Midterm II

Name:

SID:

- **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. However, you may use an electronic device such as a tablet for writing your answers.**
- **DSP Students: If you are allowed $1.5\times$ (resp. $2\times$) the regular exam duration, then you must submit your exam within $120 = 80 * 1.5$ (resp. $160 = 80 * 2$) mins.**
- **The instructors will not be answering questions during the exam. If you feel that something is unclear, please write a note in your answer.**

1 Multiple Choice (20 points)

In the multiple choice section, no explanations are needed for your answers. No points are deducted for wrong answers. Please mark your answers clearly.

1. **Public-Key Encryption:** For each of the following statements, indicate whether it is true or false.

   (a) Encrypting a message using PKE (public-key encryption) is usually slower in practice than encrypting the message using SKE (secret-key encryption).
   ◯ True
   ◯ False

   (b) EAV security is equivalent to CPA security for PKE schemes.
   ◯ True
   ◯ False

   (c) CPA-secure PKE can be constructed from key-exchange protocols and vice versa: key-exchange protocols can be constructed from CPA-secure PKE.
   ◯ True
   ◯ False

   (d) In hybrid encryption, SKE is used to encrypt a shared public key pk for a PKE scheme.
   ◯ True
   ◯ False

2. **Hard-Concentrate Predicates:** Let $f : \{0,1\}^n \to \{0,1\}^n$ be a function that has a hard-concentrate predicate $h : \{0,1\}^n \to \{0,1\}$. Also, let $f(x)_{[1,n-1]}$ be $f(x)$ without the nth bit, and let $f(x)_n$ be the nth bit of $f(x)$.

   Select all of the functions below for which h is (necessarily) a hard-concentrate predicate.

   ◯ $g_1(x) = f(x)_{[1,n-1]}$
   ◯ $g_2(x) = f(x)||\big(h(x) \oplus 1\big)$
   ◯ $g_3(x) = f(x)_n \oplus h(x)$
   ◯ $g_4(x) = f(x)_{[1,n-1]}||\big(f(x)_n \oplus h(x)\big)$

3. **Constructing A from B:** For each of the following statements, indicate whether it is true or false.

   (a) PRGs can be used to construct PRFs, but PRFs are not sufficient to construct PRGs.
   ◯ True
   ◯ False

   (b) Any OWF $f : \{0,1\}^n \to \{0,1\}^{2n}$ is also a PRG.
   ◯ True
   ◯ False

   (c) Any PRG $g : \{0,1\}^n \to \{0,1\}^{2n}$ is also a OWF.
   ◯ True
   ◯ False

   (d) Any length-preserving PRP (pseudorandom permutation) is also a PRF.
   ◯ True
   ◯ False

4. **El Gamal Encryption:** In the El Gamal encryption scheme, let the public key be $\mathsf{pk} = (\mathbb{G}, p, g, g^a)$, where $\mathbb{G}$ is a cyclic group, p is the size of the group, g is a generator of the group, and $a \in \mathbb{Z}_p$ is part of the secret key.

   Which *one* of the following algorithms correctly describes the process to encrypt a message $m \in \mathbb{G}$?

   ◯ Sample $k \leftarrow \mathbb{Z}_p$. Compute $c_1 = g^k$ and $c_2 = g^a \cdot g^k \cdot m$. Output (c_1, c_2).
   ◯ Sample $k \leftarrow \mathbb{Z}_p$. Compute $c_1 = (g^a)^k$ and $c_2 = g^k + m$. Output (c_1, c_2).
   ◯ Sample $k \leftarrow \mathbb{Z}_p$. Compute $c_1 = g^k$ and $c_2 = (g^a)^k \cdot m$. Output (c_1, c_2).
   ◯ Sample $k \leftarrow \mathbb{Z}_p$. Compute $c_1 = (g^a)^k$ and $c_2 = g^k \cdot m$. Output (c_1, c_2).

2 One-Way Functions (15 points)

Question: Let $f : \{0,1\}^n \to \{0,1\}^n$ be a OWF. Use f to construct another OWF g such that $g : \{0,1\}^n \to \{0,1\}^n$ and $g(0^n) = 0^n$. Your answer should describe a construction of g and prove that g is a OWF.

Give a construction of g.

Name:

Prove that the function g constructed above is a secure OWF.

3 Domain Extension with CRHFs (25 Points)

We will examine a simple way to extend the domain of a MAC by first hashing the message with a CRHF.

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function.

Let $\mathcal{H} = (\mathsf{Gen}, H)$ be a collision-resistant hash function with key space $\{0,1\}^n$ and input space $\mathcal{X}$, which may be very large. For every key $s \leftarrow \mathsf{Gen}(1^n)$, $s \in \{0,1\}^n$ and $H^s : \mathcal{X} \to \{0,1\}^n$.

Let $G : \{0,1\}^{2n} \times \mathcal{X} \to \{0,1\}^n$ be defined as follows:

$$G((k,s),x) = F\big(k, H^s(x)\big)$$

3.1 Pseudorandom Function (15 Points)

Question: Prove that G is a pseudorandom function.

You may wish to follow the template provided below.

