**COMS BC3262** February 2, 2026

# Problem Set 2

*Instructor: Eysa Lee* *Due: February 19, 2026*

**Guidelines.** Solutions will be graded for correctness and clarity. If you do not know how to solve a problem, you may write **"I don't know how to do this"** to receive 20% credit for any problem not marked as extra credit. In your proofs, justify every step and, if needed, write down definitions/theorems that were presented in class and that you rely on. When refuting a claim, provide a counterexample and show that it does not satisfy the required definition.

**Collaboration.** You are allowed to discuss problems with other students in the class. However, you should write up your solutions on your own and may not read or copy the solutions of others. You should try solving each problem on your own before discussing with others. **If you work with others on a problem, you must note with whom you discussed the problem at the beginning of your solution write-up.** For example, "I discussed Problem 1 with Alice and Bob and Problem 2 with Carol." You may not use external resources apart from the textbooks.

**Generative AI Policy.** The use of generative AI for anything related to assignments is prohibited in this class. **It is always prohibited to input any substantial portion of any assignment into any AI resource.** It is also always forbidden to incorporate any substantive portion of an AI resource's output into your answers, even if you paraphrase it or rewrite it in your own words.

## Problem 1 (PRG or Not?) 15 points + 5 Extra Credit

Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Each sub-problem is worth 5 points, and for each of these sub-problems you must determine whether the proposed constructions of $G'$ are *necessarily* PRGs or not. If yes, give a proof that $G'$ *must* be a PRG. Otherwise, give a counterexample. For a counterexample, you should show that if PRGs exist there is some function $G$ which is a PRG but $G'$ is not[1].

1. $G'(s) = G(s||0)$
2. $G'(s) = G(s \oplus 1^n)$
3. $G'(s) = G(s)||G(s \oplus (0^{n-1}||1))$

   (i.e., $G$ is run twice, with the second one flipping the last bit of $s$. These two outputs are appended to each other.)
4. $G'(s) = G(s) \oplus (0^n||s)$

[1] In some counterexamples it may be possible to write a distinguisher that works for *any* PRG $G$, but in others, you may need to write a distinguisher that works only for some *specific* $G$. In the latter example, provide a description of the specific $G$ and a proof that it is a PRG. If necessary, you can also assume there exists some other PRG $G''$ and use $G''$ to construct the specific $G$ you require to disprove $G'$.

## Problem 2 (EAV-Secure but not CPA-Secure) 10 pts

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Consider the following private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:

- $\mathsf{Gen}(1^n)$: Output $k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k, m)$: On input $m \in \{0,1\}^n$, output $c = m \oplus F_k(0)$
- $\mathsf{Dec}(k, c)$: On input $c \in \{0,1\}^n$, output $m = c \oplus F_k(0)$

Prove the following two statements about $\Pi$:

1. $\Pi$ has indistinguishable encryptions in the presence of an eavesdropper.
2. $\Pi$ is not CPA-secure.

## Problem 3 (EAV-Security?) 5 pts

Consider the following encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with key space $\mathcal{K} = \{0,1\}^n$ and message/ciphertext space $\mathcal{M} = \mathcal{C} = \{0,1\}^{2n}$:

- $\mathsf{Gen}(1^n)$: Output $k \leftarrow \{0,1\}^n$.
- $\mathsf{Enc}(k, m)$: Split the message $m \in \{0,1\}^{2n}$ into a "left half" $m_0 \in \{0,1\}^n$ and a "right half" $m_1 \in \{0,1\}^n$ so that $m = m_0||m_1$ where $||$ denotes string concatenation. Compute $c_0 = k \oplus m_0$, $c_1 = k \oplus m_1$, and output $c = c_0||c_1$.
- $\mathsf{Dec}(k, c)$: Parse the ciphertext as $c = c_0||c_1$, and output $m = (c_0 \oplus k)||(c_1 \oplus k)$.

Show that $\Pi$ is *not* EAV-secure.

## Problem 4 (PRF or Not?) 10 pts

Let $F$ be a PRF family with $n$-bit key, $n$-bit input and $n$-bit output.

1. Show that $F'_k(x) = F_k(x)||F_k(x \oplus 1^n)$ can never be a secure PRF.
2. Show that $F'_k(x) = F_k(x) \oplus x$ is always a secure a PRF.