Instructions

- You are allowed to work in groups of size at most 2.
- The assignments must be typed in Latex, and the resulting pdf must be submitted on Gradescope.
- The bonus question is somewhat challenging, and you are recommended to attempt it only after solving all the other problems.
- **Plagiarism policy**: You should not discuss your solutions with other group members. Sharing your solutions with other group members is strictly not allowed, and if there are significant similarities in two or more submissions, all relevant group members will be penalized.

  You can refer to resources online, but you should write your solutions in your own words (and also cite the resources used).

Notations

- For any natural number ℓ, $\{0,1\}^{\leq \ell}$ denotes the set of all binary strings of length at most ℓ.
- Some of the problems in this assignment use the $\mathsf{No\text{-}Query\text{-}Semantic\text{-}Security}$ game, which was defined in Lecture 04 (Definition 04.02). However, in some cases, we allow the message space to be $\mathcal{M} = \{0,1\}^{\leq \ell}$ for some ℓ. In such cases, the adversary must send messages m_0, m_1 of the same length.

Questions

1. (10 marks) **Encryption Schemes with relaxed security**

   Let $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme with message space $\mathcal{M}$, key space $\mathcal{K}$ and ciphertext space $\mathcal{C}$. The scheme satisfies perfect correctness, but not perfect secrecy. Instead, it satisfies the following relaxed secrecy guarantee:

   For any adversary $\mathcal{A}$, $\Pr[\mathcal{A}$ wins the $\mathsf{No\text{-}Query\text{-}Semantic\text{-}Security}$ game$] \leq 1/2 + \epsilon$, where the security game $\mathsf{No\text{-}Query\text{-}Semantic\text{-}Security}$ is an interactive game between a challenger and an adversary, and is defined in Figure 1.

$\mathsf{No\text{-}Query\text{-}Semantic\text{-}Security}$
1. Adversary sends two messages m_0, m_1 to the challenger.
2. The challenger chooses a bit $b \leftarrow \{0,1\}$, key $k \leftarrow \mathcal{K}$ and sends $\mathsf{Enc}(m_b, k)$ to the adversary.
3. The adversary sends its guess b', and wins the security game if $b = b'$.

Figure 1: The No-Query Semantic Security Game

   What can we conclude about $|\mathcal{K}|$ vs $|\mathcal{M}|$? And $|\mathcal{C}|$ vs $|\mathcal{M}|$?

2. (10 marks) **Security against key recovery attacks**

   Let $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme with message space $\mathcal{M}$, ciphertext space $\mathcal{C}$ and key space $\mathcal{K}$. Consider the following security game between a challenger and an adversary:

   We say that $\mathcal{E}$ is secure against key-recovery attacks if, for every prob. poly. time adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n,

$$\Pr[\mathcal{A} \text{ wins the } \mathsf{Key\text{-}Recovery\text{-}Security} \text{ game }] \leq 1/|\mathcal{K}| + \mu(n).$$

   1. (3 marks) Show that Shannon's One-Time Pad is not secure against key recovery attacks.

Key-Recovery-Security
1. The challenger chooses a message $m \leftarrow \mathcal{M}$, key $k \leftarrow \mathcal{K}$ and sends $(m, \mathsf{Enc}(m,k))$ to the adversary.
2. The adversary sends its guess k', and wins the security game if $k = k'$.

Figure 2: The Key-Recovery Game

2. (7 marks) Let $G : \{0,1\}^n \to \{0,1\}^{100n}$ be a secure pseudorandom generator. Show that the encryption scheme $\mathcal{E}_G$ (with key space $\mathcal{K} = \{0,1\}^n$ and message space $\mathcal{M} = \{0,1\}^{100n}$) satisfies Key-Recovery-Security, assuming G is a secure PRG.

3. (15 marks) **Bad Disk Encryption**

Disk encryption systems often use regular secret key encryption schemes. Sometimes, these systems store the secret key on the disk before encrypting the disk, and this can lead to security attacks! This may seem counter-intuitive at first, since the encryption scheme used satisfies standard security definitions (such as the semantic security definition discussed in class).

