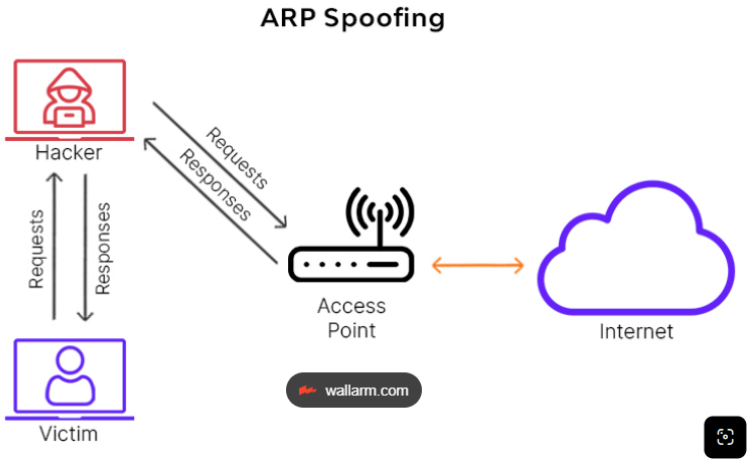
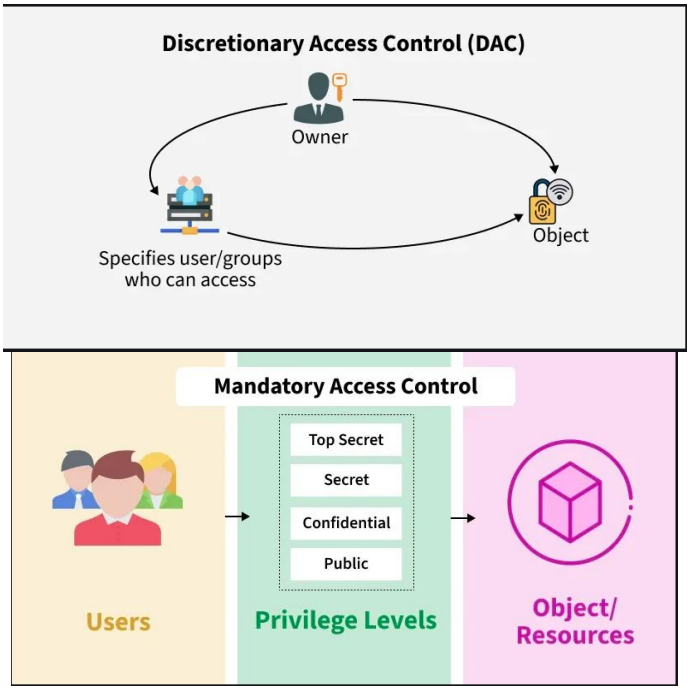
(Affiliated to University of Mumbai)	***End Semester Examination (R-24/R-25) SH 2026 Answer Key with marking scheme***
Branch: CSE IOT	Course: Cryptography and Network Security
Year/ Semester: TE/ V	Course code:CSEC501
Time: 03 hours	Marks: 80

		Marks
Q. 1	All questions are compulsory.	
A.	Describe the TCP/IP security architecture and explain the network security model with a suitable diagram. The TCP/IP security architecture protects data communication across the four layers of the TCP/IP model. **TCP/IP layer** | **Common vulnerabilities** | **Security measures** Application | DNS spoofing, application attacks | Secure application protocols, authentication Transport | TCP SYN flood, session attacks | Firewalls, rate limiting, TLS Internet | IP spoofing, packet manipulation | IPsec, packet filtering Network Access | Packet sniffing, ARP spoofing | Encryption, secure switching, network access control Network security model: A key or trusted third party may support the security transformation. The model aims to provide confidentiality, integrity, authentication and, where required, non-repudiation. • TCP/IP layers and vulnerabilities – 2 marks • Network security model and diagram – 1.5 marks • Security objectives – 1.5 mark **Marking: TCP/IP layers/vulnerabilities – 2; network security model/diagram – 1.5; security objectives – 1.5.**	5
B.	Apply the Euclidean Algorithm to find the GCD of 252 and 105. Express the GCD as a linear combination of the two numbers. **ANSWER / KEY POINTS** 252 = 2(105) + 42; 105 = 2(42) + 21; 42 = 2(21) + 0. Therefore GCD = 21. Back substitution: 21 = 105 − 2(42) = 105 − 2[252 − 2(105)] = 5(105) − 2(252). **Marking: Euclidean steps – 2; GCD – 1; linear combination – 2.**	5
C.	Explain the working of the RSA algorithm with a suitable example. **ANSWER / KEY POINTS** Choose p=3, q=11. n=pq=33; φ(n)=(p−1)(q−1)=20. Choose e=3; gcd(3,20)=1. Find	5

