ is not CCA-secure.

۳ (c) Would the above problems go away if the construction had used randomized counter mode encryption instead of CBC-mode encryption? Give a brief explanation.

۱ $\Rightarrow$

۱ $\Leftarrow$

۲

5. Show that KEMs and PKEs are equivalent in the following sense: If there exists an IND-CPA secure PKE scheme, then there exists an IND-CPA secure KEM, and vice versa.
Reminder: A key-encapsulation mechanism (KEM) is a tuple of PPT algorithms $(\mathsf{Gen}, \mathsf{Encaps}, \mathsf{Decaps})$ such that:

   - $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
   - $(c, k) \leftarrow \mathsf{Encaps}_{pk}(1^n)$
   - $k/\perp \leftarrow \mathsf{Decaps}_{sk}(c)$

   It is required that $\Pr[(pk, sk) \leftarrow \mathsf{Gen}(1^n); (c, k) \leftarrow \mathsf{Encaps}_{pk}(1^n) : \mathsf{Decaps}_{sk}(c) = k] \geq 1 - \mathsf{negl}(n)$
Reminder:

   Let $\Pi = (\mathsf{Gen}, \mathsf{Encaps}, \mathsf{Decaps})$ be a KEM and $\mathcal{A}$ an arbitrary adversary.

   The CPA indistinguishability experiment $\mathsf{KEM}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$:

   1. *$\mathsf{Gen}(1^n)$ is run to obtain keys (pk, sk). Then $\mathsf{Encaps}_{pk}(1^n)$ is run to generate (c, k) with $k \in \{0,1\}^n$.*
   2. *A uniform bit $b \in \{0,1\}$ is chosen. If $b = 0$ set $\hat{k} := k$. If $b = 1$ then choose a uniform $\hat{k} \in \{0,1\}^n$.*
   3. *Give $(pk, c, \hat{k})$ to $\mathcal{A}$, who outputs a bit b'. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.*

   In the experiment, $\mathcal{A}$ is given the ciphertext c and either the actual key k corresponding to c, or an independent, uniform key. The KEM is CPA-secure if no efficient adversary can distinguish between these possibilities.

   DEFINITION 11.11 *A key-encapsulation mechanism Π is* CPA-secure *if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there exists a negligible function* negl *such that*

   $$\Pr[\mathsf{KEM}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n).$$

The deadline for the next two questions is until **tomorrow, Friday 18:15**:

1. Say a public-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ for n-bit messages is one-way if the probability $\Pr[\mathsf{PubK}^{\mathsf{ow}}_{\mathcal{A},\Pi}(n) = 1]$ is negligible

for any PPT adversary $\mathcal{A}$. The experiment $\mathsf{PubK}^{\mathsf{ow}}_{\mathcal{A},\Pi}(n)$ is shown as follows.

- $\mathsf{Gen}(1^n)$ is run to obtain (pk, sk).
- A message m is chosen uniformly from $\{0,1\}^n$ and a ciphertext $c \leftarrow \mathsf{Enc}_{pk}(m)$ is generated.
- $\mathcal{A}$ is given (pk, c) and outputs m'.
- $\mathsf{PubK}^{\mathsf{ow}}_{\mathcal{A},\Pi}(n) = 1$ if $m' = m$.

۵ (a) Show that if a public-key encryption scheme Π for n-bit messages has CPA security, then Π is one-way.

۱۰ (b) Show that CPA security is strictly stronger than one-way security. **Hint:** Give a public-key encryption scheme example which has one-way security but does not have CPA security.

۱۰ (c) Construct a CPA secure KEM using one-way secure public-key encryption scheme in the random oracle model. Show your construction and proof ideas.

2. Let $N = pq$ be an RSA modulus and take $e \in \mathbb{N}$ to be a prime that is also relatively prime to $\phi(N)$. Let $u \leftarrow_\$ \mathbb{Z}_N^*$, and define the hash function

$$\mathsf{H}_{N,e,u} : \mathbb{Z}_N \times \{0, ..., e-1\} \to \mathbb{Z}_N \quad \text{where} \quad \mathsf{H}_{N,e,u}(x, y) = x^e u^y \in \mathbb{Z}_N$$

We want to show that under RSA assumption, $\mathsf{H}_{N,e,u}$ defined above is collision-resistant. Namely, suppose there is an efficient adversary $\mathcal{A}$ that takes as input (N, e, u) and outputs $(x_1, y_1) \neq (x_2, y_2)$ such that $\mathsf{H}_{N,e,u}(x_1, y_1) = \mathsf{H}_{N,e,u}(x_2, y_2)$. We use $\mathcal{A}$ to construct an efficient adversary $\mathcal{B}$ that takes as input (N, e, u) where $u \leftarrow_\$ \mathbb{Z}_N^*$ and outputs x such that $x^e = u \in \mathbb{Z}_N$.

   (a) (15 points) Show that using algorithm $\mathcal{A}$ defined above, algorithm $\mathcal{B}$ can efficiently compute $a \in \mathbb{Z}_N$ and $b \in \mathbb{Z}$ such that $a^e = u^b \pmod N$ and $0 \neq |b| < e$. Remember to argue why any inverse you compute will exist (or alternatively, if they do not exist, then $\mathcal{B}$ can directly break RSA).

(b) (5 points) Use the above relation to show how $\mathcal{B}$ can efficiently compute $x \in \mathbb{Z}_N$ such that $x^e = u$.
Hint: Since $|b| < e$ and e is prime, $gcd(b, e) = 1$. Now, apply Bezout's identity. Note that $\mathcal{B}$ does not know the factorization of N, so it is not able to compute $b^{-1} \pmod{\phi(N)}$.
Note: By Bezout's identity, if $gcd(b, e) = 1$, then there exists integers $s, t \in \mathbb{Z}$ such that $bs + et = 1$.

(c) (10 points) Show that if we extend the domain of $\mathsf{H}_{N,e,u}$ to $\mathbb{Z}_N \times \{0, ..., e\}$, then the function is no longer collision-resistant.