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

Endterm Exam

2024/2025 Semester 2

5 May 2025 **Time allowed:** 2 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 **TWENTY NINE (29) questions** and comprises **SIXTEEN (16) pages** including this cover page.
3. The time allowed for solving this test is **2 hour**.
4. Weightage of each question is given in square brackets. The maximum attainable score is **50**.
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 4 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 [1 mark each - 20 marks]

1. Alice uses AES in CTR mode to encrypt a message consisting of n blocks using a secret key k and a counter value v. However, she forgets to increment the counter value after encrypting each block. Suppose Mallory intercepts all n ciphertext blocks. Mallory also somehow knows the content of the first plaintext block but does not know the secret key k. How many blocks of the plaintext can Mallory derive in this scenario? [1 mark]

   A) Mallory can derive only the first plaintext block which he already knows

   B) Mallory can derive the first $n-1$ plaintext blocks

   C) Mallory can derive the first two plaintext blocks

   D) Mallory can derive all n plaintext blocks

2. Consider an encryption scheme where a plaintext, P is encrypted to produce $C1 = E(P,K1)$ and then $C2 = E(P,C1)$ with both the block size and key size being 32 bits. Suppose the attacker has access to P, $C2$ but does not know the key $K1$ and $C1$. How many *minimal* cryptographic operations (i.e., encryption, decryption) would be required to find the *correct key*, $K1$ in the worst case?

   [1 mark]

   A) 2^{32} operations

   B) 2^{33} operations

   C) 2^{64} operation

   D) 2^{65} encryption

   E) None of the above

3. Consider two systems for storing user passwords. System A stores passwords as hash values without any salt, while System B stores passwords as hash values with a unique 12-bit salt for each password. By what factor does System B increase the difficulty for an attacker attempting to crack the passwords using a dictionary attack (in terms of the number of hash operations required) compared to System A. Assume the salt is not known to the attacker. [1 mark]

   A) System B increases the number of hash operation by a factor of 12

   B) System B increases the number of hash operation by a factor of 1024

   C) System B increases the number of hash operation by a factor of 2048

   D) System B increases the number of hash operation by a factor of 4096

   E) None of the above

4. A secure messaging system encrypts each message using AES in CTR mode. For each encryption, a random 56-bit IV is chosen independently and uniformly. Approximately how many messages must be encrypted for the probability of at least one IV collision to reach 40%? [1 mark]

   A) 2^{20} **B)** 2^{24}

   C) 2^{28} **D)** 2^{32}

   E) None of the above

5. What is the primary reason for the CT log to issue Signed Certificate Timestamp (SCT) to the domain owner? Choose the most relevant answer. [1 mark]

   A) To enable browsers to validate the certificate directly using SCT without ever needing to check the CT log.

   B) To ensure that only clients with SCT can query the CT log for certificate information.

   C) To provide a timestamp on when the certificate will be included into CT log.

   D) To provide proof that the certificate has been submitted and logged into CT log.

   E) None of the above

6. A university implements a digital grading system where each student's final grade report is secured using a cryptographic hash function. The university stores only the hash of the grade report in its records. Which property of the hash function is necessary to prevent a student from generating a fake grade report that hashes to the same value as any of the original reports? [1 mark]

   A) Pre-image resistance **B)** Collision resistance

   C) Second pre-image resistance **D)** Option (A) and (B)

   E) Option (A), (B), and (C)

7. The university introduces a re-evaluation policy and ensures that updated grade reports after re-evaluation do not hash to the same value as the original. Which property of the hash function is necessary to *prevent a student* from generating a fake grade report that hashes to the same value as a particular original report? [1 mark]

   A) Pre-image resistance **B)** Collision resistance

   C) Second pre-image resistance **D)** Option (A) and (B)

   E) Option (A), (B), and (C)

8. The university's server was compromised and hashes of the final grade report is leaked. Which property of a cryptographic hash function is necessary to ensure that it is not possible to deduce the content of their original grade report from the leaked information? [1 mark]

   A) Pre-image resistance **B)** Collision resistance

   C) Second pre-image resistance **D)** Option (A) and (B)

   E) Option (A), (B), and (C)

9. Can the Same-Origin Policy prevent XSS attacks on a website that does not properly sanitize user input? Choose the most appropriate answer. [1 mark]

   A) Yes, because SOP blocks all scripts from being executed on the client browser.

   B) No, because SOP restricts cross-origin access but does not prevent malicious scripts from executing within the same origin.

