Midterm I

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 $130 = 80 * 1.5 + 10$ (resp. $170 = 80 * 2 + 10$) mins.**
- **We 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 (15 points)

In the multiple choice section, no explanations are needed for your answers. Each question is worth 3 points, and there is no penalty for wrong answers. Please mark your answers clearly.

1. Which of the following functions are negligible? (There may be multiple negligible functions.)
   ◯ $2^{-\log_2(n)}$

   ◯ $2^{-(\log_2(n))^3}$

   ◯ $2^{-\sqrt{n}}$

   ◯ $2^{-(n^2)}$
2. True or False: If $f(n)$ and $g(n)$ are non-negligible functions, then $h(n) = f(n) \cdot g(n)$ is also non-negligible.
   ◯ True

   ◯ False
3. True or False: If an encryption scheme Π is CCA-secure, then it is also CPA-secure.
   ◯ True

   ◯ False
4. Suppose $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a CPA-secure encryption scheme that encrypts messages belonging to a field $\mathbb{F}$. Construct a new encryption scheme as follows:
   - $\mathsf{Gen}_1(1^n)$: samples $k' \leftarrow \mathsf{Gen}(1^n)$. Then it samples p, a random degree-d polynomial over the field $\mathbb{F}$. The key k for this encryption scheme is the tuple of these values:
     $$k = (k', p)$$
     (here p refers to the description of the polynomial)
   - $\mathsf{Enc}_1(k, m)$ computes and outputs $c = \mathsf{Enc}(k', m) \parallel p(m)$.
   - $\mathsf{Dec}_1(k, c)$ just runs $\mathsf{Dec}(k', \cdot)$ on the first part of the ciphertext.

   In the CPA security experiment, what is the minimum number of queries to the Enc_1 oracle that are needed to break the CPA security of the scheme $(\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$. i.e. What is the minimum number of queries needed to figure out b given $\mathsf{Enc}_1(k, m_b)$?

   Only count phase-I and phase-II queries; do not count the query used to compute the challenge ciphertext.

Name:

5. Which of the following modes of encryption do **not** require the PRF/PRP F_k used to be efficiently invertible? There may be multiple such modes.

   ◯ Electronic Code Book (ECB)

   ◯ Cipher Block Chaining (CBC)

   ◯ Output Feedback (OFB)

   ◯ Counter (CTR)

2 Pseudorandom Functions (15 points)

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

$$G(k,(x,y)) = F(k,x) \oplus F(k,y)$$

Prove that G is not a secure pseudorandom function.

The parts below will outline the proof that G is not pseudorandom and ask you to fill in the missing details to complete the proof.

To show that G is not a secure PRF, let us construct a distinguishing algorithm D that can distinguish $G(k,\cdot)$ from a truly random function $R(\cdot)$ (given query access to one of these functions).

1. D makes a single query (x^*, y^*) to the function:

   $(x^*, y^*) =$ $\boxed{}$

   Let z^* be the response obtained.

2. Next, D outputs 1 if

   $\boxed{}$

   and outputs 0 otherwise.

3. *Pseudorandom case:* In the case where D is querying $G(k,\cdot)$, what is the probability that D outputs 1 (i.e. what is $\Pr[D^{G(k,\cdot)} = 1]$)? Here the probability is over the randomness of D and the randomness of sampling k.

   Explain your reasoning.

   $\boxed{}$

Name:

4. *Truly random case:* Let R be a function sampled uniformly at random from the set of all functions that map $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$.

   In the case where D is querying $R(\cdot)$, what is the probability that D outputs 1 (i.e. what is $\Pr[D^{R(\cdot)} = 1]$)? Here the probability is over the randomness of D and the randomness of sampling R.

   Explain your reasoning.

5. Finish the proof to argue that D breaks PRF security for G.

3 Pseudorandom Functions Again (15 points)

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Prove that the following function H is also a pseudorandom function:

$$H(k, x) = F(k, x) \oplus x$$

Name:

4 CPA-Secure Encryption (20 points)

Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure encryption scheme. Below, we will construct another encryption scheme and prove that it is also CPA-secure.

In the encryption scheme below, let the message m belong to $\{0,1\}^n$.

- $\mathsf{Gen}_1(1^n)$: Sample the key as follows: $k \leftarrow \mathsf{Gen}(1^n)$.
- $\mathsf{Enc}_1(k, m)$: Sample $r \leftarrow \{0,1\}^n$ uniformly at random. Then compute $c_0 := \mathsf{Enc}(k, r)$ and $c_1 := r \oplus m$. Output the ciphertext $c = (c_0, c_1)$.
- $\mathsf{Dec}_1(k, (c_0, c_1))$: **Unspecified**

1. Fill in the decryption algorithm so that every ciphertext is decrypted correctly.

   $\mathsf{Dec}_1(k, (c_0, c_1))$:

2. Prove that $(\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ satisfies CPA security.

Name:

5 Perfectly Secret Encryption (15 points)

In this problem we propose a definition of perfect secrecy for the encryption of *two* messages. We will prove that this definition *cannot* be satisfied by any encryption scheme.

Notation: We consider distributions over *pairs* of messages from the message space $\mathcal{M}$; we let M_1 and M_2 be random variables denoting the first and second message, respectively. (We stress that these random variables are not assumed to be independent.)

Encryption works as follows:

1. Generate a (single) key k, sample a pair of messages (m_1, m_2) according to the given distribution.
2. Compute ciphertexts $c_1 \leftarrow \mathsf{Enc}(k, m_1)$ and $c_2 \leftarrow \mathsf{Enc}(k, m_2)$; this induces a distribution over pairs of ciphertexts, and we let C_1 and C_2 be the corresponding random variables.

Proposed definition: Let us say that an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *perfectly secret for two messages* if for all distributions over $\mathcal{M} \times \mathcal{M}$, all $(m_1, m_2) \in \mathcal{M} \times \mathcal{M}$, and all ciphertexts $(c_1, c_2) \in \mathcal{C} \times \mathcal{C}$ for which $\Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$,

$$\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2].$$

Question: Prove that no encryption scheme can satisfy the definition above. (You may assume that the encryption scheme satisfies perfect correctness).