THE UNIVERSITY OF SYDNEY

CONFIDENTIAL

SEAT NUMBER: _____
STUDENT ID: _____
SURNAME: _____
GIVEN NAMES: _____

INFO3616/CSEC3616/CSEC5616
Principles of Security Engineering/Cybersecurity Engineering

Final Examination
2026, Semester 2

Time Allowed: 120 minutes + 10 minutes reading time

This examination paper consists of 21 pages.

INSTRUCTIONS TO CANDIDATES

1. This is a restricted open-book exam. You are allowed to bring two A4 pages of printed or written material (double sided).
2. This examination paper consists of two parts. Part 1 consists of 30 multiple choice/multiple answer questions and Part 2 consists of 2 written questions with multiple parts.
3. In Part 1, multiple answer questions have the text "SELECT ALL THAT APPLY" and other questions are multiple choice questions that have only a single answer.
4. In Part 2, each question is followed by space for your answer. There is additional space at the end if you need it. If you use the additional space you have to mention it in the given space after the question. Otherwise the additional space will not be marked.
5. The points for each question are shown at the start of the question. The total number of points for the whole paper is 100.
6. Any calculator (non-programmable or programmable) is allowed.
7. Take care to write legibly. Use blue or black ink. *Do not use a pencil.*

I have checked the examination paper and affirm it is complete.

Student Signature: _____ Date: _____

Office use only

Section	INFO3616/CSEC3616/CSEC5616
Part 1 (Questions 1–30)	/ 60
Part 2 (Questions 1–2)	/ 40
Total	/ 100

EXAMINATION PAPER NOT TO BE REMOVED FROM THE EXAMINATION ROOM

Part 1
Multiple Choice and Multiple Answer Questions
[60 points]

The options for each question are labelled A to E. Record the letter(s) of your chosen option(s) on the answer sheet provided; answers written anywhere else will not be marked. Questions marked "Select all that apply" may have more than one correct option. All other questions have exactly one correct option.

1. **[2 points]** A research laboratory's director states: "Unpublished research results must be accessible only to members of the project that produced them." The statement does not specify any software, hardware, or procedure for enforcing this requirement.

Which component of the security engineering framework does this statement represent?

- **A.** Assuarance
- **B.** Incentives
- **C.** Policy
- **D.** Access Control
- **E.** Mechanisms

2. **[2 points]** A military communication link experiences an equipment fault. The commander has two options for sending urgent instructions: use a satellite relay, which is available but introduces a long communication delay, or switch to an unencrypted communication channel, which can deliver messages immediately but could be monitored by an opponent.

The commander chooses the unencrypted channel so that the urgent instructions reach the intended recipients without delay.

Which trade-off is most directly illustrated?

- **A.** Integrity is prioritised over confidentiality
- **B.** Confidentiality is prioritised over availability
- **C.** Availability is prioritised over confidentiality
- **D.** Authentication is prioritised over availability
- **E.** Confidentiality is prioritised over integrity

3. **[2 points]** Which activities are passive attacks. **Select all that apply.**

- **A.** An attacker records the timing and volume of encrypted messages to infer when a team is active, without interfering with the messages.
- **B.** An attacker changes the delivery address in a message before forwarding it.
- **C.** An attacker reads unencrypted messages travelling over a network, without modifying or delaying them.
- **D.** An attacker retransmits a previously recorded instruction to make a system execute it again.
- **E.** An attacker disrupts a communication channel so legitimate users cannot exchange messages.

4. **[2 points]** An attacker phones an employee, says they are running a company-wide survey, and mentions the names of three colleagues in the same department who have "already completed it." The employee answers questions that reveal sensitive information. Which psychological bias/influencing technique does this demonstrate?

- **A.** Like bias
- **B.** Social proof
- **C.** Respect for authority
- **D.** Reciprocity
- **E.** Anchoring effect

5. **[2 points]** A user signs in to a website using a biometric passkey process. Their user device asks for a fingerprint, then completes the login. Which statement correctly describes the roles of the fingerprint and the keys?