The vulnerability arises because the 'message' being encrypted depends on the key itself. In the regular definitions, the adversarially chosen messages m_0, m_1 are independent of the secret key.

Let $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme with message space $\{0,1\}^{\leq \ell}$ and key space $\{0,1\}^n$, where $\ell > n$. Security against key-dependent-message attacks is captured via the security game defined in Figure 3:

KDMSecurity
1. The adversary chooses two message m_0, m_1 of equal length, $\lvert m_0 \rvert = \lvert m_1 \rvert \leq \ell - n$.
2. The challenger chooses a secret key $k \leftarrow \{0,1\}^n$, bit $b \leftarrow \{0,1\}$, and sends $\mathsf{Enc}(k \mid\mid m_b, k)$.
3. The adversary guesses whether it received a key-dependent encryption of m_0 or m_1. It sends its guess b', and wins if $b = b'$.

Figure 3: Key Dependent Message Security

An encryption scheme $\mathcal{E}$ is secure against key-dependent attacks if for any probabilistic polynomial time adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for all n, $\mathcal{A}$ wins in the above security game with probability at most $1/2 + \mathsf{negl}(n)$.

In this problem, we will show that no-query semantic security (Definition 04.02 defined in Lecture 04) does not imply key-dependent message security. Let $\mathcal{E}$ be an encryption scheme with message space $\mathcal{M} = \{0,1\}^{\leq \ell}$, key space $\mathcal{K} = \{0,1\}^n$ ($\ell > n$) and it satisfies no-query semantic security (note: since the message space allows messages of different length, in the No-Query-Semantic-Security game, both messages m_0, m_1 must be of same length).

Your goal is to build a new encryption scheme $\mathcal{E}'$ (using $\mathcal{E}$ as a building block).

- (4 marks) Construct encryption scheme $\mathcal{E}'$ using $\mathcal{E}$ as a building block. The new encryption scheme must have the same message and key space as $\mathcal{E}$. However, you are allowed to alter the ciphertext space. Show that $\mathcal{E}'$ satisfies perfect correctness, assuming $\mathcal{E}$ is perfectly correct.

  You should not assume anything about the base encryption scheme $\mathcal{E}$, other than the fact that it has key space $\mathcal{K} = \{0,1\}^n$, message space $\{0,1\}^{\leq \ell}$ and satisfies perfect correctness and No-Query-Semantic-Security.

- (7 marks) Show that $\mathcal{E}'$ satisfies no-query semantic security, assuming $\mathcal{E}$ is no-query semantic secure. That is, show that if there exists a p.p.t. adversary $\mathcal{A}$ that breaks the no-query semantic

security of $\mathcal{E}'$, then there exists a p.p.t. algorithm $\mathcal{B}$ that breaks the no-query semantic security of $\mathcal{E}$.

- (4 marks) Show that $\mathcal{E}'$ does not satisfy key-dependent message security. In particular, show that there exists a polynomial time algorithm that wins the key-dependent security game with probability close to 1.

4. (15 marks) **Bit Commitment Schemes from PRGs**

In class, we saw that a PRG can be used for building a secure encryption scheme $\mathcal{E}_G$. Here, we will use PRGs as a building block for building a *digital commitment scheme*.

Commitment Schemes: Consider the following scenario — an instructor has put out a difficult assignment, and wants to convince his students that he knows the solutions. To do so, he puts the written solutions in a locked briefcase, and hands the locked briefcase to his students. Later, once the assignment deadline is over, he opens the briefcase using his key, and the students can access the solutions, and verify that he indeed knew the solutions. We require two properties here:

- The locked briefcase should not reveal the contents inside. The students should not be able to access the solutions before the deadline. This is the *hiding property*.
- The instructor should not be able to 'modify' the contents. This is to ensure that the instructor indeed knows the solutions (and is not simply 'copying' the solutions of his bright students). In the case of a physical briefcase, such modification of contents is not possible, and we want to keep this in mind when we move to the digital analogue.

