Midterm I

Name:

SID:

- **Time: You have *1 hour and 20 minutes* (80 minutes) to complete the exam. The exam runs from 11:10 AM to 12:30 PM. No extra time will be given after 12:30 PM.**
- **After the exam starts, write your name and SID on every odd-numbered page. We reserve the right to deduct points if you do not, and you will not be allowed to do so after time is called.**
- **For short questions, your answers must be written clearly inside the box region. Any answer outside the box will not be graded. For longer questions, if you run out of space, you must clearly mention in the space provided for the question if part of your answer is elsewhere.**
- **You may consult at most *1 double-sided sheet of handwritten notes*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted for looking up content.**
- **There are 6 pages on the exam (counting this one). Notify a proctor immediately if a page is missing.**
- **We will not be answering questions during the exam. If you feel that something is unclear please write a note in your answer.**

1. Suppose $f, g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ are one-way functions. For $x \in \{0,1\}^{2n}$, let $x = (x_1, x_2)$ be the left and right halves of x of length n with "," denoting concatenation, and let $\oplus$ be the bit-wise XOR operator.
   Answer and justify the following with proofs:

   (a) Let $\alpha(x) := (f(x), g(x))$. Is this a one-way function?

   (b) Let $\beta(x) := f(x) \oplus x$. Is this a one-way function?

2. **Weak PRF definition.** In this question we will define weak PRF security and later construct a new weak PRF from a new number-theoretic assumption defined below. Let $F = \{F_n\}_{n\in\mathbb{N}}$ be an efficiently computable function ensemble with $F_n : \mathcal{K}_n \times \mathcal{X}_n \to \mathcal{Y}_n$. The weak PRF security game $\mathsf{wPRF}_F^{\mathcal{A}}(n)$ (for some q):

Challenger:

(a) Sample $b \xleftarrow{\$} \{0,1\}$, $k \xleftarrow{\$} \mathcal{K}_n$.

(b) Sample $x_1, \ldots, x_q \xleftarrow{\$} \mathcal{X}_n$ and $x^* \xleftarrow{\$} \mathcal{X}_n$ (challenge point).

(c) Let $y_i \leftarrow F_n(k, x_i)$ for $i = 1, \ldots, q$.

(d) If $b = 0$ set $y^* \leftarrow F_n(k, x^*)$; else $y^* \xleftarrow{\$} \mathcal{Y}_n$.

Adversary $\mathcal{A}$: receives $(1^n, (x_1, y_1), \ldots, (x_q, y_q), (x^*, y^*))$; outputs $b' \in \{0,1\}$.
Outcome: the game outputs 1 if $b' = b$, and 0 otherwise.

Definition (Weak PRF)**.** *$\{F_n\}_n$ is a* weak PRF (wPRF) *if for every PPT $\mathcal{A}$,*

$$\left|\Pr\left[\mathsf{wPRF}_F^{\mathcal{A}}(n) = 1\right] - \frac{1}{2}\right| \leq \mathsf{negl}(n).$$

q-DDHI assumption. Let $\{\mathbb{G}_n\}_{n\in\mathbb{N}}$ be an ensemble of groups. For $\mathbb{G}_n$, we let its generator be denoted by g and its order be denoted by p. The q-DDHI game $q\text{-}\mathsf{DDHI}_{\mathbb{G}_n}^{\mathcal{D}}(n)$:

Challenger:

(a) Sample $b \xleftarrow{\$} \{0,1\}$, $\tau \xleftarrow{\$} \mathbb{Z}_p^*$.

(b) Compute $V \leftarrow (g, g^{\tau}, g^{\tau^2}, \ldots, g^{\tau^q})$.

(c) If $b = 0$ set $T \leftarrow g^{1/\tau}$; else $T \xleftarrow{\$} \mathbb{G}_n$.

Adversary $\mathcal{D}$: receives (V, T); outputs $b' \in \{0,1\}$.
Outcome: the game outputs 1 if $b' = b$, and 0 otherwise.

Definition (q-DDHI)**.** *The* q-Decisional Diffie-Hellman Inversion (q-DDHI) assumption *holds for $\{\mathbb{G}_n\}_n$ if for every PPT $\mathcal{D}$,*

$$\left|\Pr\left[q\text{-}\mathsf{DDHI}_{\mathbb{G}_n}^{\mathcal{D}}(n) = 1\right] - \frac{1}{2}\right| \leq \mathsf{negl}(n).$$

Problem. We define the function ensemble $\{F_n\}_n$ by

$$F_n \colon (\mathbb{G}_n \times \mathbb{Z}_p) \times \mathbb{Z}_p \to \mathbb{G}_n, \qquad F_n((h,k),x) = h^{1/(k+x)},$$

where $p = |\mathbb{G}_n|$. **Prove** that $\{F_n\}_n$ is a secure wPRF according to the definition above.

Reduction. Given an adversary $\mathcal{A}$ that breaks the weak PRF, we construct an adversary $\mathcal{D}$ that breaks the q-DDHI assumption.

Adversary $\mathcal{D}(1^n, V, T)$ receives $V = (g, V_1, \ldots, V_q)$ and T from the q-DDHI challenger. The code of $\mathcal{D}$:

(1) For $i = 1, \ldots, q$: sample $x_i \leftarrow$

(2) Sample $x^* \leftarrow$

(3) Computation (if any):

(4) For $i = 1, \ldots, q$: set y_i

(5) Set $y^* =$

(6) Run $b' \leftarrow \mathcal{A}\big(1^n, (x_1, y_1), \ldots, (x_q, y_q), (x^*, y^*)\big)$.

(7) What does $\mathcal{D}$ output?

Argument that the reduction works:

3. **LOR-CPA security** Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a symmetric encryption scheme.

   The game $\mathsf{LOR\text{-}CPA}^{\mathcal{A}}_{\Pi}(\lambda)$ proceeds as follows:

   (a) $b \xleftarrow{\$} \{0,1\}$; $k \leftarrow \mathcal{G}(1^\lambda)$

   (b) $\mathcal{A}$ has access to oracle $\mathcal{O}_{k,b}(\cdot,\cdot)$ which does the following:

   - On input (m_0, m_1) with $|m_0| = |m_1|$, returns $c \leftarrow \text{Enc}(k, m_b)$

   (c) $\mathcal{A}$ makes Q queries to $\mathcal{O}_{k,b}$ and outputs b'

   (d) Output 1 iff $b' = b$ and 0 otherwise

   Prove that Π is LOR-CPA secure if and only if it is IND-CPA secure. Provide reductions and justifications for both directions.

   Direction 1: LOR-CPA $\Rightarrow$ IND-CPA. (If Π is LOR-CPA secure then Π is IND-CPA secure.)

   Start: Assume Π is LOR-CPA secure. Let $\mathcal{A}$ be a PPT adversary against IND-CPA. We construct a PPT adversary $\mathcal{B}$ against LOR-CPA such that $\mathcal{B}$ runs $\mathcal{A}$ and ...

Direction 2: IND-CPA $\Rightarrow$ LOR-CPA. (If Π is IND-CPA secure then Π is LOR-CPA secure.)

Start: Assume Π is IND-CPA secure. Let $\mathcal{A}$ be a PPT adversary against LOR-CPA. We construct a PPT adversary $\mathcal{B}$ against IND-CPA such that $\mathcal{B}$ runs $\mathcal{A}$ and ...