

MidSem Exam

Full Marks: 30, Time: 2 hours

Instructor: Sruthi Sekar

Date: 17th Sep 2026

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 answers.

Problem 1 (6 marks). Let $F = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be a strong PRP (SPRP). Define a fixed-length encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ for messages of $n/2$ -bits as:

- $\text{Gen}(1^n)$: Pick and output $k \in_R \{0, 1\}^n$.
- $\text{Enc}(k, m)$: Pick $r \in_R \{0, 1\}^{n/2}$. For $m \in \{0, 1\}^{n/2}$, compute and output $c := f_k(r || m)$.

Show how to decrypt the scheme. Are the following statements about Π true? If yes, give a complete formal proof (via reduction); if not, show a complete attack.

- a) Π is secure against a chosen plaintext attack.
- b) Π is an authenticated encryption scheme.

Problem 2 (5 marks (2+3)). Answer with just a yes/no, along with a few intuitive words of explanation (just rewriting the definition won't suffice).

- a) Is Π^{repeat} an authenticated encryption scheme or not? For an authenticated encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, define $\Pi^{\text{repeat}} = (\text{Gen}, \text{Enc}^r, \text{Dec}^r)$ as:

$$\text{Enc}_k^r(m) := (\text{Enc}_k(m), \text{Enc}_k(m)); \text{Dec}_k^r(c_1, c_2) := \begin{cases} \text{Dec}_k(c_1), & \text{if } \text{Dec}_k(c_1) = \text{Dec}_k(c_2) \\ \perp, & \text{otherwise} \end{cases}$$

- b) Is Π^{nested} an authenticated encryption scheme or not? For an authenticated encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, define $\Pi^{\text{nested}} = (\text{Gen}^{\text{ne}}, \text{Enc}^{\text{ne}}, \text{Dec}^{\text{ne}})$ as: Gen^{ne} generates $k_1 \leftarrow \text{Gen}(1^n)$, $k_2 \leftarrow \text{Gen}(1^n)$ independently, and outputs $k = (k_1, k_2)$.

$$\text{Enc}_k^{\text{ne}}(m) := \text{Enc}_{k_2}(\text{Enc}_{k_1}(m)); \text{Dec}_k^{\text{ne}}(c) := \begin{cases} \text{Dec}_{k_1}(\text{Dec}_{k_2}(c)), & \text{if } \text{Dec}_{k_2}(c) \neq \perp \\ \perp, & \text{otherwise} \end{cases}$$

Unfortunately, the adversary Mallory knows k_2 but not k_1 .

Problem 3 (5 marks (2+3)). Let $\mathcal{F} = \{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ be a pseudorandom function. For each part below, give a complete attack for the mentioned security notion. If you are building a PRF for your attack, you only need to intuitively explain why it's secure before using it in your attack (formal proof by reduction is not expected). However, formally describe the complete attack.

- An EU-CMA Attack.** $\text{Gen}(1^n)$ outputs a uniform $k \in_R \{0, 1\}^n$; $\text{Mac}(k, m)$: To authenticate a message $m = m_1 || m_2$ with $|m_1| = |m_2| = n$, output the tag $t := f_k(m_1) || f_k(f_k(m_2))$; Vrfy is the canonical one.
- PRF Attack.** This is a dual PRF $\mathcal{F}^{\text{dual}} = \{f_k^{\text{dual}} : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0, 1\}^n}$ defined as: $f_k^{\text{dual}}(x) := f_k(x) \oplus f_x(k)$.

Problem 4 (2 marks). Recall the Merkle-Damgård transform:

Let (Gen, h) be a fixed-length hash function for inputs of length $2n$ and with output length n . Construct the hash function (Gen, H) , where Gen remains unchanged and H is as follows:
H: on input a key k and a string $x \in \{0, 1\}^*$ of length $|x| < 2^n$, do the following:

- Set $\ell := \left\lceil \frac{|x|}{n} \right\rceil$ (i.e., the number of blocks in x). Pad x with zeroes so its length is a multiple of n . Parse the padded result as the sequence of n -bit blocks $x_1, \dots, x_\ell$. Set $x_{\ell+1} := |x|$, where $|x|$ is encoded as an n -bit string.
- Set $z_0 := 0^n$. (This is also called the *IV*.)
- For $i = 1, \dots, \ell + 1$, compute $z_i := h^k(z_{i-1} || x_i)$ and output $z_{\ell+1}$.

Let (Gen, H) be a collision resistant hash function constructed via the Merkle-Damgård transform. Consider the following MAC for arbitrary-length messages:

- $\text{Gen}_M(1^n)$: $r \leftarrow \text{Gen}(1^n)$, $k \in_R \{0, 1\}^n$. output (k, r) .
- $\text{Mac}_{r,k}(m)$: output $H^r(k || m)$.

Show a complete EU-CMA attack against the above MAC (using canonical verification). Note here that the hash-key r is not hidden from the MAC adversary, only k is hidden!

