

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:
Date:

Reviewer's Signature:
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 $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a private-key encryption scheme with message space $\mathcal{M} = \{m = m_1m_2m_3 \in \{0,1\}^3 : m_1 \oplus m_2 \oplus m_3 = 1\}$ and key space $\mathcal{K} = \{k = k_1k_2k_3 \in \{0,1\}^3 : k_1 \oplus k_2 \oplus k_3 = 0\}$. The algorithms of Π are defined as follows:

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

Determine whether Π is perfectly secret. Show your answers.

2. **(20 points)** Let $h : \{0,1\}^4 \rightarrow \{0,1\}^3$ be a hash function defined by $h(x) = Ax \bmod 2$, where

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

and the “mod 2” is done for every entry of Ax . Find a collision for the hash function h .

3. **(20 points)** Let $N = 17 \times 19 = 323$ and $e = 11$. Let $pk = (N, e)$ be the public key in the plain RSA signature scheme. Compute the plain RSA signature of $m = 100$.
4. **(20 points)** Let F be a length-preserving PRF. Let $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ be a fixed-length MAC for messages of $2n$ bits:

- $\text{Gen}(1^n)$: choose $k \leftarrow \{0,1\}^n$ uniformly as the secret key.
- $\text{Mac}(k, x)$: To authenticate a message $x = (x_1, x_2)$, where $x_i \in \{0,1\}^n$ for $i = 1, 2$, compute and output the tag $t = (F_k(x_1), F_k(F_k(x_1) \oplus x_2))$.
- $\text{Vrfy}(k, x, t)$: for a message $x = (x_1, x_2) \in \{0,1\}^{2n}$ and a tag $t = (t_1, t_2) \in \{0,1\}^{2n}$, output 1 if and only if $t = (F_k(x_1), F_k(F_k(x_1) \oplus x_2))$.

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

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

- $\text{Gen}(1^n)$: choose a secret key $k \leftarrow \mathcal{K}$ uniformly from \mathcal{K} .
- $\text{Enc}(k, m)$: given $k \in \mathcal{K}$ and $m = (m_1, m_2) \in \mathcal{M}$, choose $r \in \{0,1\}^{n-1}$ uniformly at random, output $c = (r, F_k(r||0) \oplus m_1, F_k(r||1) \oplus m_2)$.
- $\text{Dec}(k, c)$: given $k \in \mathcal{K}$ and $c = (c_1, c_2, c_3)$, output $m = (F_k(c_1||0) \oplus c_2, F_k(c_1||1) \oplus c_3)$.

Determine whether Π is IND-CPA secure. Show your answers.