- **A.** The website receives the fingerprint and compares it with a stored fingerprint template.
- **B.** The device sends its private key to the website after the fingerprint matches.
- **C.** The fingerprint itself is the public key registered with the website.
- **D.** The website signs the challenge with the public key, and the device verifies it using the user's fingerprint.
- **E.** The fingerprint authorises local use of the private key; the website verifies the signed challenge using the registered public key.

6. **[2 points]** A company uses the following password policy:

1. A password must be **exactly eight characters long**.
2. The **first character** must be an uppercase English letter (`A--Z`).
3. The **next five characters** must be lowercase English letters (`a--z`).
4. The **last two characters** must be digits (`0--9`). Leading zeros in this two-digit ending are allowed.
5. Repeated letters and repeated digits are allowed. Spaces and special characters are not allowed.

For example, `Abcdef07` satisfies the policy. Passwords are **generated automatically**, with each position chosen independently and uniformly from its permitted character set. An attacker knows the policy. Using $H = \log_2(N)$, where N is the number of equally likely valid passwords, what is the entropy of a generated password? Round to two decimal places.

A. 47.63 bits

B. 32.52 bits

C. 34.85 bits

D. 37.60 bits

E. 29.85 bits

7. **[2 points]** Which of the following best describes **authorization**?

A. Verifying a user's identity with a password or fingerprint.

B. The allocation of a privilege to a party, or verifying that an entity is allowed an action.

C. A matrix with rows for users and columns for files showing `r`, `w`, and `x` rights.

D. The process of analysing an attacker's motivations and capabilities.

E. Recording and auditing the actions performed by users on a system.

8. **[2 points]** Which of the following statements about the **set-user-ID (SUID)** bit are TRUE? **Select all that apply.**

A. When set on an executable, the program runs with the privileges of the file's owner rather than those of the user who launched it.

B. `passwd` and `mount` are examples of SUID-root programs.

C. `ls -l` shows a set SUID bit as an `s` in the owner's execute position.

D. The SUID bit changes the process's real UID to that of the file owner.

E. The SUID bit on a directory causes new files to inherit the directory's owner.

9. **[2 points]** In the Bell–LaPadula model, which property prevents a subject with **Secret** clearance from reading a document classified **Top Secret**?

A. The $*$-property (no write down)

B. The simple security property (no read up)

C. The invocation property

D. The simple integrity property

E. The tranquility property

10. **[2 points]** A company develops an encryption system and publishes its complete algorithm for independent security analysis. The company assumes that an attacker knows the algorithm but does not know the secret key. Which principle does this design follow?

A. The principle of least privilege

B. Kerckhoffs' principle

C. The separation of duties principle

D. The *fail-safe defaults* principle

E. The principle of security through obscurity

11. **[2 points]** Which of the following statements are TRUE? Select all that apply

A. $\mathbb{Z}_{11} = \{0, 1, \ldots, 10\}$ with addition and multiplication modulo 11 is a finite field.

B. The multiplicative inverse of 7 modulo 11 is 8.

C. 6 has a multiplicative inverse modulo 9.

D. In $\mathbb{Z}_{12}$, the element 5 is its own multiplicative inverse.

E. The set of integers $\mathbb{Z}$ with ordinary addition and multiplication is a field.

12. **[2 points]** A ciphertext produced by the Vigenère cipher contains a repeated trigram. The distance between the first and second occurrence is 40 characters, and between the second and third is 24 characters. Which key length is most consistent with both observations?

A. 3

B. 6

C. 8

D. 12

E. 24

13. **[2 points]** A simple cipher computes $c = p \oplus k$. Given $p = 11001010$ and $k = 01101100$, which statements are TRUE?

A. $c = 10100110$.

B. $c \oplus p = k$.

C. An attacker who obtains one plaintext-ciphertext pair can recover the key.

D. Reusing k to encrypt a second, different message is safe because the messages differ.

E. If the same key is used for two messages, $C_1 \oplus C_2 = P_1 \oplus P_2$.

14. **[2 points]** Bob wants to send Alice a message so that Alice, and anyone else, can be sure the message really came from Bob. Using public-key cryptography, which key does Bob use, and which key is used to verify?

