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

ShanghaiTech University Final Examination Cover Sheet

Academic Year : 2022 to 2023 Term: 1
Teaching School: School of Information Science and Technology
Instructor: Zhang Liangfeng
Course Name: Cryptography
Course Number: CS252

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. (**20 points**) Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a private-key encryption scheme with message space $\mathcal{M} = \{0, 1, 2, 3\}$ and key space $\mathcal{K} = \{1, 2, 3, 4\}$. The algorithms of Π are defined as follows:

   - Gen : choose a secret key $k \leftarrow \mathcal{K}$ uniformly from $\mathcal{K}$.
   - $\mathsf{Enc}(k, m)$: given $k \in \mathcal{K}$ and $m \in \mathcal{M}$, output $c = k \cdot m \bmod 5$.
   - $\mathsf{Dec}(k, c)$: given $k \in \mathcal{K}$ and $c \in \mathcal{C}$, output $m = c \cdot k^{-1} \bmod 5$.

   Determine whether Π is perfectly secret. Show your answers.

2. (**20 points**) Let $h : \{0,1\}^{2n} \to \{0,1\}^n$ be a collision-resistant hash function. Let $H : \{0,1\}^{8n} \to \{0,1\}^n$ be a hash function that computes the hash value of any message $x \in \{0,1\}^{8n}$ as follows:

   - write x as $x = x_1 \| x_2 \| x_3 \| x_4$, where $|x_1| = |x_2| = |x_3| = |x_4| = 2n$ and $\|$ means concatenation.
   - output $H(x) = h(h(h(x_1)\|h(x_2))\|h(h(x_3)\|h(x_4)))$.

   Determine whether H is a collision resistant hash function. Show your answers.

3. (**20 points**) Let $G = \mathbb{Z}_{23}^*$ be a cyclic group of order $q = 22$. Let $g = 5$ be a generator of G. Let $pk = (q, G, g, h) = (22, \mathbb{Z}_{23}^*, 5, 17)$ be the public key of ElGamal encryption. Let $c_1 = (22, 12)$ and $c_2 = (10, 13)$ be ciphertexts of $m_1 \in G$ and $m_2 \in G$, respectively. Find a ciphertext for $m_1 \cdot m_2 \in G$.

4. (**20 points**) Let $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ be a fixed-length MAC for messages of n bits:

   - $\mathsf{Gen}(1^n)$: choose a binary $n \times n$ matrix $A \leftarrow \{0,1\}^{n \times n}$ and a binary column vector $b \leftarrow \{0,1\}^n$ uniformly. Output $k = (A, b)$ as the secret key.
   - $\mathsf{Mac}(k, x)$: To authenticate a message $x \in \{0,1\}^n$, compute and output the tag

     $$t = (Ax + b) \bmod 2,$$

     where the "mod 2" is done for every entry of $Ax + b$.
   - $\mathsf{Vrfy}(k, x, t)$: Given $k = (A, b)$ and $x, t \in \{0,1\}^n$, output 1 if and only if $t = (Ax + b) \bmod 2$.

   Determine whether Π is EUF-CMA secure. Show your answers.

5. (**20 points**) Let F be a length-preserving PRF. Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a private-key encryption scheme with message space $\mathcal{M} = \{0,1\}^n$, key space $\mathcal{K} = \{0,1\}^n \times \{0,1\}^n$ and ciphertext space $\mathcal{C} = \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n$:

   - $\mathsf{Gen}(1^n)$: choose a secret key $k = (k_1, k_2) \leftarrow \mathcal{K}$ uniformly from $\mathcal{K}$.
   - $\mathsf{Enc}(k, m)$: given $k = (k_1, k_2) \in \mathcal{K}$ and $m \in \mathcal{M}$, if $m = k_1$, output $c = (0^n, m, k_1)$; otherwise, choose $r \in \{0,1\}^n \setminus \{0^n\}$ uniformly, output $c = (r, F_{k_2}(r) \oplus m, k_1)$.
   - $\mathsf{Dec}(k, c)$: given $k = (k_1, k_2) \in \mathcal{K}$ and $c = (c_1, c_2, c_3)$, if $c_1 = 0^n$, output $m = c_2$; otherwise, output $m = F_{k_2}(c_1) \oplus c_2$.

   Determine whether Π is IND-m-EAV secure. Show your answers.