	d such that ed ≡ 1 (mod 20), giving d=7. Public key=(3,33); private key=(7,33). For M=4, encryption C=M^e mod n=4^3 mod 33=31. Decryption M=C^d mod n=31^7 mod 33=4. **Marking: key generation – 2; encryption – 1.5; decryption – 1.5.**	
D.	Explain the working of ARP spoofing with a suitable diagram. **ANSWER / KEY POINTS** ARP spoofing is a local-network attack in which forged ARP messages associate the attacker's MAC address with another device's IP address, often the gateway. Working: attacker sends forged ARP replies; the victim updates its ARP cache with a false mapping; traffic may be redirected through the attacker and intercepted or modified. Diagram: Victim PC ↔ Attacker ↔ Gateway/Internet; label the forged ARP reply from attacker to victim.  Countermeasures: Dynamic ARP Inspection, DHCP snooping, network segmentation, monitoring and end-to-end encryption such as TLS. **Marking: definition – 1; working – 2; diagram – 1; countermeasures – 1.**	5
E.	Define a cryptographic hash function. List the properties of a secure hash function and state the purpose of MD5 and SHA-256. **ANSWER / KEY POINTS** A cryptographic hash function maps input data of arbitrary length to a fixed-length digest. Properties: preimage resistance, second-preimage resistance, collision resistance, deterministic output and avalanche effect. MD5 produces a 128-bit digest but is cryptographically broken due to collision weaknesses; it should not be used for security-sensitive applications. SHA-256 is a SHA-2 hash producing a 256-bit digest and is used for integrity checking and in secure authentication/signature systems. **Marking: definition – 1; properties – 2; MD5 – 1; SHA-256 – 1.**	5
F.	Explain the working of Discretionary Access Control (DAC) and Mandatory Access Control (MAC) with suitable examples. **ANSWER / KEY POINTS** DAC: the resource owner decides who can access a resource and can grant/revoke permissions. Example: a faculty member shares a document with selected	5

	colleagues. MAC: a central policy enforces access using security labels and clearances; users cannot freely change the rules. Example: defence documents classified Confidential, Secret and Top Secret. DAC is owner-controlled and flexible; MAC is centrally controlled and stricter.  **Marking: DAC definition/example – 2; MAC definition/example – 2; comparison – 1.**	
Q.2A	A college wants to send confidential examination information from the examination department to the principal. To protect the message from unauthorized access, the department decides to use a Caesar cipher with a key value of 4. a) Encrypt the plaintext "EXAMINATION" using the Caesar cipher with the given key. b) Explain how the principal can recover the original message using decryption. Demonstrate the decryption process. **ANSWER / KEY POINTS** Encryption: C=(P+4) mod 26, using A=0,…,Z=25. Plaintext: E X A M I N A T I O N. Ciphertext: I B E Q M R E X M S R. Encrypted message = IBEQMREXMSR. Decryption: P=(C−4) mod 26. Shift each ciphertext letter backward by four positions (I→E, B→X, etc.) to recover EXAMINATION. **Marking: formula – 2; character-wise encryption – 4; decryption formula/process – 2; recovered plaintext – 2.**	10
	OR	
Q.2B.	A military communication unit needs to transmit an operational message securely. It uses a Vigenère cipher with the keyword "**SECURE**" to encrypt the plaintext **"ATTACKATDAWN**".	10