   C) Yes, because SOP ensures that only trusted scripts can be executed on client browser.

   D) No, because SOP is designed to prevent access to same-origin data.

   E) None of the above

10. Consider four nodes A, B, C, and D with IP and MAC address (IP_A, MAC_A), (IP_B, MAC_B), (IP_C, MAC_C), and (IP_D, MAC_D), respectively, all belonging to the same subnetwork connected via a switch. Node A is malicious and wants to observe the traffic between nodes B, C , D by acting as a Man-in-the-Middle (MITM). Which of the following actions should node A take to achieve this using ARP poisoning? [1 mark]

    A) Node A should broadcast ARP replies to B, C, and D associating the MAC addresses MAC_B, MAC_C, and MAC_D with its own IP address IP_A.

    B) Node A should broadcast ARP request to B, C, and D, requesting MAC address of the IP addresses IP_B, IP_C, and IP_D.

    C) Node A should broadcast ARP replies to B, C, and D, associating its MAC address MAC_A with the IP addresses IP_B, IP_C, and IP_D.

    D) Node A should broadcast ARP request to B, C, and D, requesting IP address of the MAC addresses MAC_B, MAC_C, and MAC_D.

    E) Node A is inherently a MITM as it is already positioned to automatically intercept traffic between nodes B, C, and D.

11. Based on the previous scenario from Q10, which of the following is the main reason that allowed Node *A* to position itself as MITM using ARP poisoning? Choose the most appropriate answer. [1 mark]

    A) ARP is a stateful protocol, meaning hosts accept ARP replies without verifying if they previously sent a request.

    B) Switches always forward every frames to all devices, making MITM attacks easier.

    C) Both ARP request and ARP response are always broadcast.

    D) ARP replies are only accepted by devices that request for it.

    E) The lack of authentication in the ARP protocol, allowing it to send spoofed ARP messages.

12. An attacker is present in an airport café and connects to the open Wi-Fi network. Alice, who is also connected to the same café Wi-Fi, uploads a file named *A.txt* to the server *SoCserver* using secure HTTPS. Assume that any DNS resolution done is not protected. Which of the following information can the attacker obtain? Choose the most appropriate answer. [1 mark]

    A) The attacker can see that a file named *A.txt*, along with its content, has been sent to the destination server *SoCserver*.

    B) The attacker can determine that *A.txt* was sent by Alice but cannot see its content or the destination server *SoCserver*.

    C) The attacker can observe that some data was transmitted but cannot identify the destination server *SoCserver*.

    D) The attacker can detect that some data was sent to *SoCserver* but cannot see its content.

    E) The attacker can only see that some data was transmitted, without knowledge of its content or destination.

13. Consider the same scenario from previous question Q12, but now Alice connects via a VPN (using IPSec) to the server *SoCserver* first and then uploads the file. All other assumptions remain the same. Which of the following information can the attacker obtain? Choose the most appropriate answer. [1 mark]

    A) The attacker can see that a file named *A.txt*, along with its content, has been sent to the destination server *SoCserver*.

    B) The attacker can determine that *A.txt* was sent by Alice but cannot see its content or the destination server *SoCserver*.

    C) The attacker can observe that some data was transmitted but cannot identify the destination server *SoCserver*.

    D) The attacker can detect that some data was sent to *SoCserver* but cannot see its content.

    E) The attacker can only see that some data was transmitted, without knowledge of its content or destination.

14. Consider the following C statement: [1 mark]

```
printf("%08x %08x %08x %08x %08x");
```

Is this statement vulnerable? Choose the most appropriate answer.

A) No, this statement is safe as long as it does not take user input.

B) Yes, this statement retrieves five parameters from the stack and then crashes the program.

C) Yes, this statement retrieves five parameters from the stack and displays them as hexadecimal numbers.

D) No, statement prints memory addresses but does not affect program security.

E) Yes, statement prints memory addresses that affect the security of the program.

15. An attacker registers and configures the spoofed website `comp.nus.edu.sg\0.attacker.com` and tricks a victim into visiting the site. The attacker server presents a valid certificate, which the browser verifies according to the non-null termination scheme. Which of the following statements is true? [1 mark]

A) The vigilant victim can detect that he is visiting the spoofed `comp` domain if the browser displays the URL using non-null termination.

B) The vigilant victim can detect that he is visiting the spoofed `comp` domain if the browser displays the URL using null termination.

