

Information Security (CS3002)

Date: Jan 2nd 2026

Course Instructors

Ahmad Ali Shah, Ammar Haider, Aqsa Khalid,
Nosheen Manzoor, Zeeshan Ali Khan

Final Exam

Total Time (Hrs): 3

Total Marks: 85

Total Questions: 7

Student Roll No

Section

Student Signature

Instructions:

- Attempt questions **1 to 3** on this question paper, and submit it along with the answer booklet.
- If you think some information is missing, then make an assumption and state it clearly.

CLO-1	Explain key concepts of information security such as design principles, cryptography, risk management.
CLO-2	Discuss legal, ethical, and professional issues in information security.
CLO-3	Analyze real world scenarios, model them using security measures, and apply various security and risk management tools for achieving information security and privacy.
CLO-4	Identify appropriate techniques to tackle and solve problems of real life in the discipline of information security.
CLO-5	Describe issues related to ethics in the field of information security.

CLO 1

Q1: MCQs - Fill in the answer table with correct letter A to D.

[14 marks]

No credit will be awarded in case of cutting/overwriting/pencil-use.

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

- Which block cipher mode is insecure because identical plaintext blocks produce identical ciphertext blocks?
 - Cipher Block Chaining (CBC)
 - Counter (CTR)
 - Electronic Codebook (ECB)
 - Output Feedback (OFB)
- Security of RSA encryption mainly depends on the difficulty of:
 - Discrete logarithm
 - Factoring large primes
 - Hash collisions
 - XOR inversion

3. The primary drawback of using Certificate Revocation Lists (CRLs) for checking certificate validity, which led to the development of OCSP, is:
 - A) They are subject to Man-in-the-Middle (MITM) attacks during transmission.
 - B) The inability of a Certificate Authority (CA) to sign the list.
 - C) They only list certificates that have expired, not those compromised before expiration.
 - D) They are large, static files that increase client processing work and Internet traffic.
4. In a Public Key Infrastructure, Registration Authority (RA) is the logical entity responsible for:
 - A) Maintaining the trust store containing all pre-installed public keys.
 - B) Signing and publishing the X.509 Identity certificates.
 - C) Creating the Certificate Revocation List (CRL) and publishing it frequently.
 - D) Verifying identity and eligibility of certificate requester.
5. Which of the following best describes SQL injection?
 - A) Manipulating SQL statements through user input
 - B) Compressing SQL files
 - C) Creating hidden indexes
 - D) Optimizing queries automatically
6. In-band attacks cannot include which one of the following elements?
 - A) Tautology
 - B) Prepared statements
 - C) End-of-line comment
 - D) Piggybacked queries
7. In a Cross-Site Request Forgery (CSRF) attack, what does the browser automatically include in the forged request that allows the attack to succeed?
 - A) The victim's plaintext password
 - B) A secret CSRF token
 - C) The victim's session cookie
 - D) The attacker's IP address
8. Which defense against CSRF is specifically recommended for devices with limited memory?
 - A) Synchronization Token Pattern (STP)
 - B) Checking Referer header
 - C) Input validation
 - D) Output encoding
9. Authentication is primarily concerned with:
 - A) verifying a user's identity
 - B) what resources a user can access
 - C) logging user actions
 - D) encrypting user traffic
10. _____ attack tries password guesses from a list of commonly used/leaked passwords?
 - A) Dictionary
 - B) Brute-force
 - C) Challenge-response
 - D) Replay
11. Forensic analysis is mainly conducted during incident _____ phase.
 - A) detection
 - B) containment
 - C) recovery
 - D) policy review

12. Which three core questions form the foundation of security management?
- A) Who attacked, when, and how
 - B) What failed, who failed, and why
 - C) What assets, what threats, what controls
 - D) What policies, what tools, what budget
13. The primary goal of a _____ case is punishment because an illegal act harmed society, while the goal of a _____ case is restitution for the victim.
- A) civil, criminal
 - B) policy, law
 - C) legal, ethical
 - D) criminal, civil
14. Which of the following describes a key difference between Ethics and Laws?
- A) Laws are unwritten principles, Ethics are formal documents.
 - B) Laws are enforced by courts, Ethics are enforced by principles and beliefs.
 - C) Ethical principles are universal, Laws vary by culture.
 - D) Laws are idealistic, Ethics are strictly realistic.

CLO 2

Q2

[6 marks]

In Pakistan, Prevention of Electronic Crimes Act (PECA) defines several offences, some of which are listed here:

- a) unauthorized access
- b) unauthorized access to critical infrastructure systems
- c) unauthorized copy
- d) unauthorized copy of critical infrastructure data
- e) unauthorized modifications
- f) unauthorized modifications to critical infrastructure systems
- g) electronic forgery
- h) distributing and transmitting malicious code
- i) cyber stalking
- j) offence against dignity of a person

For each of the following actions, pick ONE offense from the above list that best matches the case description.

