CS2107 —Introduction to Information Security
School of Computing
National University of Singapore

Midterm Test

2024/2025 Semester 2

6 March 2025 **Time allowed:** 1 hour

Instructions (please read carefully):

1. This is a **CLOSED** book assessment, but you are allowed to bring **ONE** double-sided A4 sheet of notes for this assessment.
2. The assessment paper contains **SEVENTEEN (17) questions** and comprises **TEN (10) pages** including this cover page.
3. The time allowed for solving this test is **1 hour**.
4. Weightage of each question is given in square brackets. The maximum attainable score is **25**.
5. Use of non-programmable calculators are allowed in the test.
6. You are allowed to use pencils, ball-pens or fountain pens, as you like as long as it is legible (no red color, please).
7. **Marks may be deducted** for unrecognizable handwriting. All corrections should be cleanly erased or covered with correction fluid or tape.

Instructions for ANSWER SHEET:

1. Write down your **student number** in the answer sheet and shade the corresponding circles with dark ink or pencil.
2. DO NOT WRITE YOUR NAME!
3. This answer sheet comprises 2 pages.
4. You must submit only the **ANSWER SHEET** and no other documents. The question set may be used as scratch paper.
5. All answers must be written within the corresponding box provided. **Anything written outside the answer box will not be accepted.**

GOOD LUCK!

This page is intentionally left blank for you to use as scratch paper.

Multiple Choice Questions [15 marks]

1. In the context of an ATM where users provide a personal identification number (PIN) and a card for account access, which of the following statements are False? [1 mark]

   A) The confidentiality of the user's PIN is crucial to prevent unauthorized access to their bank account.

   B) The ATM must be operational and accessible to ensure availability of services.

   C) Integrity involves ensuring that the transaction amount requested by the user is accurately deducted from their account balance.

   D) Ensuring the accuracy of transaction records is an aspect of confidentiality.

   D

2. Consider the following property of an encryption scheme: The same plaintext, when encrypted multiple times independently with the same key, results in different ciphertexts each time. What property does this describe? [1 mark]

   A) Deterministic encryption

   B) Probabilistic encryption

   C) Homomorphic encryption

   D) Block Cipher encryption

   B

3. Why is it important to develop an attack model or threat model when describing the security requirements of a system? Choose the most relevant answer. [1 mark]

   A) To ensure all software bugs are identified and fixed.

   B) An attack model is only useful for systems that have already been compromised.

   C) It helps identify and describe the class of attacks that the system can prevent.

   D) An attack model guarantees that a system is completely immune to all threats.

   C

4. Consider a permutation encryption applied twice to the message, `HeyCS2107` as follows: $P_{k2}(P_{k1}(HeyCS2107)$ where $k1 = (2,4,3,9,8,7,1,5,6)$ and $k2 = (7,1,3,2,8,9,6,5,4)$. Which of the following is the correct ciphertext? [1 mark]

   A) `HeyCS2107`

   B) `1Hye072SC`

   C) `HeSCy0271`

   D) `Heycs2107`

   A

5. Consider an 8-byte cipher block using the *PKCS*#7 padding scheme and an attacker who has access to a padding oracle. What is the maximum number of padding oracle calls required to determine the number of padding bytes added in the last ciphertext block in case of brute force attack?

   A) 8

   B) 255

   C) 255 x number of padded bytes

   D) 256 x number of padded bytes

   Void

6. AES in CBC mode is applied to an input consisting of 5 blocks, each block being 64 bits in size. During decryption, if the first bit of the third block of ciphertext is corrupted, how many bits of the whole plaintext are affected? [1 mark]

   A) 64 bits

   B) 65 bits

   C) 194 bits

   D) 320 bits

   B

7. An insecure version of RSA has been deployed. Given that a user's public key is $e = 13$ and $n = 77$. Find d [1 mark]

   A) 13

   B) 15

   C) 25

   D) 37

   D

8. NUSCorp is preparing to launch a new software update for its flagship product which will be downloaded by vast number of clients. To ensure that clients can download the file while maintaining both data integrity and authenticity, which of the following solutions best meets NUSCorp's requirements? [1 mark]

   A) Using hash function

   B) Using digital signature

   C) Using message authentication code

   D) Using basic encryption

   B

9. Which of the following statements regarding the "hash-then-sign" approach in digital signatures is true? [1 mark]

   A) Hash-then-sign decreases security by exposing the message to attackers.

   B) Hash-then-sign is less efficient because it requires signing the hash directly.

   C) Hash-then-sign eliminates the need for a private key, making the process more accessible.

   D

   D) Hash-then-sign ensures that only a fixed-size hash is signed.

10. An attacker has access to a single hashed password. The attacker possesses a dictionary containing 1 million (i.e., 10^6) potential passwords and knows that a unique 16-bit salt is concatenated with each password before hashing. If the attacker can test $10,000$ password-salt combinations per second, how long will it take to find the correct password in the worst-case scenario? Choose the closest approximate answer. [1 mark]

    A) 0.02 hours

    B) 18 hours

    C

    C) 75 days

    D) 100 days

11. What is the main reason that makes a system vulnerable to a password reset poisoning attack? Choose the most relevant answer. [1 mark]

    A) The system uses outdated encryption algorithms for storing user passwords.

    B) The system uses predictable tokens for password reset links, allowing attackers to guess them easily.

    C) The system allows users to choose weak passwords.