C) The browser does not trust the `comp` domain containing a null character and prevents them from loading.

D) The attacker cannot spoof the `comp` domain because the certificate verification will fail.

E) None of the above is true.

16. Consider the following code snippet:

```
void test_func(char *input) {
  Line 1.   char buffer[10];
  Line 2.   strcpy(buffer, input);
  Line 3.   printf("Buffer content: %s");
}
int main() {
  Line 4.  char user_input[20];
    ...
  Line 5.  test_func(user_input);  //  user_input inputted by the the user
    return 0;
}
```

Which line of code may cause a buffer overflow? [1 mark]

A) Line 1 **B)** Line 2

C) Line 3 **D)** Line 5

E) No vulnerable line

17. Based on the code from the previous questions Q16, how can the code be modified to prevent a buffer overflow vulnerability if present? Choose the most appropriate answer. [1 mark]

A) Use `strcpy()` with an additional safety parameter to limit the characters copied.

B) Allow the input size to be flexible and handle any input length in the buffer.

C) Increase the size of buffer to be equal to or larger than user_input.

D) Use `strncpy()` to safely copy the input into the buffer, specifying the buffer's size.

E) No vulnerable line

18. Which of the following best demonstrates the Swiss Cheese Model used as guide to set security perimeter? [1 mark]

A) A university allows students to access all campus IT resources with a single password.

B) A company enforces a strict password policy requiring employees to update their passwords every 30 days.

C) A company isolates its internal systems from external access using a single firewall.

D) A bank requires multi-factor authentication (MFA) and uses fraud detection systems to flag unusual transactions.

E) None of the above

19. Which of the following statements regarding Access Control Lists (ACL) and Capability Lists is true? [1 mark]

    A) Capability Lists store access rights per object, while ACLs store them per subject.

    B) Capability Lists provide an easier way to review access rights of objects compared to Access Control Lists.

    C) ACLs make it difficult to determine all objects a subject has access to, while Capability Lists make it difficult to determine all subjects who have access to a specific object.

    D) Both ACLs and Capability Lists allow easy retrieval of access rights for both subjects and objects.

    E) None of the above

20. Alice executes the script `example.sh`, which is owned by Bob and located at `/home/bob/example.sh`. The script displays both real and effective user IDs (UIDs). Consider the following two cases:

    - Case 1: The script is executed by Alice without the SUID (SetUID) bit set.
    - Case 2: The SUID bit is set on `example.sh`, and then Alice executes the script.

    Which of the following statements correctly describes the output of the id command in both cases? [1 mark]

    A) In Case 1, both the real and effective UIDs are Bob. In Case 2, both UIDs are Alice.

    B) In Case 1, both the real and effective UIDs are Alice. In Case 2, the real UID is Alice, and the effective UID is Bob.

    C) In Case 1, the real UID is Bob, and the effective UID is Alice. In Case 2, both UIDs are Bob.

    D) In Case 1, the real UID is Alice, and the effective UID is Bob. In Case 2, both UIDs are Alice.

    E) In Case 1, both the real and effective UIDs are Alice. In Case 2, the real UID is Bob, and the effective UID is Alice.

Multiple Choice Questions [2 marks each - 10 marks]

21. Why is it recommended to use different cryptographic keys for operations such as encryption and authentication in a secure system? Choose the most relevant answer. [2 marks]

    (1) To reduce the number of keys an attacker needs to obtain to compromise the entire system.

    (2) It prevents attackers from modifying both the ciphertext and its tag without detection.

    (3) Enhances security by limiting the impact of a compromised key.

    (4) To make the system more complex and difficult for clients/users.

    A) (1), (2), (3)

    B) (2), (3)

    C) (2), (3), (4)

    D) (1), (3), (4)

    E) (1), (2), (3), (4)

22. What is the benefit of the Encrypt-then-MAC (EtM) scheme over Encrypt-and-MAC (E&M) and MAC-then-Encrypt (MtE) schemes for authenticated encryption? [2 marks]

    (1) EtM is the only scheme that encrypts and compute MAC tag directly on the plaintext.

    (2) Only EtM uses separate keys for encryption and message authentication unlike E&M and MtE.

    (3) EtM ensures that any tampering with the ciphertext is detected before decryption.

    (4) EtM verifies integrity before decryption, preventing attacks that exploit ciphertext malleability.