Problem 5 (2 marks). Recall from the in-class quiz: assuming $(\text{Gen}, \hat{h})$ to be a fixed-length collision resistant hash function with input length $2n - 1$ and output length $n - 1$, the following (Gen, h) (uses the same Gen and takes inputs of length $2n$ -bits) is not collision resistant:

$$h^k(b || x) := \begin{cases} b || \hat{h}^k(x), & \text{if } b = 0 \\ 1^n, & \text{otherwise} \end{cases}$$

But then, is the (Gen, H) obtained using the Merkle-Damgård transform to (Gen, h) collision resistant? If yes, give an intuitive proof, and if no, give a complete formal attack.

Problem 6 (10 marks (2+3+5)). Consider the following “weaker” definition for collision resistance of a keyed hash function $\Pi_h = (\text{Gen}, H)$, where $\text{Gen}(1^n) \rightarrow k$ picks a key k that decides the specific hash function $H^k : \{0, 1\}^* \rightarrow \{0, 1\}^{\ell(n)}$ with arbitrary input length $> \ell(n)$ (has to be compressing). Consider the game $\text{WCollRes}_{\text{Collin}, \Pi_h}(n)$ between a challenger and adversary **Collin**:

1. **Collin**, on input 1^n outputs a query x .
2. **Challenger** generates $k \leftarrow \text{Gen}(1^n)$ and sends $y = H^k(x)$ to **Collin**.
3. **Collin** sends x_0, x_1 . The game outputs 1 if $(x_0 \neq x_1 \text{ and } H^k(x_0) = H^k(x_1))$, and 0, otherwise.

Π_h is said to be **weak collision resistant (WCR)** if $\forall$ PPT adversary **Collin**, $\exists$ negligible negl such that $\forall n, \Pr[\text{WCollRes}_{\text{Collin}, \Pi_h}(n) = 1] \leq \text{negl}(n)$. Answer the following questions:

- a) Prove formally that every deterministic EU-CMA secure MAC is WCR.
- b) Give an example of a WCR hash that is not an EU-CMA secure MAC (prove formally).
- c) Can you generalize the “one-query” WCR definition to a correct (oracle-based) multi-query WCR definition (as was suggested in class) such that both the conditions below hold?
 - i) it is strictly weaker than a collision resistant hash function, and
 - ii) this notion is sufficient to prove the EU-CMA security of the hash-and-MAC scheme, Π^{arb} . (Recall that Π^{arb} uses the key $k = (k_H, k_M)$, for hash key k_H and underlying fixed-input-length MAC key k_M , and signs an arbitrary length message m as: $\text{Mac}^{\text{arb}}(k, m) := \text{Mac}^{\text{fix}}(k_M, H^{k_H}(m))$.)

Give the definition and formally show (i) via an example that satisfies your definition but is not collision resistant. For (ii), just give an intuitive explanation for why this definition is sufficient to prove EU-CMA security of Π^{arb} .

Cheat Sheet

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): A deterministic poly-time algorithm G is a *pseudorandom generator (PRG)* if it is length-expanding: for polynomial ℓ , 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 $\forall 0 \leq i < \ell(n), \forall n$

$$\Pr_{k \in_R \{0,1\}^n} [\text{Eve}(G(k)|_{1,2,\dots,i}) = G(k)|_{i+1}] \leq 1/2 + \text{negl}(n),$$

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

Strong Pseudorandom Permutations (SPRPs): A family of functions $\{f_k : \{0, 1\}^n \rightarrow \{0, 1\}^n\}_{k \in \{0,1\}^n}$ is a *strong pseudorandom permutation (SPRP)* if for every PPT adversary, **Eve**, there exists a negligible function negl such that $\forall n$

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

where Perm_n is the set of permutations or bijections on $\{0, 1\}^n$. Here $\text{Eve}^{f_k(\cdot), f_k^{-1}(\cdot)}$ and $\text{Eve}^{R(\cdot), R^{-1}(\cdot)}$ denote **Eve** getting oracle access to functions f_k, f_k^{-1} and R, R^{-1} , 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 .

- **Perfect Security:** Π is *perfectly secure* if for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $\Pr[C = c] > 0$ (where C is the distribution: sample $m \leftarrow M$, $k \leftarrow \text{Gen}$ and output $c \leftarrow \text{Enc}(k, m)$):

$$\Pr[M = m | C = c] = \Pr[M = m]$$

- **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. Given the oracle, Eve, on input 1^n , outputs a pair of messages m_0, m_1 with $|m_0| = |m_1|$.
2. Challenger picks $b \in_R \{0, 1\}$; sends $c_b \leftarrow \text{Enc}(k, m_b)$ to Eve.
3. Eve continues to have oracle access to $\text{Enc}_k(\cdot)$ and outputs a bit b' .
4. 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 $\forall n, \Pr[\text{PrivK}_{\text{Eve}, \Pi}^{\text{cpa}}(n) = 1] \leq 1/2 + \text{negl}(n)$.