    D

    D) The system fails to validate and sanitize user-controllable inputs.

12. A biometric authentication system was tested using 3,500 total attempts out of which 1,500 are genuine attempts. The results of the test are as follows:
    (A) Genuine attempts incorrectly rejected: 75
    (B) Imposter attempts incorrectly accepted: 60
    Using these results, calculate the False Match Rate (FMR) and False Non-Match Rate (FNMR) of the system. [1 mark]

    A) FMR = 5%, FNMR = 3%

    B) FMR = 3%, FNMR = 5%

    C) FMR = 4%, FNMR = 3%

    B

    D) FMR = 1%, FNMR = 2%

13. What is the primary purpose of having multiple levels of Certificate Authorities (CAs) in a CA hierarchy for certificate issuance? Choose the most relevant answer. [1 mark]

    A) To create a more complex system that is harder for attackers to understand and compromise.

    B) To improve certificate validity by having multiple CAs sign a single certificate.

    C) To ensure that certificates can only be issued for domains with a specific geographic location.

    D) To enhance the security and trust of the PKI by distributing trust across multiple levels.

    D

14. What is the primary advantage of stapling an OCSP response alongside a certificate? [1 mark]

    A) It eliminates the need for the client to contact the Certificate Authority (CA) directly.

    B) It reduces the size of the certificate, making the connection faster.

    C) It allows the server to use multiple certificates for the same domain, enhancing security.

    D) It automatically updates the certificate's expiration date to ensure continuous validity.

    A

15. How does Certificate Transparency (CT) help in detecting rogue CAs that issue unauthorized certificates? [1 mark]

    A) CT requires all CAs to store their private keys in a public repository, ensuring transparency.

    B) CT encrypts all issued certificates, making it impossible for rogue CAs to issue unauthorized certificates.

    C) CT logs all issued certificates in a publicly accessible log.

    D) CT automatically revokes any certificate that is not registered in the public log.

    C

Short Answer Section [10 marks]

16. Imagine a company called `BlockSecure` that uses blockchain technology to record digital transactions. In this simplified model, each transaction is stored as a unique block within the blockchain. A transaction represents an action, such as transferring funds or exchanging information between two parties. When a user initiates a transaction, it is submitted to `BlockSecure`'s network for validation. Once validated, it is combined with other relevant information to form a complete block. The company compiles multiple validated blocks into a blockchain.

    Clients, like small devices or applications with limited processing power, need to verify the accuracy of a transaction by confirming its presence in the blockchain. However, due to their limited resources, these clients require a method to quickly verify transactions without the need to download the entire blockchain. BlockSecure seeks a solution to implement blockchain that ensures data integrity while minimizing resource use, allowing efficient transaction verification. [6 marks]

    Merkle tree, append only property, hashing of the child nodes and building it up, sign root hash

    (a) Given the criteria for clients, which data structure (*among all data structures taught in the lecture*) is best suited for implementing the blockchain? Explain the property that makes it a good choice. [3 marks]

    (b) Explain what information the client needs to verify whether a transaction is present in the blockchain data structure you decided on. proof of inclusion [3 marks]

17. Alice designs a new hash function $H(x)$ based on the existing `SHA-256` in this way:

$$H(x) = \texttt{SHA3}(x \oplus k) \oplus \texttt{SHA3}(\texttt{rot}(x,n))$$

    where k is a fixed secret key of the same length as x and `rot(x, n)` performs a cyclic bit rotation on the binary sequence x by n positions (e.g., $rot(110,1) = 011$). Provide a collision example (i.e., two inputs $x1$ and $x2$ along with key, k and position, n) to show that H is not collision resistant. In your answer, the length of each input should be at least 4 bits. [4 marks]

    Many solution, one is X1= 0101, X2 = 1010, k =0000, n = 4

— END OF QUESTIONS —

This page is intentionally left blank for you to use as scratch paper.

This page is intentionally left blank for you to use as scratch paper.

This page is intentionally left blank for you to use as scratch paper.

— E N D O F P A P E R —

CS2107 Introduction to Information Security

Midterm Test — Answer Sheet

STUDENT NUMBER

A

U ○
A ●
HT ○
NT ○

0	0	0	0	0	0	0	A	N
1	1	1	1	1	1	1	B	R
2	2	2	2	2	2	2	E	U
3	3	3	3	3	3	3	H	W
4	4	4	4	4	4	4	J	X
5	5	5	5	5	5	5	L	Y
6	6	6	6	6	6	6	M	
7	7	7	7	7	7	7		
8	8	8	8	8	8	8		
9	9	9	9	9	9	9		■

FOR EXAMINER'S USE

Question	Marks
Q1-Q15	/ 15
Q16a	/ 3
Q16b	/ 3
Q17	/ 4
Total	/ 25

1. (A) (B) (C) (D)
2. (A) (B) (C) (D)
3. (A) (B) (C) (D)
4. (A) (B) (C) (D)
5. (A) (B) (C) (D)
6. (A) (B) (C) (D)
7. (A) (B) (C) (D)
8. (A) (B) (C) (D)
9. (A) (B) (C) (D)
10. (A) (B) (C) (D)
11. (A) (B) (C) (D)
12. (A) (B) (C) (D)
13. (A) (B) (C) (D)
14. (A) (B) (C) (D)
15. (A) (B) (C) (D)

16. (a) Block Secure: Data structure

(b) Block Secure: Information needed

17. Collision example

— END OF ANSWER SHEET —