COMS BC3262 February 15, 2026

Problem Set 3

Instructor: Eysa Lee *Due: March 5, 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 from class or the textbook 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 (CBC Counter?) 5 pts

Recall CBC-mode encryption from Lecture 6. Consider a variant of CBC where, after the first encryption with a randomly sampled initialization vector (IV), subsequent encryptions simply increment the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is *not* CPA-secure.

Problem 2 (CPA-Secure Encryption from PRPs) 10 pts

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom permutation (PRP) and define an encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ for messages of length $n/2$ as follows.

- $\mathsf{Gen}(1^n)$: Output key $k \leftarrow \{0,1\}^n$.
- $\mathsf{Enc}(k, m)$: Sample $r \leftarrow \{0,1\}^{n/2}$ and output $c = F_k(r||m)$, where $||$ denotes string concatenation.
- $\mathsf{Dec}(...)$: ...

Part A. (2 pts) Complete the definition of Π by showing how to decrypt and briefly show correctness.

Part B. (8 pts) Prove that Π is CPA-secure.

Problem 3 (PRGs are OWFs) 5 pts

Let G be any candidate pseudorandom generator (PRG) with n-bit stretch (i.e., when $|s| = n$, $|G(s)| = 2n$). Show that G is also a one-way function (OWF).

Hint: Show this via a reduction. If some adversary managed to break the security of G as a OWF, use that adversary to also break the security of G as a PRG.

Problem 4 (OWF or Not?) 5 pts + 5 Extra Credit

Assume that $f : \{0,1\}^* \to \{0,1\}^*$ is a one-way function (OWF). For each of the following candidate constructions f' argue whether it is also *necessarily* a OWF or not. If yes, give a proof (via a reduction showing how to convert an attack against f' into one against f). If no, give a counter-example. For a counterexample, you should show that if OWFs exist then there is some function f which is one-way but f' is not.

1. $f'(x) = f(x)||x_1$ where x_1 is the first bit of x and $||$ denotes string concatenation.
2. $f'(x) = f(x)||0$.