Introduction to Cryptography

Example Final Exam Fall 2026

Name _____

Instructions

- You have 110 minutes.
- This is a closed-book exam.
- You may use results from class as long as you state them properly.
- Write each answer in the box below its question. Your answer can be shorter than the space provided.
- There is an extra emergency answer box on the last page. If you use it, write the question number above the box.

Question 1

Let $G\colon \{0,1\}^n \to \{0,1\}^{n+1}$ be a pseudorandom generator. Consider the function $f\colon \{0,1\}^n \to \{0,1\}^n$ defined by $f(x) = G_{[n]}(x)$, where $G_{[n]}(x)$ denotes the first n output bits of $G(x)$.

Prove or disprove: f is a one-way function.

Question 2

Let $\{F_k\}_{k\in\{0,1\}^n}$ be a family of pseudorandom functions $F_k\colon \{0,1\}^n \to \{0,1\}^{n\times 2n}$, where each output is interpreted as an $n \times 2n$ binary matrix. Consider the family $F'_{A,k}\colon \{0,1\}^{2n} \to \{0,1\}^{n\times 2n}$ indexed by $(A,k) \in \{0,1\}^{n\times 2n} \times \{0,1\}^n$, with

$$F'_{A,k}(x) = \begin{cases} A & \text{if } x = 0^{2n}, \\ F_k(Ax) & \text{if } x \neq 0^{2n}, \end{cases}$$

where Ax denotes matrix–vector multiplication modulo 2.

Prove or disprove that $\{F'_{A,k}\}$ is a pseudorandom function family.

Question 3

Two-fold 3COL. Let $G = (V, E)$ be a graph. Consider two independent copies of the GMW protocol run in parallel. The honest prover is given a proper 3-coloring of G. In each copy, the prover chooses an independent uniform permutation of the three colors and commits to the resulting color of every vertex using perfectly binding, computationally hiding commitments. After receiving both sets of commitments, the verifier chooses one uniform edge for each copy, independently. The prover opens the commitments for the endpoints of each chosen edge in its corresponding copy. The verifier accepts if all openings are valid and each edge has two distinct colors.

Show that the soundness error is at most $(1 - 1/|E|)^2$. Describe a zero-knowledge simulator for the two-fold protocol. There is no need to prove that the simulator is valid or analyze its running time.

Emergency Answer Box

Question number _____