A. Bob encrypts with Alice's public key; only Alice verifies with her private key.

B. Bob encrypts with Alice's private key; anyone verifies with Alice's public key.

C. Bob encrypts (signs) with his own private key; anyone verifies with Bob's public key.

D. Bob encrypts with his own public key; anyone verifies with Bob's private key.

E. Bob encrypts with Alice's public key; anyone verifies with Bob's public key.

15. **[2 points]** Which of the following correctly states the **Discrete Logarithm Problem** on which Diffie-Hellman relies?

A. Given a large $n = pq$, find the prime factors p and q.

B. Given c, e, and n with $c = m^e \bmod n$, find m.

C. Given y, g, and a prime p with $y = g^x \bmod p$, where g is a primitive root of p, find x.

D. Given g, x, and p, compute $y = g^x \bmod p$.

E. Given g, y, and a prime p, determine whether g is a primitive root of p.

16. **[2 points]** Let H be a cryptographic hash function. Given a randomly chosen output value y, it is computationally infeasible to find any input x such that $H(x) = y$. Which property does this define?

A. Collision resistance

B. Second preimage resistance

C. Preimage resistance

D. Pseudo-randomness

E. One-wayness

17. **[2 points]** A protocol first encrypts the message, $C = E(K_2, M)$, and then computes a message authentication code over the ciphertext, $T = MAC(K_1, C)$, sending (C, T). Which approach is being used, and which protocol uses this approach?

A. MAC-then-Encrypt; SSL/TLS

B. Encrypt-then-MAC; IPsec

C. Encrypt-and-MAC; SSH

D. Hash-then-Encrypt; SSH

E. Encrypt-then-Hash; HTTPS

18. **[2 points]** Under the Dolev-Yao model, which of the following actions can an attacker perform?

A. Eavesdrop on messages transmitted over the network.

B. Delay, delete, modify, replay, or inject messages.

C. Decrypt a message encrypted under a key that the attacker does not possess.

D. Replay a previously captured message, even if the message is encrypted.

E. Modify a MAC-protected message without the receiver detecting the modification.

19. **[2 points]** Which of the following statements about authentication factors are TRUE?

A. A fingerprint is an example of the inherence factor (something you are).

B. A code sent by SMS to a phone is a possession factor, but it can be undermined because SMS can be rerouted through weaknesses in the SS7 signalling network.

C. A password is a possession factor because the user possesses knowledge of the password.

D. A security question such as “mother’s maiden name” is a knowledge factor whose answer may be predictable or discoverable from social networks.

E. Multi-factor authentication makes social engineering attacks impossible.

20. **[2 points]** Which of the following statements about intermediate certificates and root CAs are TRUE?

A. Most websites hold certificates signed by an intermediate CA rather than directly by the root.

B. One reason for intermediates is to delegate signing authority to another organisation or region, creating a sub-CA.

C. Keeping the root CA’s private key offline and using the intermediate’s key for day-to-day issuance means that a compromised intermediate can be revoked without replacing the root in every user’s root store.

D. In modern browsers, all pre-installed root CAs are equally trusted, so compromise of any single root CA can be used to issue a fake certificate for any domain.

E. Users individually choose which CAs to trust when they install a browser.

21. **[2 points]** Which TLS subprotocol signals that the following messages will be protected with the newly negotiated cryptographic parameters?

