MIT 6.5620/6.875/18.425: Foundations of Cryptography **Due: Sept. 23, 2026**

Problem Set 1

Your name **Your Collaborators**

Total Number of Points: 40.
Instructions: Solutions should be typeset in LaTeX and submitted as PDF by 11:59:59 PM ET on the due date. You can collaborate on the psets in small groups (of up to three), but must write your solutions separately, in your own words. This means not copying from a board nor from your collaborator's computer.

We strongly recommend ***not*** using AI tools to solve your problem sets. You are responsible for understanding everything you submit and you must be able to explain and justify every part of your solution. In particular, the oral problem set review (10% of the course grade) will evaluate your understanding of the solutions you submit. In all cases, you must list your collaborators, human or machine.

Problem 1. Negligible or not? (8 points) For each of the following functions below, either prove or disprove that it is negligible.

(a) (2 points) $\mu(n) := 1.01^{-n}$. (**Note**: Here, and throughout the course, all logarithms are in base 2 unless otherwise specified.)

(b) (2 points) $\mu(n) := e^{-(\log n)^3} + e^{-(\log n)^2} + e^{-\log n}$.

(c) (4 points) $\mu(n) := \mu'(n) \cdot p(n)$, for some negligible function $\mu'(n)$ and some polynomial function $p(n)$. Is such a $\mu(n)$ always negligible?

Problem 2. PRG or not? (12 points) Let $G : \{0,1\}^{2n} \to \{0,1\}^{3n}$ be a pseudorandom generator (PRG). For each part below, either prove or disprove that the specified function G' is *necessarily* a PRG no matter which PRG G is used.

(a) (3 points)

$$G'(x) := G(\pi(x))$$

where $\pi : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is any $\mathsf{poly}(n)$-time computable bijective function. (You may not assume that π^{-1} is $\mathsf{poly}(n)$-time computable.)

(b) (3 points)

$$G'(x||y) := G(x||x \oplus y)$$

where $x, y \in \{0,1\}^n$. (**Note**: Here, and throughout the course, $x||y$ refers to the concatenation of two strings x and y.)

(c) (3 points)

$$G'(s) := G(s)_{1,\ldots,2n+1}$$

That is, the first $2n+1$ bits of $G(s)$, so $G' : \{0,1\}^{2n} \to \{0,1\}^{2n+1}$.

(d) (3 points) Let $F : \{0,1\}^{2n} \to \{0,1\}^{3n}$ be another PRG, and define

$$G'(s) := G(s)||F(s)\ .$$

Problem 3. Mixing PRGs. (6 points)

The cryptography community is debating between two different PRG candidates, G_1 and G_2. Everyone agrees that at least one of them is secure, but they disagree on which it is. Can you make everyone happy by constructing a PRG out of G_1 and G_2 that is guaranteed to be secure assuming only that *at least* one of G_1 or G_2 is a PRG?

Explicitly, you may assume that the candidates G_1 and G_2 are polynomial-time computable functions expanding by one bit, and your goal is to come up with a PRG from G_1 and G_2 that has any non-trivial stretch (even one bit is fine).

Problem 4. Hiding Promises. (14 points) We define a cryptographic protocol called a *promise hiding* scheme between two parties, Alice and Bob. Alice wants to promise something to Bob (for now, let's say one bit $\sigma \in \{0,1\}$), but Alice wants this promise to be hidden from Bob until Alice decides the time is right to reveal σ.

(a) (2 points) Suppose Alice samples $r \leftarrow \{0,1\}$ and sends the message $A(\sigma; r) := \sigma \oplus r$ to Bob to promise $\sigma \in \{0,1\}$. Later, when Alice decides the time is right, to reveal σ, Alice sends (σ, r) to Bob, and Bob can compute $A(\sigma; r)$ to verify that it is consistent with the message he received from Alice. We would like two properties to hold:

- **(Statistically) Hiding**: The distributions $A(0; r)$ and $A(1; r)$ are identical for random r.
- **(Statistically) Promising**: There does not exist $r_0, r_1 \in \{0,1\}$ such that $A(0; r_0) = A(1; r_1)$.

Prove or disprove that this scheme is hiding, and prove or disprove that this scheme is promising.

(b) (4 points) Let G be any length-tripling PRG. Suppose Alice samples $r \leftarrow \{0,1\}^n$ and sends the message

$$A(\sigma; r) = \begin{cases} G(r) & \text{if } \sigma = 0, \\ G(r) \oplus 1^{3n} & \text{if } \sigma = 1. \end{cases}$$

We would like similar properties to hold:

- **(Computationally) Hiding**: The distributions $A(0; r)$ and $A(1; r)$ are computationally indistinguishable for random r.
- **(Statistically) Promising**: There does not exist $r_0, r_1 \in \{0,1\}^n$ such that $A(0; r_0) = A(1; r_1)$.

Prove or disprove that this scheme is hiding, and prove or disprove that this scheme is necessarily promising.

(c) (2 points) Let G be any length-tripling function. Show that

$$\Pr_{b \leftarrow \{0,1\}^{3n}}[\exists r_0, r_1 \in \{0,1\}^n : b = G(r_0) \oplus G(r_1)] \leq \frac{1}{2^n}.$$

(d) (6 points) Let's change things up a bit. Assume the existence of a length-tripling PRG G. Now, suppose that Bob is allowed to send a uniformly random string $b \leftarrow \{0,1\}^{3n}$ before Alice sends her message. Then, Alice's message can be described as a function

$A(b, \sigma; r)$, so that it can depend on b as well. Consider the following promise hiding scheme for Alice and Bob:

$$A(b, \sigma; r) = \begin{cases} G(r) & \text{if } \sigma = 0, \\ G(r) \oplus b & \text{if } \sigma = 1. \end{cases}$$

Prove that it satisfies the two properties below:

- **(Computationally) Hiding**:[1] For all $b \in \{0,1\}^{3n}$, the distributions $A(b, 0; r)$ and $A(b, 1; r)$ are computationally indistinguishable for random r.
  Prove this via a hybrid argument and make sure to clearly define your hybrids and prove formally that any two adjacent hybrids are computationally indistinguishable.
- **(Statistically) Promising**:

$$\Pr_{b \leftarrow \{0,1\}^{3n}} [\exists r_0, r_1 \in \{0,1\}^n : A(b, 0; r_0) = A(b, 1; r_1)] \leq \mathsf{negl}(n).$$

[1] For this part, we allow the distinguishers to be non-uniform: they may have a polynomial-size advice string depending only on the input length. In particular, a fixed string $b = b_n$ may be hardwired into the (PRG) distinguisher.