Digital Commitment Schemes: Digital commitment schemes are the digital analogue of a sealed briefcase. In this problem, we will consider one-round bit commitment schemes. Here, Alice wants to commit to a single bit $b \in \{0,1\}$. She interacts with Bob. Bob sends the first message, after which Alice sends the commitment to Bob. At a later point, Alice can give an 'opening' to convince Bob that she had committed to bit b. Until Bob receives the opening, Bob should not be able to know whether Alice had committed to bit 0 or 1. This is a one-round commitment scheme since Bob sends one message, Alice sends another message and that completes the commitment phase.

More formally, a one-round commitment scheme consists of three algorithms: $\mathsf{Commit\text{-}Rec}, \mathsf{Commit\text{-}Send}$ and Open with the following syntax:

- $\mathsf{Commit\text{-}Rec}(1^n)$: takes as input the security parameter, and outputs the receiver-message $\mathsf{r\text{-}msg}$.
- $\mathsf{Commit\text{-}Send}(\mathsf{r\text{-}msg}, b)$: takes as input the receiver-message, the bit b to be committed, and outputs a commitment com and opening op.
- $\mathsf{CheckOpen}(\mathsf{r\text{-}msg}, \mathsf{com}, \mathsf{op}, b)$: is a deterministic algorithm that takes as input the receiver-message $\mathsf{r\text{-}msg}$, a commitment com, opening op, bit b and outputs 1 (indicating that op is a valid opening for (com, b)) or 0 (indicating that op is not a valid opening for (com, b)).

These algorithms must satisfy the following correctness property for any $b \in \{0,1\}$:

$$\Pr\left[\begin{array}{c} \mathsf{r\text{-}msg} \leftarrow \mathsf{Commit\text{-}Rec}(1^n); \\ (\mathsf{com}, \mathsf{op}) \leftarrow \mathsf{Commit\text{-}Send}(\mathsf{r\text{-}msg}, b); \\ \mathsf{CheckOpen}(\mathsf{r\text{-}msg}, \mathsf{com}, \mathsf{op}, b) = 1 \end{array}\right] = 1$$

where the probability is over the randomness used by $\mathsf{Commit\text{-}Rec}$, $\mathsf{Commit\text{-}Send}$.

A commitment scheme must satisfy the following two security properties:

- **Binding property**: Intuitively, no adversarial sender should be able to commit to one bit, and later produce opening for a different bit.

  Formally, a commitment scheme satisfies the binding property if for any prob. poly. time adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n, $\Pr[\mathcal{A} \text{ wins the binding security game}] \leq \mu(n)$ where the binding security game is defined below:

Binding-Game
– Challenger chooses $\mathsf{r\text{-}msg} \leftarrow \mathsf{Commit\text{-}Rec}(1^n)$ and sends $\mathsf{r\text{-}msg}$ to $\mathcal{A}$.
– Adversary sends a commitment com, together with two openings op_0 and op_1. The adversary wins if $\mathsf{CheckOpen}(\mathsf{r\text{-}msg}, \mathsf{com}, \mathsf{op}_0, 0) = \mathsf{CheckOpen}(\mathsf{r\text{-}msg}, \mathsf{com}, \mathsf{op}_1, 1) = 1$.

Figure 4: The Binding Security Game

- **Hiding property**: Intuitively, no advesarial receiver should be able to learn the bit committed, given only the commitment. Note that the adversary is allowed to choose the receiver-message arbitrarily. This security is defined via the bit-guessing game, but we can also consider the equivalent two-worlds formulation.

  Formally, a commitment scheme satisfies the hiding property if for any prob. poly. time adversary $\mathcal{A}$, there exists a neglibile function $\mu(\cdot)$ such that for all n, $\Pr[\mathcal{A} \text{ wins the hiding security game}] \leq 1/2 + \mu(n)$ where the binding security game is defined below:

Hiding-Game
– Adversary sends $\mathsf{r\text{-}msg}$ to the challenger.
– Challenger chooses $b \leftarrow \{0,1\}$, computes $(\mathsf{com}, \mathsf{op}) \leftarrow \mathsf{Commit\text{-}Send}(\mathsf{r\text{-}msg}, b)$ and sends com to $\mathcal{A}$ (note that the adversary does not get op).
– Adversary sends guess b' and wins if $b = b'$.