A person uses a hacking toolkit to bypass the security of NADRA databases.	b
A cyber attacker alters the configuration of a railway signaling system to cause train delays.	f
A person creates multiple fake Instagram profiles to follow and message their ex-partner.	i
A hacker intercepts a secure transmission between two businesses to steal trade secrets.	a
A person creates a fake website that looks exactly like a popular e-commerce site to harvest credit card details.	g
Someone takes a screenshot of a private, intimate conversation and shares it in a public WhatsApp group to shame the sender.	j

CLO 3

Q3

[3 + 5 + 3 + 3 + 2 + 3 marks]

- A. Consider a Public Key Infrastructure (PKI) setup consisting of three entities: a web server **W**, an intermediate certificate authority **N**, and root certificate authority **R**. Client machines trust only the root CA (**R**). However, **R** does not issue certificates directly to websites.

To be authenticated by clients, the server **W** must present a *chain* of three certificates. Provide the contents of each certificate in the table below.

	Subject	Issuer (signing entity)
Certificate 1	W	N
Certificate 2	N	R
Certificate 3	R	R (self signed)

- B. Read the following scenarios carefully and fill in the box with most-appropriate malware type.

A free software application works normally but secretly deletes user files and steals credentials.	trojan
Months after an employee is terminated, payroll data is suddenly erased.	logic bomb
Users receive fake virus alerts forcing them to download “security software”.	scareware
A malware disguises itself as a system process and participates in DDoS attacks.	zombie / bot
A malicious program spreads rapidly across a corporate network, generating excessive traffic without user involvement.	worm

- C. IPsec operates at Layer 3 and provides two operating modes. Compare these modes by stating when to use them, and a key pro and con.

IPsec mode	Primary use case	Pros	Cons
Transport	Host to host security	Computationally light	IP header fields are clearly visible
Tunnel	Gateway to gateway security	Hides actual sender / receiver	Computationally heavy

- D. You studied four risk treatment (control) strategies. Identify which one has been followed in the given circumstances?

A company decides not to encrypt a low-value internal notice board.	Acceptance
A firm outsources hosting to a cloud provider with a service-level agreement.	Transference
A budgeting app refuses bank-account integration.	Avoidance

- E. Assume that Alice, Bob, and Chris grant certain privileges on `Student` table to Joe, who in turn grants them to Peter, as shown in the following table. Numerical entries indicate the time of granting.

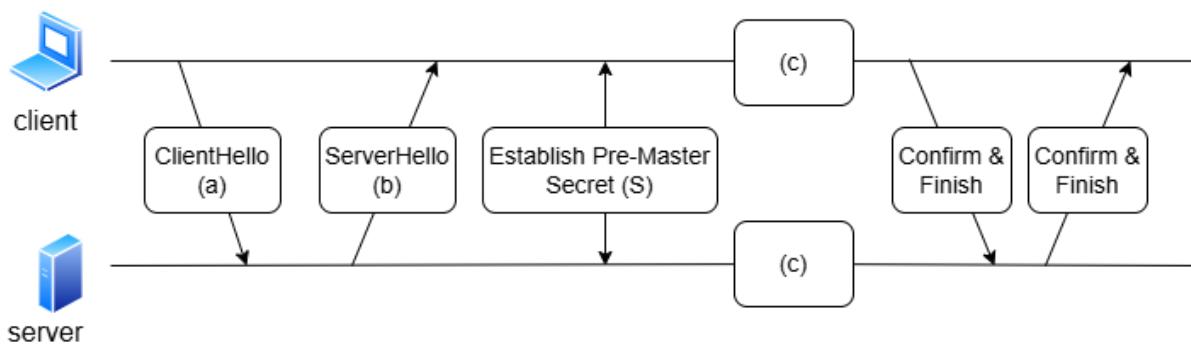
UserID	Grantor	SELECT (read)	INSERT	DELETE
Joe	Alice	10	----	10
Joe	Bob	20	20	---
Joe	Chris	30	---	30
Peter	Joe	35	---	---
Peter	Joe	---	40	---

At time t=45, Bob issues the command `REVOKE ALL PRIVILEGES ON Student FROM Joe`. Which of Peter's access rights, if any, should be revoked? Explain with reason.

Only INSERT should be revoked.
Peter also has SELECT privilege indirectly from Alice and Chris. Alice assigned that privilege before Bob (t=10), so we got to keep it.

