

Quiz 1

Full Marks: 20, Time: 1 hour

Instructor: Sruthi Sekar

Date: 3rd Sept 2025

Roll Number: _____ Name: _____

1. Enter both roll number and name in the answer sheet.
2. Answer each question on a new page of the answer booklet.
3. Do not use pencils. Pens only!
4. If you are using the secure construction from any question in another question, feel free to just refer to that question and use it as it is.
5. If you are using some fact proved in class during lectures, please mention the fact clearly and intuitively explain it before using it in your questions.

Definitions You Need

Negligible Functions: Recall that a function $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ is negligible if for every polynomial p , there exists $n_0 \in \mathbb{N}$ such that: $\mu(n) < 1/p(n)$, for all $n > n_0$.

Pseudorandom Generators (PRGs): Recall the definition of pseudorandom generators (PRGs). A deterministic polynomial-time algorithm G is a pseudorandom generator (PRG) if it is length-expanding: for any n , and any $k \in \{0, 1\}^n$, $G(k) \in \{0, 1\}^{\ell(n)}$ with $\ell(n) > n$, and satisfies either of the following two equivalent properties:

- **Unpredictability:** G is next-bit unpredictable if for every PPT adversary, **Eve**, there exists a negligible function negl such that $\forall n$

$$\forall i, \Pr[\text{Eve}(G(k)|_{1,2,\dots,i}) = G(k)|_{i+1}] \leq 1/2 + \text{negl}(n),$$

where $G(k)|_{1,2,\dots,i}$ denotes the first i -bits of $G(k)$, and $G(k)|_{i+1}$ denotes its $(i+1)$ -th bit.

- **Pseudorandomness:** G is pseudorandom if for every PPT adversary, **Eve**, there exists a negligible function negl such that $\forall n$

$$\left| \Pr_{k \in_R \{0,1\}^n} [\text{Eve}(G(k)) = 1] - \Pr_{r \in_R \{0,1\}^{\ell(n)}} [\text{Eve}(r) = 1] \right| \leq \text{negl}(n)$$

Pseudorandom Functions (PRFs): Recall the definition of pseudorandom functions (PRFs). A family of functions $\{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0,1\}^n}$ is a pseudorandom function (PRF) if for every PPT adversary, **Eve**, there exists a negligible function negl such that $\forall n$

$$\left| \Pr_{k \in_R \{0,1\}^n} [\text{Eve}^{f_k(\cdot)}(1^n) = 1] - \Pr_{R \in_R \mathcal{F}_n} [\text{Eve}^{R(\cdot)}(1^n) = 1] \right| \leq \text{negl}(n),$$

where $\mathcal{F}_n$ is the set of functions: $\mathcal{F}_n := \{f : \{0, 1\}^n \rightarrow \{0, 1\}^n\}$. Here $\text{Eve}^{f_k(\cdot)}$ and $\text{Eve}^{R(\cdot)}$ denote **Eve** getting oracle access to functions f_k and R , respectively.

Symmetric key Encryption: A symmetric-key encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ with message space $\mathcal{M}$ satisfies correctness: for every n , for every $k \leftarrow \text{Gen}(1^n)$, and for every $m \in \mathcal{M}$, $\Pr[\text{Dec}(k, \text{Enc}(k, m)) = m] = 1$. Additionally, recall the following security notions for Π .

- **Ciphertext Only Attack (COA):** Define the following game $\text{PrivK}_{\text{Eve}, \Pi}^{\text{coa}}(n)$ between a challenger and the adversary Eve:

1. Eve, on input 1^n outputs a pair of messages m_0, m_1 with $|m_0| = |m_1|$.
2. Challenger generates $k \leftarrow \text{Gen}(1^n)$; picks $b \in_R \{0, 1\}$; sends $c_b \leftarrow \text{Enc}(k, m_b)$ to Eve.
3. Eve on input c_b outputs a bit b' .
4. Output 1 if $b' = b$, and 0, otherwise.

Π is said to be secure against a ciphertext only attack if for all PPT adversaries Eve, there exists a negligible function negl such that $\forall n$, $\Pr[\text{PrivK}_{\text{Eve}, \Pi}^{\text{coa}}(n) = 1] \leq 1/2 + \text{negl}(n)$.

