Cryptography
Purdue University
Instructor: Hanshen Xiao

October 10, 2025
CS55500 Fall 2025
Solution: Midterm Practice Exam

Solution: Midterm Practice Exam

- Do not open this quiz booklet until directed to do so. Read all the instructions on this page.
- When the quiz begins, write your name on the top of every page of this quiz booklet.
- You have 80 minutes to earn a maximum of 80 points. Do not spend too much time on any one problem. Skim them all first, and attack them in the order that allows you to make the most progress.
- **You are allowed three double-sided letter-sized sheet with your own notes**. No calculators, cell phones, or other programmable or communication devices are permitted.
- Write your solutions in the space provided. Pages will be scanned and separated for grading. If you need more space, write “Continued on S1” (or S2, S3) and continue your solution on the referenced scratch page at the end of the exam.
- Do not waste time and paper rederiving facts that we have studied in lecture, recitation, or problem sets. Simply cite them.
- **Pay close attention to the instructions for each problem**. Depending on the problem, partial credit may be awarded for incomplete answers.

Problem	Parts	Points
0: Information	2	2
1: True or False?	8	32
2: PKE and OWFs	1	16
3: Homomorphic OWFs	1	18
4: SIS Please	1	12
Total		80

Name: ______________________________

School Email: ______________________________

Problem 1. True or False? (8 parts)

For each of the following questions, circle either **T** (True) or **F** (False). Each problem is worth 4 points. **You will get 4 points for a correct answer, 0 points for an incorrect answer, and 2 points if you leave it blank.** No justification is necessary, and no partial credit will be given.

(a) $\boxed{\textbf{T}}$ $\boxed{\textbf{F}}$ If the Diffie-Hellman key-exchange protocol is secure, then the discrete log assumption is true.

Solution: **True**. An adversary that breaks the discrete log assumption would immediately allow an adversary to break the security of the Diffie-Hellman key exchange protocol, as the adversary could non-negligibly find a given g^a, which allows the adversary to compute $(g^b)^a = g^{ab}$.

(b) $\boxed{\textbf{T}}$ $\boxed{\textbf{F}}$ It is known that one-way functions exist if and only if collision-resistant hash functions exist.

Solution: **False**. The existence of a collision-resistant hash function from the existence of one-way functions is an open question.

(c) $\boxed{\textbf{T}}$ $\boxed{\textbf{F}}$ For every one-way function $f : \{0,1\}^n \to \{0,1\}^n$, $g(x) = f(f(x))$ is also a one-way function.

Solution: **False**. Shown in hw2, problem 3(a).

(d) $\boxed{\textbf{T}}$ $\boxed{\textbf{F}}$ If $\mathbf{P} = \mathbf{NP}$, then one-way functions exist.

Solution: **False**. If one-way functions exist, then length-doubling PRGs exist. If $\mathbf{P} = \mathbf{NP}$, then there is a simple polynomial time algorithm that breaks security of any PRG G. Let $L = \{(1^n, y) : \exists x \in \{0,1\}^n \text{ such that } G(x) = y\}$. Clearly, $L \in \mathbf{NP}$, so $L \in \mathbf{P}$ if $\mathbf{NP} = \mathbf{P}$. Moreover, a polynomial time algorithm for L gives a distinguisher for G, contradicting the assumption that G is a PRG.

(e) $\boxed{\textbf{T}}$ $\boxed{\textbf{F}}$ Every pseudorandom generator (PRG) must be injective.

Solution: **False**. Take any PRG G, and modify it on 0^n so that $G(0^n) = G(1^n)$. This will still be a PRG since only a 2^{-n} fraction of inputs are changed, but it is clearly not injective.

(f) $\boxed{\textbf{T}}$ $\boxed{\textbf{F}}$ If pseudorandom generators (PRGs) exist, then pseudorandom functions (PRFs) exist.

Solution: **True**. This follows directly from the GGM tree-based construction.

(g) $\boxed{\textbf{T}}$ $\boxed{\textbf{F}}$ Let $G_1, G_2 : \{0,1\}^n \to \{0,1\}^{n+1}$ be arbitrary pseudorandom generators (PRGs). The function $G : \{0,1\}^n \to \{0,1\}^{n+1}$ given by $G(x) := G_1(x) \oplus G_2(x)$ is a pseudorandom generator.

Solution: **False**. If G_1 and G_2 are the same PRG, then G is the all 0s function.

(h) $\boxed{\textbf{T}}$ $\boxed{\textbf{F}}$ If $(\mathsf{Gen}, \mathsf{MAC}, \mathsf{Ver})$ is a message authentication code (MAC) scheme for messages of length n, then $\mathsf{MAC}'_k(m_1||m_2) := \mathsf{MAC}_k(m_1)||\mathsf{MAC}_k(m_2)$ is a MAC scheme for messages of length $2n$. ($\mathsf{Gen}' = \mathsf{Gen}$ but Ver' is now $\mathsf{Ver}'_k(m_1||m_2, \sigma_1||\sigma_2) = \mathsf{Ver}_k(m_1, \sigma_1) \wedge \mathsf{Ver}_k(m_2, \sigma_2)$.)

