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) **T** **F** If the Diffie-Hellman key-exchange protocol is secure, then the discrete log assumption is true.

(b) **T** **F** It is known that one-way functions exist if and only if collision-resistant hash functions exist.

(c) **T** **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.

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

(e) **T** **F** Every pseudorandom generator (PRG) must be injective.

(f) **T** **F** If pseudorandom generators (PRGs) exist, then pseudorandom functions (PRFs) exist.

(g) **T** **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.

(h) **T** **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 $\mathsf{Ver}'_k(m_1||m_2, \sigma_1||\sigma_2) = \mathsf{Ver}_k(m_1, \sigma_1) \wedge \mathsf{Ver}_k(m_2, \sigma_2)$.)

y

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.

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.

Problem 4. [12 points] **SIS Please**

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*

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

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

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.