Let's define several hybrids. For a given adversary $\mathcal{A}$:

1. Let $\mathsf{Hyb}_0(\mathcal{A}, n)$ be the PRF security game in which the adversary $\mathcal{A}$ gets query access to G. In particular:
   (a) The PRF challenger samples $k \leftarrow \{0,1\}^n$ and $s \leftarrow \mathsf{Gen}(1^n)$.
   (b) The adversary $\mathcal{A}$ gets query access to the following function:
   $$G(\cdot) = F(k, H^s(\cdot))$$
   (c) The adversary outputs a bit b, which is the output of the hybrid.
2. Let $\mathsf{Hyb}_1(\mathcal{A}, n)$ be the same as $\mathsf{Hyb}_0(\mathcal{A}, n)$, except $F(k, \cdot)$ is replaced with a uniformly random function $R_1 : \{0,1\}^n \to \{0,1\}^n$:
   (a) The PRF challenger samples a function R_1 uniformly at random from the set of all functions mapping $\{0,1\}^n \to \{0,1\}^n$. They also sample $s \leftarrow \mathsf{Gen}(1^n)$.
   (b) The adversary $\mathcal{A}$ gets query access to the following function:
   $$R_1(H^s(\cdot))$$
   (c) The adversary outputs a bit b, which is the output of the hybrid.

3. Let $\mathsf{Hyb}_2(\mathcal{A}, n)$ be the same as $\mathsf{Hyb}_0(\mathcal{A}, n)$ except $F(k, H^s(\cdot))$ is replaced with a uniformly random function $R_2 : \mathcal{X} \to \{0,1\}^n$:
   (a) The PRF challenger samples a function R_2 uniformly at random from the set of all functions mapping $\mathcal{X} \to \{0,1\}^n$.
   (b) The adversary $\mathcal{A}$ gets query access to:
   $$R_2(\cdot)$$
   (c) The adversary outputs a bit b, which is the output of the hybrid.

Lemma 3.1 *For any PPT adversary $\mathcal{A}$,* $\left|\Pr[\mathsf{Hyb}_0(\mathcal{A}, n) \to 1] - \Pr[\mathsf{Hyb}_1(\mathcal{A}, n) \to 1]\right| \leq \mathsf{negl}(n)$.

Proof:

Name:

Lemma 3.2 *For any PPT adversary* $\mathcal{A}$, $\left|\Pr[\mathsf{Hyb}_1(\mathcal{A}, n) \to 1] - \Pr[\mathsf{Hyb}_2(\mathcal{A}, n) \to 1]\right| \leq \mathsf{negl}(n)$.

Proof:

Name:

Finish the proof.

3.2 Message Authentication Code (10 points)

Question: Use G (defined above) to construct a secure MAC $\Pi = (\mathsf{Gen}_\Pi, \mathsf{Mac}_\Pi, \mathsf{Verify}_\Pi)$ that takes messages $m \in \mathcal{X}$.

You may use the template provided below. You do not need to prove that your construction is secure.

1. $\mathsf{Gen}_\Pi(1^n)$: Sample $k \leftarrow \{0,1\}^n$ and $s \leftarrow \mathsf{Gen}(1^n)$, and output $k_\Pi = (k, s)$.
2. $\mathsf{Mac}_\Pi(k_\Pi, m)$:
3. $\mathsf{Verify}_\Pi(k_\Pi, m, t)$:

4 Public-Key Encryption (20 points)

The composition of two PKE schemes with independent keys is CPA-secure as long as at least one of the schemes is CPA-secure. We will show most of the proof of this claim.

Question: Follow the outline given below and fill in any blanks.

Let us be given two public-key encryption schemes $\Pi_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $\Pi_2 = (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$. Let the ciphertext space of Enc_2 be the same as the message space of Enc_1. Also, one of Π_1 or Π_2 is CPA secure, and the other one is not, but we don't know which one is secure.

Define the composed scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follows. **Fill in the algorithm for Dec so that Π satisfies correctness.**

- $\mathsf{Gen}(1^n)$: Run $\mathsf{Gen}_1(1^n) \to (\mathsf{pk}_1, \mathsf{sk}_1)$ and $\mathsf{Gen}_2(1^n) \to (\mathsf{pk}_2, \mathsf{sk}_2)$. Return $((\mathsf{pk}_1, \mathsf{pk}_2), (\mathsf{sk}_1, \mathsf{sk}_2))$.
- $\mathsf{Enc}((\mathsf{pk}_1, \mathsf{pk}_2), m)$: Return $c = \mathsf{Enc}_1(\mathsf{pk}_1, \mathsf{Enc}_2(\mathsf{pk}_2, m))$.
- $\mathsf{Dec}((\mathsf{sk}_1, \mathsf{sk}_2), c)$: Return $\boxed{}$

Theorem 4.1 *If Π_1 is CPA-secure or Π_2 is CPA-secure, then Π is CPA-secure.*

Proof:

1. Overview: To show that Π is CPA-secure, we will give a proof by contradiction. Suppose that there is a PPT adversary $\mathcal{A}$ that wins the CPA security game for Π with non-negligible probability. Then we will construct an adversary $\mathcal{B}_1$ for the CPA game for Π_1 and an adversary $\mathcal{B}_2$ for the CPA game for Π_2. Both $\mathcal{B}_1$ and $\mathcal{B}_2$ will succeed with non-negligible probability, which breaks CPA security for both Π_1 and Π_2. This contradicts the fact that at least one of them was CPA-secure.

Name:

2. **Use $\mathcal{A}$ to construct an adversary $\mathcal{B}_1$ for the CPA game for Π_1. $\mathcal{B}_1$ should win the CPA game for Π_1 with the same probability that $\mathcal{A}$ wins the CPA game for Π. Do not include the proof that your adversary works, just construct the adversary.**

3. **Use $\mathcal{A}$ to construct an adversary $\mathcal{B}_2$ for the CPA game for Π_2. $\mathcal{B}_2$ should win the CPA game for Π_2 with the same probability that $\mathcal{A}$ wins the CPA game for Π. Do not include the proof that your adversary works, just construct the adversary.**

■