

JK Lakshmipat University Jaipur
INSTITUTE OF ENGINEERING AND TECHNOLOGY
 End Term Examination, December 2025
 B. Tech. and BCA V Semester (Department Elective)

Roll No.....

CS1233: Introduction to Cyber Security

Time: 3 hours

Max. Marks: 30

Instructions to students:

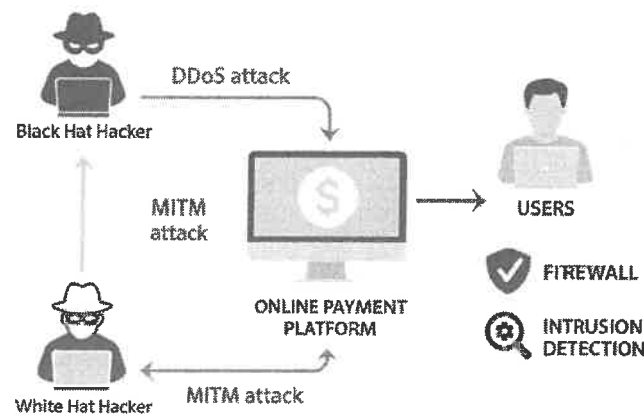
1. Scientific calculator (Non-programmable) is allowed.
2. Assume suitable data wherever required and mention it clearly.
3. Writing appropriate units, nomenclature, and drawing neat sketches/schematics/ flow chart wherever, required are an integral part of the answer.

Q.1A	Decode/decipher the following messages. i) Caesar cipher using frequency analysis ALZAPUN AV SLHYUPUN ii) Use the Columnar cipher to decipher the message TRLEELIGCIGEHALANTNCTECYENEN That was enciphered using the keyword "Analyst".	03 Marks CO4
Q.1B	Suryodaya Bank recently launched an upgraded online banking platform. To ensure customer data is protected from cyberattacks—especially during login and fund transfer—the bank decided to implement RSA public-key cryptography. Every time a customer logs in, a unique session token is generated and encrypted using RSA before being sent to the bank server. This prevents attackers from reading or modifying the data even if they capture the network traffic. RSA parameters: • $p = 71$ • $q = 67$ • $e = 23$ Credit card number encoded as integer: $M = 31$ Tasks: 1. Compute public key (e, n). 2. Compute the private key d. 3. Show Encryption 4. Show decryption process	04 Marks CO6
Q.2A	A global fintech company, FinTrust Payments, recently faced a series of sophisticated cyberattacks targeting its online transaction platform. • During a routine security audit, the White Hat security team discovered	04 Marks CO3,

unusual network traffic patterns and attempted to trace the origin.

CO5

- Meanwhile, a **Black Hat hacker group** launched a **Distributed Denial of Service (DDoS)** attack, overwhelming the payment gateway and causing severe service outages for customers.
- Taking advantage of the chaos, another group of attackers performed a **Man-in-the-Middle (MITM)** attack by intercepting communication between users and the company's mobile app, capturing session tokens and login credentials.
- As a result, several users reported unauthorized transactions, data leaks, and compromised accounts.



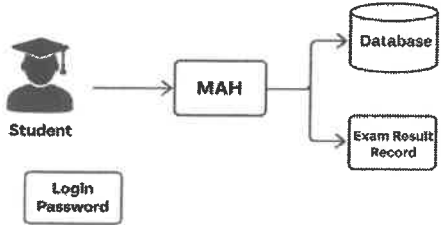
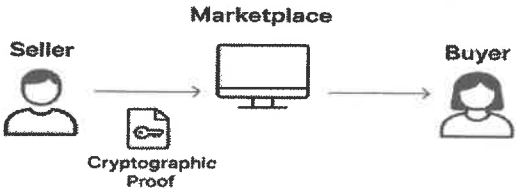
Answer followings-

- How did the attackers use a DDoS attack to disrupt FinTrust's payment services?
- What weaknesses could allow a MITM attack to succeed even when HTTPS is used?
- What immediate actions should the White Hat team take to detect and control both DDoS and MITM attacks?
- Suggest two network-level and two application-level defenses to prevent similar attacks in the future.

Q.2B A financial services company was compromised through a **targeted phishing campaign** that installed a **keylogger** on employees' systems. The attackers later deployed a **backdoor** to maintain access and extract financial data. The intrusion went unnoticed as the logs were not actively monitored.

04 Marks
CO4,
CO7

- Describe how the keylogger and backdoor worked together to steal credentials and maintain long-term unauthorized access.
- Analyze weaknesses in the email security gateway that allowed phishing emails to bypass filtering.
- Discuss how improved log monitoring, correlation, and anomaly detection could have uncovered the intrusion earlier.
- Recommend multi-layered security measures including MFA, email filtering, endpoint protection, and network monitoring.
- Explain how cyber hygiene, phishing awareness training, and periodic security assessments reduce such risks.

Q.3A	You have been hired as a cybersecurity consultant to perform a full penetration test on a newly deployed online banking portal. Describe the complete testing methodology you would follow – from initial reconnaissance to final reporting. For each phase list at least three tools you would use and explain why each tool is appropriate. Your answer should be concise, structured, and tool-focused, explaining how each step contributes to assessing the security of the banking portal.	03 Marks CO1, CO3
Q.3B	A university maintains a central database that stores student records, exam results, and login credentials. Recently, the IT audit team discovered that the database stores passwords using a weak hashing method without salting. They are now planning to implement a Message Authentication Hash (MAH) mechanism to ensure data integrity, secure authentication, and tamper-proof result records. MAH for securing university database  <pre> graph LR Student[Student] -- Login Password --> MAH[MAH] MAH --> Database[(Database)] MAH --> ExamResult[Exam Result Record] </pre> Explain how a MAC (Message Authentication code/Hash) can be used to secure: - Student login passwords - Exam result records stored in the database - Data exchanged between the application server and database server	04 Marks CO4
Q.3C	OR A large e-commerce marketplace requires all vendors to attach a cryptographic proof of authorship and integrity whenever they upload contracts, policy documents, or vendor-seller agreements on the portal. Each vendor uses a private cryptographic credential stored securely on their device to generate a unique authentication code for the document. When the document reaches the marketplace server, the system uses the vendor's public verification credential to check: Secure Contract Approval  <pre> graph LR Seller[Seller] -- Cryptographic Proof --> Marketplace[Marketplace] Marketplace --> Buyer[Buyer] </pre> Whether the document truly originated from that specific vendor	04 Marks CO3, CO5

2. Whether the document was modified at any point during upload
3. Whether the vendor can later deny having submitted that document

Task-

- Explain how the organization can ensure the integrity and authenticity of documents exchanged between employees and departments.
- Propose a secure validation mechanism that allows recipients to confirm whether a document is original or altered.
- Recommend best practices to safeguard high-value transactions and sensitive corporate files from future integrity breaches.

Q.4A	Your organization has two departments – Finance and HR – connected through the same internal network. You are asked to configure a firewall so that: • Finance systems can access the company database server. • HR systems can only access the company's internal web server. • Both departments are denied access to social media websites. Task: Design the basic firewall rules to implement the above policy. Explain the reasoning behind each rule.	04 Marks CO2, CO7
Q.4B	A smart-home IoT manufacturer wants to encrypt device logs using symmetric encryption. Their microcontrollers have limited CPU power and memory. Question Should they choose DES, AES-128 or AES-256? Explain your answer considering energy consumption, performance, and required security level.	04 Marks CO4, CO3

***** All The Best *****