- **Chosen Plaintext Attack (CPA):** Define the following game $\text{PrivK}_{\text{Eve}, \Pi}^{\text{cpa}}(n)$ between a challenger and the adversary Eve:

1. Challenger generates $k \leftarrow \text{Gen}(1^n)$ and gives oracle access of $\text{Enc}_k(\cdot)$ to Eve.
2. Eve, on oracle access to $\text{Enc}_k(\cdot)$ and input 1^n , outputs a pair of messages m_0, m_1 with $|m_0| = |m_1|$.
3. Challenger picks $b \in_R \{0, 1\}$; sends $c_b \leftarrow \text{Enc}(k, m_b)$ to Eve.
4. Eve continues to have oracle access to $\text{Enc}_k(\cdot)$ and outputs a bit b' .
5. Output 1 if $b' = b$, and 0, otherwise.

Π is said to be secure against a chosen plaintext attack if for all PPT adversaries Eve, there exists a negligible function negl such that $\forall n$, $\Pr[\text{PrivK}_{\text{Eve}, \Pi}^{\text{cpa}}(n) = 1] \leq 1/2 + \text{negl}(n)$.

Problem 1 (3 marks (1+1+1)). Are the following functions negligible or not? Justify in a sentence or two (no detailed proof needed if negligible, give a counterexample if not negligible).

- a) $\mu_1(n) := 1/n^{\log n}$
- b) $\mu_2(n) := \nu_1(n) \div \nu_2(n)$, for any negligible functions ν_1 and ν_2 .
- c) $\mu_3(n) := n^{\log n} \cdot \nu(n)$, for a negligible function ν .

Problem 2 (3 marks). Let $F := \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be a PRF. Define the following family of functions. $F' := \{f'_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ is such that:

$$f'_k(x) := \begin{cases} 0^n, & \text{if } k = 0^n \\ f_k(x), & \text{otherwise} \end{cases}$$

Using a formal security reduction, prove that if F is a PRF, then F' is a PRF.

Problem 3 (8 marks (3+3+2)). Show that G_1 and G_2 are not PRGs, with a clear distinguishing attack on pseudorandomness or a clear next-bit predictor. Show that F is not a PRF, with a clear distinguisher between the PRF world and the random function oracle world. Explain the attacks in complete detail.

- a) $G_1(s) := G(s) || G(\bar{s})$, for any PRG G and $||$ denotes concatenation. Here, $\bar{s}$ denotes the string obtained by negating each bit of s .
- b) $G_2(s) := f_1(s) || f_2(s) || \dots || f_n(s)$, for any PRF $\{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$. (Here, $k \in \{1, \dots, n\}$ are each represented as n -bit strings.)
- c) F is a keyed function family: for security parameter n , the key is an $n \times n$ boolean matrix A and an n -bit boolean vector b . $F_{A,b} : \{0, 1\}^n \rightarrow \{0, 1\}^n$ is defined by $F_{A,b}(x) := Ax + b$, where all operations are done modulo 2.

(**Hint:** If needed, come up with underlying PRGs/PRFs that will help you with an attack.)

Problem 4 (6 marks (3+3)). For each of the following symmetric key encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, which of the following attacks is Π secure against: ciphertext only attack (COA), chosen plaintext attack (CPA)? For each answer, give a complete formal proof of security (by reduction) or a counterexample along with a complete attack.

- a) Let $\{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be a PRF. Define $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ for $\mathcal{M} = \{0, 1\}^n$ as:
 - $\text{Gen}(1^n)$ outputs $k \in_R \{0, 1\}^n$.
 - $\text{Enc}(k, m)$: Generate $r \in_R \{0, 1\}^n$ and output $c = (r, f_k(r) \oplus m, f_k(m))$.
 - $\text{Dec}(k, c = (r, s, t))$: Compute $m := f_k(r) \oplus s$. If $f_k(m) = t$, output m , else output $\perp$.
- b) Let $\{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be a PRF. Define $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ for $\mathcal{M} = \{0, 1\}^n$ as:
 - $\text{Gen}(1^n)$ outputs $k \in_R \{0, 1\}^n$.
 - $\text{Enc}(k, m)$: Output $c = f_k(1^n) \oplus m$.
 - $\text{Dec}(k, c)$: Compute and output $m := f_k(1^n) \oplus c$.