- **Chosen Ciphertext Attack (CCA):** Define the following game $\text{PrivK}_{\text{Mallory}, \Pi}^{\text{cca}}(n)$ between a challenger and the adversary Mallory:

1. Challenger generates $k \leftarrow \text{Gen}(1^n)$ and gives oracle access of $\text{Enc}_k(\cdot)$ and $\text{Dec}_k(\cdot)$ to Mallory. Mallory, on oracle access to $\text{Enc}_k(\cdot)$ and $\text{Dec}_k(\cdot)$, and input 1^n , outputs a pair of messages m_0, m_1 with $|m_0| = |m_1|$.
2. Challenger picks $b \in_R \{0, 1\}$; sends $c_b \leftarrow \text{Enc}(k, m_b)$ to Mallory.
3. Mallory continues to have oracle access to $\text{Enc}_k(\cdot)$ and $\text{Dec}_k(\cdot)$ (not allowed to query $\text{Dec}_k(\cdot)$ on c_b) and outputs a bit b' .
4. Output 1 if $b' = b$, and 0, otherwise.

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

- **Ciphertext Integrity (CI):** Define the following game $\text{EncForge}_{\text{Mallory}, \Pi}^{\text{ci}}(n)$ between a challenger and the adversary Mallory:

1. Challenger generates $k \leftarrow \text{Gen}(1^n)$ and gives oracle access of $\text{Enc}_k(\cdot)$ to Mallory. Let Q be the set of messages queried by Mallory.
2. Mallory outputs a ciphertext c' .
3. Output 1, if $\text{Dec}_k(c') = m' \neq \perp$, and $m' \notin Q$ and 0, otherwise.

Π has *ciphertext integrity* if for all PPT adversaries Mallory, there exists a negligible function negl such that $\forall n, \Pr[\text{EncForge}_{\text{Mallory}, \Pi}^{\text{ci}}(n) = 1] \leq \text{negl}(n)$.

- **Authenticated Encryption (AE):** Π is an authenticated encryption (AE) scheme if it is CCA-secure and has ciphertext integrity.

Message Authentication Codes: A message authentication code $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ with message space $\mathcal{M}$ satisfies correctness. Additionally, recall the following security notions for Π .

- **Chosen Message Attack (EU-CMA):** Define the following game $\text{MacForge}_{\text{Mallory}, \Pi}^{\text{cma}}(n)$ between a challenger and the adversary Mallory:

1. Challenger generates $k \leftarrow \text{Gen}(1^n)$ and gives oracle access of $\text{Mac}_k(\cdot)$ to Mallory. Let $Q := \{m_1, \dots, m_q\}$ be all the queries made by Mallory.
2. Mallory outputs (m, t) .
3. Output 1 if $\text{Vrfy}_k(m, t) = 1$ and $m \notin Q$, and 0, otherwise.

Π is said to be *existentially unforgeable under a chosen message attack*, if for all PPT adversaries Mallory, $\exists$ a negligible negl such that $\forall n, \Pr[\text{MacForge}_{\text{Mallory}, \Pi}^{\text{cma}}(n) = 1] \leq \text{negl}(n)$.

- **Strong Chosen Message Attack (EU-SCMA):** Define the game $\text{MacForge}_{\text{Mallory}, \Pi}^{\text{scma}}(n)$ between a challenger and the adversary Mallory:

1. Challenger generates $k \leftarrow \text{Gen}(1^n)$ and gives oracle access of $\text{Mac}_k(\cdot)$ to Mallory. Let $Q := \{(m_1, t_1), \dots, (m_q, t_q)\}$ be all the query-response pairs.
2. Mallory outputs (m, t) .
3. Output 1 if $\text{Vrfy}_k(m, t) = 1$ and $(m, t) \notin Q$, and 0, otherwise.

Π is said to be *existentially unforgeable under a strong chosen message attack*, if for all PPT adversaries Mallory, $\exists$ a negligible negl such that $\forall n, \Pr[\text{MacForge}_{\text{Mallory}, \Pi}^{\text{scma}}(n) = 1] \leq \text{negl}(n)$.

Collision Resistant Hash Function: A pair of PPT algorithms (Gen, H) with $\text{Gen}(1^n) \rightarrow k$ picks the key k which decides the specific hash function $H^k : \{0, 1\}^* \rightarrow \{0, 1\}^{\ell(n)}$ with arbitrary input length $> \ell(n)$ (has to be compressing). (Gen, H) is said to be *collision resistant* if for all PPT adversary Collin, there exists a negligible negl such that $\forall n$,

$$\Pr_{k \leftarrow \text{Gen}(1^n)} [(x, x') \leftarrow \text{Collin}(k) : (H^k(x) = H^k(x')) \wedge (x \neq x')] \leq \text{negl}(n)$$