A. Alert Protocol

B. Change Cipher Spec Protocol

C. Record Protocol

D. Application Data Protocol

E. Handshake Protocol

22. **[2 points]** Which of the following are TRUE about TLS 1.3 compared with earlier versions of TLS? **(Select all that apply.)**

A. TLS 1.3 removed static RSA key exchange and uses ephemeral Diffie-Hellman key exchange to provide forward secrecy.

B. TLS 1.3 removed support for older, insecure cryptographic algorithms and cipher suites.

C. TLS 1.3 no longer uses certificates to authenticate servers.

D. TLS 1.3 provides confidentiality but does not provide message integrity.

E. TLS 1.3 requires a new public key to be generated for every message sent during a session.

23. **[2 points]** Two branch offices connect their LANs over the Internet using IPSec **tunnel mode** between their gateway routers. Which of the following statements are TRUE? **(Select all that apply.)**

- **A.** The entire original IP packet, including its header, is encapsulated as the payload of a new outer IP packet.
- **B.** Routers on the Internet path can read the inner IP header to make forwarding decisions.
- **C.** The outer packet may carry completely different source and destination addresses (the gateways) from the inner packet.
- **D.** Hosts inside the LANs do not need to implement IPSec themselves.
- **E.** This arrangement is the basis of a site-to-site Virtual Private Network.

24. **[2 points]** A stateful firewall performs connection tracking using the "5-tuple". Which fields make up the 5-tuple?

- **A.** Source MAC, destination MAC, protocol, source port, destination port.
- **B.** Source IP, destination IP, protocol, source port, destination port.
- **C.** Source IP, destination IP, TCP flags, interface, action.
- **D.** Source IP, destination IP, protocol, TTL, sequence number.
- **E.** Source IP, destination IP, source port, destination port, packet length.

25. **[2 points]** In the C memory model, where is memory allocated by a call to `malloc()` placed?

- **A.** The text (code) segment
- **B.** The stack
- **C.** The heap
- **D.** The data segment
- **E.** The read-only data segment

26. **[2 points]** Which of the following statements about a stack-based buffer overflow are TRUE? **(Select all that apply.)**

- **A.** The overflow can occur when a function such as `strcpy()` copies more input bytes than the buffer allocated to hold the input can accommodate.
- **B.** If 30 bytes of `0x41` are copied into a 10-byte buffer and the saved return address is reached, bytes from the input can overwrite the saved return address, potentially changing the address to which the function returns.
- **C.** A buffer used to hold input can be located within a function's stack frame, which can also contain the saved return address.
- **D.** A stack-based buffer overflow requires the buffer used for input to be dynamically allocated using `malloc()`.
- **E.** The saved return address is stored outside the stack frame, so overflowing a buffer used for input cannot affect it.

27. **[2 points]** A search page echoes the user's search term straight into the response. An attacker sends a victim a link containing `?term=<script>...</script>`; when the victim clicks it, the server includes the script in the page and the victim's browser runs it. The script is never stored on the server. Which attack is this?

- **A.** Stored XSS
- **B.** Reflected XSS
- **C.** SQL injection
- **D.** CSRF
- **E.** DOM-based XSS

28. **[2 points]** A web page loads a JavaScript library from a Content Delivery Network (CDN), which is a service that hosts and delivers files for websites. Which of the following statements are TRUE? **(Select all that apply.)**

- **A.** If the externally hosted script is replaced with a malicious copy, the including application can become vulnerable.
- **B.** Subresource Integrity (SRI) lets the browser verify the script against an expected cryptographic hash and reject it if the hash does not match.
- **C.** Loading a script from a CDN means the script is isolated from the including page and cannot access its data.
- **D.** SRI encrypts the downloaded script before it is executed by the browser.
- **E.** Content Security Policy (CSP) can specify a hash of an allowed script and block scripts that do not match an allowed hash.

29. **[2 points]** A web application passes a user-supplied field to a system `ping` command. An attacker enters `localhost;cat /etc/passwd`, and the application returns the contents of the password file. Which vulnerability class does this input exploit?