    A) (1), (2)

    B) (2), (3)

    C) (3), (4)

    D) (1), (2), (3)

    E) (2), (3), (4)

23. Which of the following is an advantage of QUIC over traditional TLS over TCP? [2 marks]

    (1) QUIC eliminates the need for any cryptographic handshakes, making it faster.

    (2) QUIC reduces latency by combining TLS encryption with transport-layer functionality.

    (3) Before the cipher suite is negotiated, QUIC uses a three-way handshake like TCP to ensure reliability .

    (4) QUIC runs over UDP, reducing latency since no prior connection setup is required.

    A) (2), (4) **B)** (1), (2), (4)

    C) (2), (3) **D)** (1), (2), (3)

    E) (1), (2), (3), (4)

24. Which of the following is a reason for the DoS amplification attack? [2 marks]

    (1) Ability of the attacker to command and control botnets.

    (2) Ability of the attacker to find intermediate nodes that use protocols that generate large responses compared to small requests.

    (3) Ability of the attacker to manipulate the DNS cache to redirect traffic to a specific IP address.

    (4) Ability of the attacker to direct traffic to a specific IP address.

    A) (1), (2) **B)** (2), (3)

    C) (1), (2), (3) **D)** (1), (2), (4)

    E) (1), (2), (3), (4)

25. Which of the following malicious input correctly generate the SQL query that return all the rows from the TABLE. The SQL query generated is:

    `"SELECT␣*␣FROM␣TABLE␣WHERE␣username␣=␣'"␣+␣UN␣+"';"`

    where UN is the input received from the user. [2 marks]

    (1) `'␣OR␣'1'␣=␣'1';␣--␣`

    (2) `'␣OR␣'1'␣=␣'1'␣--␣`

    (3) `''␣OR␣'1'␣=␣'1';␣--␣`

    (4) `admin'␣OR␣'1'␣=␣'1';␣--␣`

    A) (2), (4) **B)** (1), (4)

    C) (1), (3), (4) **D)** (1), (2), (3)

    E) (1), (2), (4)

Short Answer Section [20 marks]

26. Alice has a one-block message $M1$. She chooses a random IV and computes the MAC tag as $t = MAC(K, IV \oplus M1)$ where MAC is `AES-CBC` scheme. [5 marks]

    (a) Mallory wants to change the message from $M1$ to $M2$, while keeping the MAC tag the same t. To achieve this, what value should Mallory choose for IV'. Explain the attack step. Assume Mallory knows $M1$, IV and t, but not the key, K. [3 marks]

    (b) What is a possible countermeasure? [2 marks]

27. Imagine Alice, Bob and Charlie are three explorers who have found an ancient treasure chest with a special combination lock. They want to set a secret code to unlock it later, but there's a problem — a group of rival treasure hunters are eavesdropping on their conversation. They need a way to establish a shared lock combination without directly revealing it to their rivals. They decide to use the following protocol (a variant of Diffie-Hellman), but need your help to fill in the blanks.

    [4 marks]

    (a) Alice, Bob, and Charlie agree on a public prime number (p) and a multiplier (g), both of which are written on the chest itself and visible to everyone.

    (b) Alice and Bob pick two secret numbers, a and b, respectively. They do not share these secret numbers with anyone.

    (c) Alice computes: $\underline{X = (1)}$; Bob computes $\underline{Y = (2)}$.

    (d) Alice and Bob speaks out X and Y out loud.

    (e) Next, Alice and Bob compute: $\underline{K_{AB} = (3)}$.

    (f) Next Bob and Charlie pick two secret numbers, b' and c, such that $\underline{b' = (4)}$. They do not share these secret numbers with anyone.

    (g) Bob computes: $\underline{Z = (5)}$; Charlie computes $\underline{U = (6)}$.

    (h) Alice computes: $\underline{a' = (7)}$.

    (i) Bob and Charlie speaks out Z and U out loud.

    (j) Finally, Alice, Bob and Charlie computes the common lock combination: $\underline{K_{ABC} = (8)}$.

