

Quiz 1

Full Marks: 20, Time: 1 hour

Instructor: Sruthi Sekar

Date: 19th Aug 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 (4 marks (2+2)). 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) $\mu_1(n) := \nu_1(n) \div \nu_2(n)$, for any negligible functions ν_1 and ν_2 with $\nu_2(n) > 0, \forall n$.
- b) $\mu_2(n) := n^{\log n} \cdot \nu(n)$, for any negligible function ν .

Problem 2 (4 marks). We consider the following definition of perfect secrecy for the encryption of two messages (using the same key). Here we consider distributions over pairs of messages from the message space $\mathcal{M}$ with $|\mathcal{M}| \geq 2$; we let M_1, M_2 be random variables denoting the first and second message, respectively. (these random variables are not assumed to be independent!) We generate a (single) key k , sample a pair of messages (m_1, m_2) according to the given distribution, and then compute ciphertexts $c_1 \leftarrow \text{Enc}_k(m_1)$ and $c_2 \leftarrow \text{Enc}_k(m_2)$; this induces a distribution over pairs of ciphertexts and we let C_1, C_2 be the corresponding random variables. Prove that no encryption scheme can satisfy Definition 1 below.

Definition 1. [Perfect Security for Multiple Encryptions] An encryption scheme ($\text{Gen}, \text{Enc}, \text{Dec}$) is *perfectly secret for two messages* if for all distributions over $\mathcal{M} \times \mathcal{M}$, all $m_1, m_2 \in \mathcal{M}$, and all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\mathbb{P}[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\mathbb{P}[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \mathbb{P}[M_1 = m_1 \wedge M_2 = m_2].$$

Problem 3 (8 marks (4+4)). Are G_1 and G_2 PRGs? If yes, give a complete proof (by reduction along with a complete probability analysis). Else, give a clear distinguishing attack on pseudorandomness or a clear next-bit predictor (explain the attacking algorithm along with an analysis of the winning probability).

- 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/flipping each bit of s .
- b) $G_2(s) := G'(s || 0)$, for any PRG G' .

Problem 4 (4 marks (2+2)). Each part below has a collection of three statements containing two truths and a lie. Can you identify the lie in each part and justify *only the lie* intuitively (complete formal argument not needed, but intuition should say something more than simply re-writing or stating definitions)?

a) Identify the lie amongst the three:

- i) For the computational indistinguishability definition for encryption security of any scheme designed for arbitrary-length messages, it is necessary to assume that the adversary chooses same-length messages m_0 and m_1 .
- ii) Even if $P = NP$, pseudorandom generators will exist.
- iii) For a perfect secure encryption with key space $\mathcal{K}$ and message space $\mathcal{M}$, it is necessary that $|\mathcal{K}| \geq |\mathcal{M}|$.

b) Identify the lie amongst the three:

- i) For encryption security, saying that it is hard for the adversary **Eve** to recover the key k , given the ciphertext c would imply the definitions we saw.
 - ii) Recall we discussed first-bit unpredictability, which says that given all bits except the first bit of $G(s)$ for random seed s , it is hard for any PPT **Eve** to predict the first-bit of $G(s)$. This notion does not imply pseudorandomness.
 - iii) The length-extension method for PRG that we saw in class was: Sequentially keep using the same PRG $G : \{0, 1\}^n \rightarrow \{0, 1\}^{n+1}$ to get $2n$ bits (in each iteration, output the last bit and use the first n -bits as input for G). This method gives an insecure PRG if we extend all the way to get an exponential stretch.
-

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): Recall the definition of pseudorandom generators (PRGs). A deterministic polynomial-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 $\forall n$

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

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 $m \in \mathcal{M}$, $\Pr[\text{Dec}(k, \text{Enc}(k, m)) = m] = 1$. We defined the following two notions for security so far:

- **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 $c \leftarrow \text{Enc}(k, m)$):

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

- **Computational Indistinguishability:** Define the game $\text{PrivK}_{\text{Eve}, \Pi}^{\text{eav}}(n)$ between a challenger and an adversary **Eve** as follows:

1. **Eve**, on input 1^n (this is just security parameter n in unary notation) 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 *computationally indistinguishable against an eavesdropper* if for all PPT adversaries **Eve**, there exists a negligible function negl such that $\forall n$,

$$\Pr[\text{PrivK}_{\text{Eve}, \Pi}^{\text{eav}}(n) = 1] \leq 1/2 + \text{negl}(n)$$