- F. The diagram below briefly illustrates the SSL/TLS handshake process. Specify the following missing information:

Contents of ClientHello message (a)	supported ciphers, random R _{CLIENT}
Contents of ServerHello message (b)	supported ciphers, random R _{SERVER} , certificate
Operation performed by both entities at step (c)	derive Master key K = f(S, R _{CLIENT} , R _{SERVER})



CLO 1

Q4

[1 + 2 + 3 marks]

- A. A system grants access by scanning a fingerprint without prompting for a user ID. Is this biometric verification or identification?

Biometric identification

B. What is the difference between an access control list and a capability ticket?

ACL is a list of (subject, privileges) tuples assigned to a specific resource.

Ticket is a list of (asset, privileges) for a given user.

C. Cryptographic Hash Functions must possess following three security properties to be useful in applications like digital signatures and MACs. Define these properties with respect to the goal of an attacker (Eve).

- i. Preimage resistance
- ii. Second preimage resistance
- iii. Collision resistance

i. one-way property: Eve can not reverse a given digest

ii. given a (message, digest) pair, Eve can not find another message with same digest

iii. Eve can not find two messages which hash to same digest.

CLO 3

Q5

[3 + 6 + 3 marks]

A. Explain why TOTP (Time based One-Time Passcode) systems require time synchronization between the client and server. How do these systems handle minor time drift?

OTP is derived via a function that takes shared secret and current time as input. Out of sync clocks will mean different OTPs calculated at client and server.

Minor time drift is tolerated because server validates OTPs corresponding to a small time window, e.g. codes from the previous time step, the current time step, and the next time step (TC-1, TC0, TC+1) are all considered valid.

B. Consider the following screenshot of an online gaming portal where users can create profiles and play games online. In the screenshot, a user has searched for a specific type of game (zombie). The page displays search results, and the sidebar shows the Top Players of the week along with their self-described bio taglines. Based only on the information visible in the screenshot:

- i. Identify a page feature that could be vulnerable to a Reflected XSS attack. Explain how an attacker would exploit this feature.
- ii. Identify a page feature that could be vulnerable to a Stored XSS attack. Once again, also explain how an attacker would exploit this feature.

Your answer should clearly mention how the malicious script would reach and execute in a victim's browser.

The screenshot shows a web browser window with the URL www.gamingsite.com/search?query=zombies. The main content area displays "Results for ‘Zombies’" with a message stating "Found 128 games matching your search." Below this, four game thumbnails are shown: "Zombie Apocalypse" (Survival Horror), "Dead City Shooter" (Action FPS), "Zombie Defense" (Strategy), and "Undead Nightmare" (RPG Adventure). Each thumbnail includes a star rating of 4. Below the thumbnails is a navigation bar with links 1, 2, 3, 4, 5, and "Next >". To the right, a sidebar titled "Top Players This Week" lists four users: "GamerKev" (Just here to break the leaderboard 😊), "ZombieQueen" (If it moves, I shoot. If it doesn't, I loot.), "SurvivorDan" (Ctrl + Headshot + Repeat), and "NerdyMike" (Zombies fear my ping).

i.

reflected XSS might be possible via the search feature because query param in url is being reflected in page content. Attacker would craft a malicious url embedding the XSS script in query param. Victim user clicks the url link and script gets downloaded as part of the page.

ii.

stored XSS might be possible via users' bio tagline feature, since bio text is coming from user input. Attacker would write malicious script in their bio, and then try to appear in top player list so that their script gets executed in other user's browsers who are visiting the site.

C. Alice wants to use Asymmetric crypto to:

1. Send a confidential message to Bob
2. provide assurance to Bob that the message was sent by Alice and not by an imposter.

For each goal, mention

(a) the appropriate cryptographic technique (b) keys used for those operations.

1. Confidentiality → Public key encryption. Encrypt message with Bob's public key

2. Authentication → Digital signature. Sign message with Alice's private key. Verify signature with Alice's public key.

CLO 4

Q6

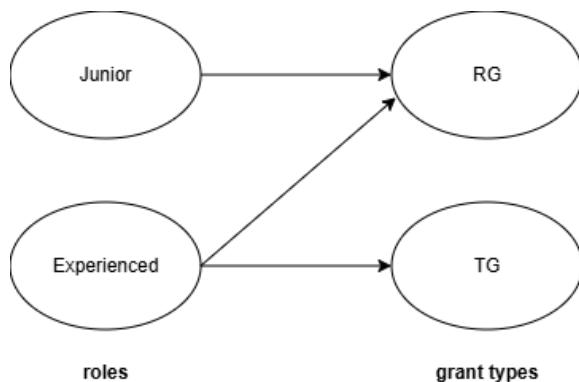
[(3 + 3) + (2 + 1 + 2) + (3 + 2) + (2 + 2) marks]

A. Consider an online system for submitting grant applications. Access to different types of funding must be controlled based on the applicant's age. The access control policy is defined as follows:

- Applicants younger than 35 years may apply only for Research Grants (RG).
- Applicants 35 years or older may apply for both Research Grants (RG) and Travel Grants (TG).
 - i. How this policy can be enforced using a Role-Based Access Control (RBAC) model? Draw a diagram showing the roles and the privileges available to each role.
 - ii. Now assume the same policy is to be enforced using an Attribute-Based Access Control (ABAC) model. Write the corresponding policy rules in Boolean expression form.

i.

create two roles, such as junior (<35) and experienced (≥ 35). An RBAC assignment will look like below



ii.