28. Upon learning that the AES encryption using CBC mode of operation and PKCS#7 padding is susceptible to a padding oracle attack, Alice attempts to design her own padding scheme, called OSC#1, which modifies the padding content of PKCS#7. For simplicity, the following specification will be applicable to blocks of size 16 bytes. Let l be the length of the plaintext, in bytes. **Each byte below are denoted in hexadecimal** [16 symbols (0-9 and A-F) to represent numbers, where A-F represent 10-15 in decimal]. The following is the padding to be appended at the trailing end:

01	if l mod 16 = 15
FF FF	if l mod 16 = 14
02 02 02	if l mod 16 = 13
FE FE FE FE	if l mod 16 = 12
03 03 03 03 03	if l mod 16 = 11
FD FD FD FD FD FD	if l mod 16 = 10
04 04 04 04 04 04 04	if l mod 16 = 9
FC FC FC FC FC FC FC FC	if l mod 16 = 8
05 05 05 05 05 05 05 05 05	if l mod 16 = 7
FB FB FB FB FB FB FB FB FB FB	if l mod 16 = 6
06 06 06 06 06 06 06 06 06 06 06	if l mod 16 = 5
FA FA FA FA FA FA FA FA FA FA FA FA	if l mod 16 = 4
07 07 07 07 07 07 07 07 07 07 07 07 07	if l mod 16 = 3
F9 F9 F9 F9 F9 F9 F9 F9 F9 F9 F9 F9 F9 F9	if l mod 16 = 2
08 08 08 08 08 08 08 08 08 08 08 08 08 08 08	if l mod 16 = 1
F8 F8 F8 F8 F8 F8 F8 F8 F8 F8 F8 F8 F8 F8 F8 F8	if l mod 16 = 0

For clarity, if the plaintext size is a multiple of 16 bytes, the padding will occupy a full block. Here are some examples on plaintexts padded with OSC#1 padding, with the padding bytes in bold:

- A message of length 7 bytes, which is then padded with 9 padding bytes:

53	6E	45	41	6B	79	21	**05**	**05**	**05**	**05**	**05**	**05**	**05**	**05**	**05**

- A message of length 16 bytes, which is then padded with 16 padding bytes:

75	53	65	5F	72	6F	54	28	6E	29	74	6F	3B	23	44	65
F8	**F8**	**F8**	**F8**	**F8**	**F8**	**F8**	**F8**	**F8**	**F8**	**F8**	**F8**	**F8**	**F8**	**F8**	**F8**

- A message of length 14 bytes, which is then padded with 2 padding bytes

43	52	79	70	74	20	63	20	62	45	6C	4F	77	21	**FF**	**FF**

Unfortunately, OSC#1 is still susceptible to padding oracle attack. Mallory obtains the following IV, v ; and 1 block of ciphertext, c as follows:

v	49	63	4C	75	50	6D	4F	73	4D	6E	47	6C	52	75	46	72
c	76	51	69	59	37	2E	61	63	41	2E	59	6D	52	73	47	75

Mallory then performs a linear search and found out that the original plaintext is padded with 4 bytes. Additionally, after doing two rounds of padding oracle attack, Mallory obtains the last 2 bytes of the non-padding plaintext as follows:

v	49	63	4C	75	50	6D	4F	73	4D	6E	47	6C	52	75	46	72
c	76	51	69	59	37	2E	61	63	41	2E	59	6D	52	73	47	75
p	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	36	83	FE	FE	FE	FE

Please answer the following questions: [7 marks]

(a) In the third round of the padding oracle attack, Mallory sends the v' (check answer sheet). Fill in the empty entries in the table. Calculate your value and answer in hexadecimal. [6 marks]

(b) Mallory sends 256 pairs of (v', c) to the padding oracle, varying the value of x from 00 to FF. The padding oracle replies “correct padding” when x is 29. What is the value of $p10$? Give your answer in hexadecimal. [1 mark]

29. Alice is a user of the FaceTalk web application, which allows users to chat with each other. The application provides a feature to change the user’s password using a POST request via the following form:

```
<form id="changepass" method="POST" action="http://facetalk.com/password.php">
<input type="text" name="password" value="P@ssw0rD">
<input type="submit" value="Change my password"/>
</form>
```

Mallory discovers that the application lacks any CSRF protection and decides to hijack Alice’s account by changing her password to one known to her (e.g., 1234). Additionally, `FaceTalk` does not use two-factor authentication (2FA). [4 marks]

(a) As a first step, Mallory sends Alice a malicious email with a link, enticing her to click on it. When Alice clicks the link, her browser *stealthily* sends a password change request to `FaceTalk`. Write down the malicious HTML form that Mallory could send to change Alice’s password to 1234. [3 marks]

(b) Mallory notices that Alice’s password has not changed. Identify and explain the most likely reason why the attack did not succeed. [1 mark]

— 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.

— END OF PAPER —