Student Name: _____
Student Number: _____
School: _____
Year of Entrance: _____

ShanghaiTech University Final Examination Cover Sheet

Academic Year: 2021 to 2022 Term: 2
Teaching School: School of Information Science and Technology
Instructor: Zhang Liangfeng
Course Name: Applied Cryptography
Course Number: CS152

Exam Instructions for Students:

1. All examination rules must be strictly observed during the entire exam, and any form of cheating is prohibited.

2. Other than allowable materials, students taking closed-book tests must place their books, notes, tablets and any other electronic devices in places designated by the examiners.

3.Students taking open-book tests may use allowable materials authorized by the examiners. They must complete the exam independently without discussion with each other or exchange of materials.

For Marker's Use:

Section	**1**	**2**	**3**	**4**	**5**	**Total**
Marks						
Recheck						

Marker's Signature: **Reviewer's Signature:**
Date: **Date:**

Instructions for Examiners:

1. The format of the exam papers and answer sheets shall be determined by the school and examiners according to actual needs. All pages should be marked by the page numbers in order (except the cover page). All text should be legible, visually comfortable and easy to bind on the left side. A4 double-sided printing is recommended for the convenience of archiving (There are all-in-one printers in the university).

2. The examiners should make sure that exam questions are accurate and appropriate. If students have any enquiries about the exam questions during the exam, the examiners should be responsible to respond on site, which will be taking into account in the teaching evaluation.

1. In a cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ if an encryption function $e_K \in \mathcal{E}$ is identical to the decryption function $d_K \in \mathcal{D}$, then the key K is said to be an **involutory** key.

   (a) (**5 points**) Suppose that $K = (a, b)$ is a key in an Affine Cipher over $\mathbb{Z}_n$. Prove that K is an involutory key if and only if $a^{-1} \bmod n = a$ and $b(a+1) \equiv 0 \pmod{n}$.

   (b) (**10 points**) Determine all the involutory keys in the Affine Cipher over $\mathbb{Z}_9$.

   (c) (**5 points**) Suppose that $n = p^2$, where p is an odd prime. Determine the number of involutory keys in the Affine Cipher over $\mathbb{Z}_n$. Prove your answers.

2. Let $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ be a cryptosystem with $\mathcal{P} = \mathcal{C} = \mathbb{Z}_5$ and $\mathcal{K} = \{0, 1, 2, 3, 4, 5\}$. For any $K \in \mathcal{K}, x \in \mathcal{P}, y \in \mathcal{C}$, the encryption rule e_K and the decryption rule d_K are defined as follows:

$$e_K(x) = x + K \bmod 5;\ d_K(y) = y - K \bmod 5.$$

   (a) (**10 points**) Suppose that $\Pr[\mathbf{x} = x] = \frac{1}{5}$ for any $x \in \mathcal{P}$ and $\Pr[\mathbf{K} = K] = \frac{1}{6}$ for any $K \in \mathcal{K}$. Determine if this cryptosystem has perfect secrecy.

   (b) (**5 points**) Suppose that $\Pr[\mathbf{x} = x] = \frac{1}{5}$ for any $x \in \mathcal{P}$. Determine if there is a probability distribution $\mathbf{K}$ of the secret key such that the cryptosystem has perfect secrecy.

3. For any $a, b \in \mathbb{Z}_p$, define a function $f_{(a,b)} : \mathbb{Z}_p \to \mathbb{Z}_p$ by the rule

$$f_{(a,b)}(x) = x^2 + ab \bmod p.$$

   (a) (**15 points**) Compute the authentication matrix of the hash family $(\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Z}_p \times \mathbb{Z}_p, \{f_{(a,b)} : a, b \in \mathbb{Z}_p\})$ for $p = 3$. Based on the authentication matrix, determine the deception probabilities Pd_0 and Pd_1 of this specific hash family.

   (b) (**5 points**) Determine the deception probabilities Pd_0 and Pd_1 of $(\mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Z}_p \times \mathbb{Z}_p, \{f_{(a,b)} : a, b \in \mathbb{Z}_p\})$ for any odd prime p. Prove your answers.

4. Consider a public key cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where

$$\mathcal{K} = \{(\lambda, p, q, n, g, h) : \lambda > 2,\ p \text{ and } q \text{ are } \lambda\text{-bit primes}, p \neq q, n = p^2 q, g \in \mathbb{Z}_n^* \text{ is an}$$

$$\text{element such that } g_p = g^{p-1} \bmod p^2 \text{ has order } p \text{ in } \mathbb{Z}_{p^2}^*, h = g^n \bmod n\}.$$

   For any $K = (\lambda, p, q, n, g, h) \in \mathcal{K}$, (λ, n, g, h) form a **public key** that will be used to encrypt the plaintexts, and (p, q) form a **private key** that will be used to decrypt the ciphertexts.

   To **encrypt** any plaintext x with (λ, n, g, h), where $0 < x < 2^{\lambda-1}$, we choose an integer $r \in \mathbb{Z}_n$ uniformly and at random, and then compute the ciphertext as

$$y = g^x h^r \bmod n. \tag{1}$$

   To **decrypt** y with (p, q), we compute $y_p = y^{p-1} \bmod p^2, g_p = g^{p-1} \bmod p^2$ and finally output

$$x' = \frac{L(y_p)}{L(g_p)} \bmod p, \tag{2}$$

   where $L(t) = \frac{t-1}{p} \bmod p$ is a function from $\mathcal{T} = \{t \in \mathbb{Z}_{p^2}^* : t \equiv 1 (\bmod\ p)\}$ to $\mathbb{Z}_p$.

(a) (**5 points**) Show that $\mathcal{T} = \{1 + sp : s = 0, 1, \ldots, p-1\}$.

(b) (**5 points**) Show that $\mathcal{T}$ is a subgroup of $\mathbb{Z}^*_{p^2}$.

(c) (**5 points**) Show that if $t \in \mathbb{Z}^*_{p^2}$ has order p, then $t \in \mathcal{T}$.

(d) (**5 points**) Show that $L(t_1 t_2) = L(t_1) + L(t_2) \bmod p$ for any $t_1, t_2 \in \mathcal{T}$.

(e) (**5 points**) Suppose that $t \in \mathcal{T}$, $L(t) \not\equiv 0 (\text{mod } p)$ and $t' = t^x \bmod p^2$ for some $x \in \mathbb{Z}_p$. Show that

$$x = \frac{L(t')}{L(t)} \bmod p.$$

(f) (**5 points**) Note that (c) shows that $g_p \in \mathcal{T}$. Based on this fact, show that the x' in (2) is equal to the x in (1), i.e., the cryptosystem is correct.

5. (**15 points**) Show that if the same value k is used to sign two different messages in the **ElGamal Signature Scheme**, then an adversary can determine the secret key without solving the discrete logarithm problem.