Assuming that the applicant is indicated as a and grant as g , the policy rule can be created by combining two rules as follows:

R: $\text{can_apply}(a, g, e) \leftarrow (\text{Age}(a) < 35 \wedge \text{Type}(g) \in \{\text{RG}\}) \vee (\text{Age}(a) \geq 35 \wedge \text{Type}(g) \in \{\text{RG}, \text{TG}\})$

B. An organization's network includes a web server, a database server, and multiple employee workstations. The security requirements are as follows: The web server must be accessible from the Internet. The database server must be accessible only from within the internal network. Employee workstations should be allowed to initiate outbound web browsing, but inbound connections to them must be blocked.

- i. Describe an ideal network layout that satisfies these requirements. Indicate where the web server should be placed within that layout.
- ii. Among the four types of firewalls studied in the course, identify which type is best suited for inspecting HTTP-based attacks (such as SQLi, XSS).
- iii. State ONE limitation of firewalls, regardless of their type.

i.

Org should split their network into an internal network and a DMZ that contains the web server. Two-firewall setup is ideal: one directly on Internet gateway, second in front of internal network.

ii.

application-level gateway

iii.

sample answer: can be bypassed via mobile data connections, or via pre-infected devices connecting to company network

- C. An organization has deployed an anomaly-based network-based Intrusion Detection System (NIDS) to monitor traffic between its internal network and the Internet. Over several weeks, the IDS has generated a high number of alerts including
1. repeated failed authentication attempts on internal servers
 2. high CPU and RAM usage on the database server
 3. spikes in outbound traffic during non-working hours

Additionally, the system administrators observed that not all alerts correspond to real attacks, and responding to every alert is becoming operationally expensive.

- i. Identify the types of intrusions (attacks) that each of the above alerts 1–3 may indicate.
- ii. Suggest two strategies that organization could implement to reduce IDS false positives.

i.

1: brute force login

2: DoS attack

3: data exfiltration

ii.

incorporate signature based detection, as that has fewer false positives

tune or retrain the anomaly detection engine on organization's usage pattern.

- D. Answer the following questions in reference to contingency management which involves three types of plans: Incident Response Plan (IRP), Disaster Recovery Plan (DRP), Business Continuity Plan (BCP).

- i. A flood destroys the primary data center. Backup systems are intact, but employees cannot access the office. Which plan should guide the response and why?
- ii. A company experiences a short-term server outage and immediately activates its DRP. Is this an appropriate response, or would a different action be more suitable?

i.

BCP should guide the response in this situation. This plan is designed to ensure that critical business functions continue with minimal disruption, even when primary facilities are inaccessible. Since

employees cannot physically access the office, the BCP outlines procedures for relocating staff, enabling remote work, and maintaining essential operations from alternate locations or through other means.

ii.

It is inappropriate because DRP is intended for handling major disasters where normal recovery efforts have failed. Instead, the company should first initiate an Incident Response process, which focuses on quickly diagnosing, containing, and resolving routine or temporary disruptions like short-term outages. The DRP is only triggered when the incident escalates to a level that prevents timely recovery using standard operational procedures

CLO 5

Q7

[8 marks]

A cyber security scenario is described below. Review the situation and **analyze both courses of action** based on ethical principles. Your response will be evaluated based on the strength and clarity of your arguments. Identifying the key stakeholders will help structure and support your analysis.

You are a Senior Security Engineer at a regional power company. While performing a routine audit, you discover a zero-day vulnerability that is currently being exploited by a sophisticated state-sponsored actor. The exploit is silently altering data and could lead to a total blackout. You have developed a “hot-fix” patch (software update) that can stop the attack immediately. However, your company’s policy requires a 48-hour testing window and formal sign-off from the Board before any patch is deployed. The Board is currently unreachable due to a holiday. What should you do?

Option A: Deploy the patch immediately without authorization. You save the grid but risk your job for bypassing the company authorization protocols.

Option B: Follow the protocol and wait for sign-off. You maintain the chain of command, but the attackers might cause a massive power outage in the meantime, causing losses in tens of millions to the town economy.

Open ended

- End -