Sample Quiz Questions

1. Let $\mathcal{E} = (\mathsf{Enc}, \mathsf{Dec})$ be a perfectly secure encryption scheme (satisfies Def. 02.04). Is it possible that there exists message m and ciphertexts c_0, c_1 such that $\Pr\Big[\mathsf{Enc}(m,k) = c_0\Big] \neq \Pr\Big[\mathsf{Enc}(m,k) = c_1\Big]$ where the probabilities are over the choice of key k.

2. Let $[A-Z]$ denote the set of all characters from A to Z, and Γ the set of all permutations $\sigma : [A-Z] \to [A-Z]$.

   Consider the following encryption scheme: the message space is $[A-Z]^{100}$, key space is the set Γ^{100} (that is, every message consists of 100 characters, and every key consists of 100 permutations). To encrypt a message $m = (m_1, \ldots, m_{100})$ using key $k = (\sigma_1, \ldots, \sigma_{100})$, output $(\sigma_1(m_1), \ldots, \sigma_{100}(m_{100}))$. Does this scheme satisfy perfect security?

3. Consider the following security game (w.r.t encryption scheme $\mathcal{E} = (\mathsf{Keygen}, \mathsf{Enc}, \mathsf{Dec})$):

Key-Recovery

- Challenger chooses a uniformly random key k, a uniformly random message m and outputs $\Big(m, \mathsf{Enc}(m,k)\Big)$.
- Adversary outputs k' and wins if $k = k'$.

Figure 1: Security Against Key Recovery Attacks

An encryption scheme is secure against key recovery attacks if, for any prob. poly. time adversary $\mathcal{A}$, there exists a negligible function $\mu(\cdot)$ such that for all n, $\Pr\Big[\mathcal{A} \text{ wins the } \mathsf{Key\text{-}Recovery} \text{ game }\Big] \leq \mu(n)$.

Show that Shannon's One Time Pad is not secure against key recovery attacks.

4. Let $G : \{0,1\}^n \to \{0,1\}^{3n}$ be a secure pseudorandom generator. Consider the following function $G' : \{0,1\}^{2n} \to \{0,1\}^{3n}$:
$$G'(s_1 \mid\mid s_2) = G(s_1) \ \wedge \ G(s_2)$$
   where $||$ denotes string concatenation, and $\wedge$ denotes bitwise AND. Explain (intuitively) why G' is not a secure PRG.

5. Consider the following encryption scheme with key space $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^n$:
   - $\mathsf{Enc}(m,k)$: Let $n = |k|$ (the bit-length of k). If n is prime, then output m, else output $m \oplus k$.
   - $\mathsf{Dec}(\mathsf{ct},k)$: Let $n = |k|$. If n is prime, then output ct, else output $\mathsf{ct} \oplus k$.

   Does this scheme satisfy $\mathsf{No\text{-}Query\text{-}Semantic\text{-}Security}$ (Definition 04.02)?

Sample Assignment Question: Pseudorandom Generators with Related Key Security

Problem Statement:

In Lecture 04, we discussed the notion of pseudorandom generators. A length-doubling pseudorandom generator is a deterministic function $G : \{0,1\}^n \to \{0,1\}^{2n}$, and for all p.p.t. adversaries $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for all n,
$$\Pr[\mathcal{A} \text{ wins the PRG security game}] \leq 1/2 + \mathsf{negl}(n).$$

Recall, we discussed that PRGs may not be secure if the adversary sees the outputs on 'related seeds'. In this exercise, we define a special case of PRG security w.r.t. related seeds. Let $G : \{0,1\}^n \to \{0,1\}^{\ell}$, with $\ell > n$. Consider the following security game between a challenger and an adversary:

Related-PRG

1. The challenger chooses a uniformly random bit $b \leftarrow \{0,1\}$.
   If $b = 0$, the challenger chooses a seed $s \leftarrow \{0,1\}^n$, sets $s' = s \oplus 0\ldots01$,[a] and sends $u_1 = G(s)$, $u_2 = G(s')$.
   If $b = 1$, the challenger chooses two uniformly random strings $u_1, u_2 \leftarrow \{0,1\}^\ell$ and sends u_1, u_2 to $\mathcal{A}$.
2. The adversary sends its guess b', and wins the security game if $b = b'$.

[a]The string s' is same as s, except that the last bit is flipped.

Figure 2: Related Seed PRG Security Game

A length expanding function $G : \{0,1\}^n \rightarrow \{0,1\}^\ell$ (with $\ell > n$) is said to satisfy pseudorandomness security with related seeds if, for any p.p.t. adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\cdot)$ such that for all n,

$$\Pr[\mathcal{A} \text{ wins in the Related Seed PRG Security Game}] \leq 1/2 + \mathsf{negl}(n).$$

We will show that PRG security does not imply pseudorandomness security with related seeds. Let $G : \{0,1\}^n \rightarrow \{0,1\}^{2n}$ be a secure pseudorandom generator. Construct a new length expanding function G' with appropriate input/output space such that G' is also a secure pseudorandom generator (assuming G is a secure pseudorandom generator), but G' does not satisfy pseudorandomness with related seeds.

1. Construct G'. Your construction should use G as a building block.
2. Show that G' is a secure pseudorandom generator. That is, if there exists a p.p.t. adversary $\mathcal{A}$ and a non-negligible function ϵ such that

   $$\Pr[\mathcal{A} \text{ wins the PRG security game against } G'] = \epsilon_{\mathcal{A}},$$

   then there exists a p.p.t. algorithm $\mathcal{B}$ and a non-negligible function $\epsilon_{\mathcal{B}}$ such that

   $$\Pr[\mathcal{B} \text{ wins the PRG security game against } G] = \epsilon_{\mathcal{B}}.$$

3. Show that G' does not satisfy security pseudorandomnes security with related keys.