- **A.** SQL injection
- **B.** Command injection
- **C.** Stored XSS
- **D.** CSRF
- **E.** Path traversal

30. **[2 points]** Which of the following statements about RSA are TRUE? **(Select all that apply.)**

- **A.** One factor that makes RSA secure is the computational difficulty of factoring the modulus n into its two large prime factors.
- **B.** RSA remains secure regardless of key size, so 512-bit keys are still acceptable.
- **C.** Padding schemes such as OAEP are required to make RSA encryption secure in practice.
- **D.** Any two distinct prime numbers may be chosen as p and q, regardless of their size or relationship.
- **E.** RSA operations are much slower than symmetric encryption such as AES, which is why hybrid encryption schemes typically use RSA to establish or protect a symmetric key rather than encrypting large amounts of data directly.

Part 2

Written Questions

[40 points]

Answer each question in the space provided below it. Show your working for all calculations. If you run out of space, continue in the "Additional space" pages at the end of this paper and say so clearly in the original answer space.

Question 1: Public Key Cryptography [20 points]

(a) **[4 points]** Let p be a prime number. Explain what it means for an integer g to be a primitive root modulo p.

(b) **[10 points]** Suppose A and B are trying to establish a key using the Diffie-Hellman key exchange. The public parameters they are using are $p = 11$ and $g = 2$.

i If A computes their public key as 10, what is A's private key? Explain your calculation. **(2 marks)**

ii If B computes their public key as 7, what is B's private key? Explain your calculation. **(2 marks)**

iii Assuming A and B exchange their public keys, show the calculation A performs to find the shared key and calculate the shared key. **(4 marks)**

iv Assuming A and B exchange their public keys, show the calculation B performs to find the shared key and calculate the shared key. **(2 marks)**

(c) **[3 points]** Explain what *Perfect Forward Secrecy (PFS)* is in the context of cryptographic protocols.

(d) **[3 points]** Explain how the Diffie-Hellman key exchange can be used to achieve Perfect Forward Secrecy.

Question 2: Network Security [20 points]

(a) **[12 points]** A firewall sits between an internal network and the Internet. The internal network uses the public IP address range 203.10.45.0/24. The firewall has two interfaces: `inet` (connected to the Internet) and `lan` (connected to the internal network). Consider the following firewall rule table:

Rule	Iface	Src IP	Dst IP	Proto	Src Port	Dst Port	State	Action
A	inet	external	203.10.45.10	TCP	*	80	New	Accept
B	inet	external	203.10.45.10	TCP	*	443	New	Accept
C	lan	203.10.45.0/24	external	TCP	*	80	New	Accept
D	lan	203.10.45.0/24	external	TCP	*	443	New	Accept
E	lan	203.10.45.0/24	external	UDP	*	53	New	Accept
F	*	*	*	*	*	*	Est.	Accept
G	*	*	*	*	*	*	*	Drop

For each statement below, indicate whether it is **TRUE** or **FALSE** and provide a brief explanation justifying your answer. Where applicable, reference the specific rule(s) involved in your reasoning.

a) This is a stateful firewall. **(2 marks)**

b) An external host can initiate an SSH connection to any internal host on the network. **(2 marks)**

c) An internal host at 203.10.45.50 can browse HTTPS websites on the Internet. **(2 marks)**

d) The web server at 203.10.45.10 can accept incoming HTTP and HTTPS connections from the Internet. **(2 marks)**

e) An external host can send a DNS response (UDP port 53) to an internal host at 203.10.45.100. **(2 marks)**

f) An internal host at 203.10.45.20 can send a file to another internal host at 203.10.45.30 using any protocol. **(2 marks)**

(b) **[4 points]** In IPSec, there are two main security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). Briefly explain the main difference between AH and ESP in terms of the security services they provide.

(c) **[4 points]** Explain how TLS 1.3 achieves 1-RTT (one round-trip time) communication during the handshake, compared to TLS 1.2 which requires 2-RTT. In your answer, focus on the role of Diffie-Hellman key exchange parameters in the initial handshake. You may use a diagram if required.

Additional space Use this space if you need additional room for your answers. If you use it, make sure to reference it in the original answer space; otherwise, this space will not be marked.

Additional space Use this space if you need additional room for your answers. If you use it, make sure to reference it in the original answer space; otherwise, this space will not be marked.