Figure 5: The Hiding Security Game

Construction: Let $G : \{0,1\}^n \to \{0,1\}^{3n}$ be a secure PRG. Consider the following commitment scheme:

- $\mathsf{Commit\text{-}Rec}(1^n)$: sends a uniformly random $3n$-bit string $\mathsf{r\text{-}msg} \leftarrow \{0,1\}^{3n}$.
- $\mathsf{Commit\text{-}Send}(\mathsf{r\text{-}msg}, b)$: chooses a uniformly random n-bit string $s \leftarrow \{0,1\}^n$. If $b = 0$, it sets $\mathsf{com} = G(s)$, else it sets $\mathsf{com} = G(s) \oplus \mathsf{r\text{-}msg}$. The opening is the string s.
- $\mathsf{CheckOpen}(\mathsf{r\text{-}msg}, \mathsf{com}, \mathsf{op}, b)$: if $b = 0$, the algorithm checks if $G(\mathsf{op}) = \mathsf{com}$, and if $b = 1$, it checks if $G(\mathsf{op}) \oplus \mathsf{r\text{-}msg} = \mathsf{com}$.

Questions:

1. (6 marks) Show that if G is a secure PRG, then the above commitment scheme satisfies the hiding property. Give a formal proof by first defining the reduction algorithm, then analyse the reduction algorithm's success probability.
2. (6 marks) Show that the above scheme satisfies the binding property. This part does not rely on the security of PRG, and should hold true for any function G with input space $\{0,1\}^n$ and output space $\{0,1\}^{3n}$.
3. (3 marks) What is the role of the receiver's first message in this scheme? In other words, what would break if $\mathsf{Commit\text{-}Rec}$ simply outputs an empty message, and $\mathsf{Commit\text{-}Send}$ chooses $\mathsf{r\text{-}msg}$?

5. (Bonus Question: 5 marks) In this question, we will see a variant of the PRG definition, called *circular PRG security*. We want to study whether regular PRG security implies circular PRG security.

Let $G : \{0,1\}^n \to \{0,1\}^{n^2}$ be a deterministic function. We can parse the output as n strings, each n bits long. We say that G satisfies circular PRG security, if for any p.p.t adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n, $\Pr[\mathcal{A} \text{ wins the circular PRG security game}] \leq 1/2 + \mu(n)$, where the circular PRG security game is defined below:

Circular-PRG security

- Challenger chooses $b \leftarrow \{0,1\}$, $s \leftarrow \{0,1\}^n$ and $y = (y_1 \mid\mid \ldots \mid\mid y_n) \leftarrow \{0,1\}^{n^2}$ (where each $y_i \in \{0,1\}^n$).
  If $b = 0$, it first computes $z = G(s)$. Parse $z = (z_1 \mid\mid z_2 \ \ldots \mid\mid z_n)$ where each $z_i \in \{0,1\}^n$. For each $i \in [n]$, if $s_i = 0$, then sets $u_i = y_i$, else sets $u_i = z_i$. It sends u to $\mathcal{A}$.
  If $b = 1$, it sends $u = y$ to $\mathcal{A}$.
- Adversary sends guess b' and wins if $b = b'$.

Figure 6: The Circular PRG Security Game

Intuitively, it appears that PRG security should imply circular PRG security. If $b = 0$, the adversary receives pseudorandom bits at some positions, and random bits at some positions, and we might expect that if G satisfies PRG security, then it must also satisfy circular PRG security. However, note that the obvious reduction does not work. This is because PRG security does not imply circular PRG security.

Let $G : \{0,1\}^n \to \{0,1\}^{n^2}$ be a secure PRG. Construct a new function G' with the same input/output domain such that G' is a secure PRG, but does not satisfy circular PRG security.