Solution: **False**. A mix-and-match attack breaks this. By feeding in $0^n||0^n$ and $1^n||1^n$ into the MAC' oracle, the adversary can directly generate a valid tag for $0^n||1^n$ and $1^n||0^n$, breaking EUF-CMA security.

Problem 2. [16 points] **Public-key Encryption and One-way Functions**

Show that public-key encryption (with perfect correctness) implies the existence of one-way functions.

Hint: Think about the key generation algorithm.

Solution: Consider the function $f(r)$ that computes $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^n; r)$ and outputs pk.

Claim: f is a OWF. Clearly f is deterministic and efficiently computable, so it suffices to show that it is hard to find pre-images. Suppose for contradiction that an adversary A inverts f non-negligibly often. Then, we can use A to break IND-CPA security. Specifically, run A on pk to get r such that $f(r)$ outputs $(\mathsf{pk}, \mathsf{sk}')$ for some sk' (non-negligibly often). Then, using sk', an adversary can distinguish between $\mathsf{ct} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_0)$ and $\mathsf{ct} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m_1)$ for any distinct m_0 and m_1 by running $\mathsf{Dec}_{\mathsf{sk}'}(\mathsf{ct})$. Assuming A succeeds in finding r such that $f(r) = (\mathsf{pk}, \mathsf{sk}')$ for some sk', then by *perfect* correctness, we know that sk' must always be a valid secret key. Therefore, this attack breaks IND-CPA security.

Problem 3. [18 points] **Homomorphic One-Way Functions?**

Let $f : \{0,1\}^n \to \{0,1\}^n$ be a function with the property that

$$\forall x, y \in \{0,1\}^n : f(x \oplus y) = f(x) \oplus f(y) \ .$$

Show that f cannot be a one-way function.

Solution: If this property holds for f, then f is a linear map over the vector space $\mathbb{F}_2^n$. (This is true because scalar multiplication here just considers the scalars 0 and 1.)

Therefore, $f(x) = Ax \pmod 2$ for some matrix $A \in \mathbb{F}_2^{n \times n}$. Computing the n values

$$f(1||0^{n-1}), f(0||1||0^{n-2}), \cdots, f(0^{n-1}||1),$$

immediately gives the columns of A. This gives the following p.p.t. adversary: given $y = Ax$, compute A using f, and use Gaussian elimination to find some x such $Ax = y$. Output x.

Problem 4. [32 points] **SIS Please** (2 parts)

A commonly used cryptographic assumption (that we have not seen in class) is called the *short integer solution* (SIS) assumption. A version of it can be stated as follows:

Definition 1 (SIS Assumption). *For all n, $m = 100n \log n$ and $q = n^2$, given a uniformly random $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, it is hard to output some non-zero vector $\mathbf{x} \in \{-1, 0, 1\}^m$ such that $\mathbf{Ax} = 0^n \in \mathbb{Z}_q^n$. More precisely, for all p.p.t. algorithms B, there exists a negligible function $\mu(n)$ such that*

$$\Pr[\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}; \mathbf{x} \leftarrow B(\mathbf{A}) : \mathbf{x} \in \{-1, 0, 1\}^m \setminus \{0^m\} \textit{ and } \mathbf{Ax} = \mathbf{0}] \leq \mu(n).$$

Assuming the SIS assumption, show that the function family $\mathcal{H} = \{H_{\mathbf{A}} : \{0, 1\}^m \rightarrow \mathbb{Z}_q^n\}$ given by $H_{\mathbf{A}}(\mathbf{x}) := \mathbf{Ax} \bmod q$ is a collision resistant hash function family.

Solution: Suppose for contradiction that $\mathcal{H}$ is not a collision resistant hash function. Then, there is a p.p.t. adversary M such that $(\mathbf{x}_0, \mathbf{x}_1) \leftarrow M(\mathbf{A})$, which satisfies $H_{\mathbf{A}}(\mathbf{x}_0) = H_{\mathbf{A}}(\mathbf{x}_1)$, and $\mathbf{x}_0 \neq \mathbf{x}_1$ non-negligibly often. By linearity, this implies $\mathbf{A}(\mathbf{x}_0 - \mathbf{x}_1) = 0^n$. Therefore, $\mathbf{x} = \mathbf{x}_0 - \mathbf{x}_1$ satisfies $\mathbf{Ax} = 0^n$. Moreover, since $\mathbf{x}_0 \neq \mathbf{x}_1 \in \{0, 1\}^m$, it follows that $\mathbf{x} \in \{-1, 0, 1\}^m$ and $\mathbf{x} \neq 0^m$. This attack (namely subtracting the two outputs of M) breaks the SIS assumption, as desired.

SCRATCH PAPER 1. DO NOT REMOVE FROM THE EXAM.

You can use this paper to write a longer solution if you run out of space, but be sure to write “Continued on S1” on the problem statement’s page.

SCRATCH PAPER 2. DO NOT REMOVE FROM THE EXAM.

You can use this paper to write a longer solution if you run out of space, but be sure to write “Continued on S2” on the problem statement’s page.

SCRATCH PAPER 3. DO NOT REMOVE FROM THE EXAM.

You can use this paper to write a longer solution if you run out of space, but be sure to write "Continued on S3" on the problem statement's page.