	a) Encrypt the plaintext using the Vigenère cipher. Show the repeated keyword and character-wise encryption steps. b) Explain how the receiver can decrypt the ciphertext using the same keyword. Demonstrate the decryption procedure. **ANSWER / KEY POINTS** Use A=0,…,Z=25. Encryption: $C_i=(P_i+K_i) \bmod 26$; decryption: $P_i=(C_i-K_i) \bmod 26$. Plaintext: ATTACKATDAWN. Repeated key: SECURESECURE. Ciphertext by character: S X V U T O S X F U N R. Ciphertext = SXVUTOSXFUNR. Subtract each repeated-key letter value modulo 26 to recover ATTACKATDAWN. **Marking: formula – 2; repeated keyword – 1; encryption steps – 4; decryption – 2; recovered plaintext – 1.**	
Q.3A	Explain the principles of block ciphers and describe the working of any two modes of operation with suitable examples. **ANSWER / KEY POINTS** A block cipher encrypts fixed-size blocks using a secret key. Its design uses substitution/permutation and aims for confusion and diffusion. ECB: each block is encrypted independently; identical plaintext blocks produce identical ciphertext blocks, revealing patterns. It is generally unsuitable for patterned data. CBC: each plaintext block is XORed with the previous ciphertext block before encryption. $C_1=E_k(P_1 \oplus IV)$; $C_i=E_k(P_i \oplus C_{i-1})$. CBC requires correct IV handling and padding; CBC alone does not provide integrity/authentication. **Marking: block-cipher principles – 2; ECB – 1.5; CBC/formula/IV – 1.5.**	5
	OR	
Q.3B	Explain the concept of Fermat's theorem and Chinese Remainder Theorem with suitable example. **ANSWER / KEY POINTS** Fermat's Little Theorem: if p is prime and p does not divide a, then $a^{(p-1)} \equiv 1 \pmod p$. Example: $3^{10} \bmod 11 = 1$. CRT: if the moduli are pairwise coprime, a system of congruences has a unique solution modulo their product. Example: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$. $x=23$ satisfies all three, so $x \equiv 23 \pmod{105}$. **Marking: Fermat statement – 1.5; example – 1; CRT statement – 1; CRT example/calculation – 1.5.**	5
Q.4A	Define public key cryptography and explain its principles. Differentiate between public and private keys. **ANSWER / KEY POINTS** Public-key (asymmetric) cryptography uses a mathematically related public/private key pair. The public key can be shared; the private key must remain secret. The recipient's public key can encrypt data that the corresponding private key decrypts. A private key can create a digital signature that is verified with the public key. Public key: shared openly; used to encrypt for the owner or verify signatures.	5

	Private key: protected secret; used to decrypt or create signatures. **Marking: definition – 1; principles – 2; comparison – 2.**	

Public Key	Private Key
1. It is shared openly with others.	1. It is kept secret by its owner.
2. It is used to encrypt data for the key owner.	2. It is used to decrypt data encrypted with the corresponding public key.
3. It is used to verify digital signatures.	3. It is used to create digital signatures.
4. It can be distributed through digital certificates.	4. It must be stored securely to prevent unauthorized access.
5. It is not required to be kept secret.	5. Its secrecy is essential for security.

Q.4 B	A college system allows students to view marks, faculty members to enter marks, and administrators to modify user accounts. Apply the RBAC model to assign suitable roles and permissions. **ANSWER / KEY POINTS** RBAC assigns permissions to roles and assigns users to roles. Student: view own marks. Faculty: enter/update marks for assigned courses. Administrator: create/modify user accounts and assign roles. The system checks whether the user's role has the requested permission. A student attempting to modify marks is denied. Apply least privilege by assigning only necessary permissions. **Marking: definition – 1; role-permission mapping – 2; access-check example – 1; least privilege – 1.**	5
	OR	
Q.4A	Explain the working of the ElGamal public key cryptosystem, including key generation, encryption and decryption. Illustrate the process with a suitable example. **ANSWER / KEY POINTS** ElGamal is an asymmetric cryptosystem based on the discrete logarithm problem. Let p=23, g=5, private key x=6. Key generation: y=g^x mod p=5^6 mod 23=8. Public key=(23,5,8); private key=6. Encrypt M=10 with random k=3: c_1=5^3 mod 23=10. Since 8^3 mod 23=6, c_2=10×6 mod 23=14. Ciphertext=(10,14). Decrypt: s=c_1^x mod p=10^6 mod 23=6. The inverse of 6 modulo 23 is 4. M=$c_2 s^{-1}$ mod p=14×4 mod 23=10. **Marking: principle/key generation – 2; encryption – 1.5; decryption – 1.5.**	5
Q.4 B	Consider a system with Confidential, Secret, and Top Secret security levels. Apply the Bell–LaPadula Model to explain whether a Secret-level user can read a Top Secret document and write to a Confidential document. **ANSWER / KEY POINTS** Bell–LaPadula protects confidentiality. Simple Security Property: "no read up"; a Secret-level user cannot read a Top Secret document.	5

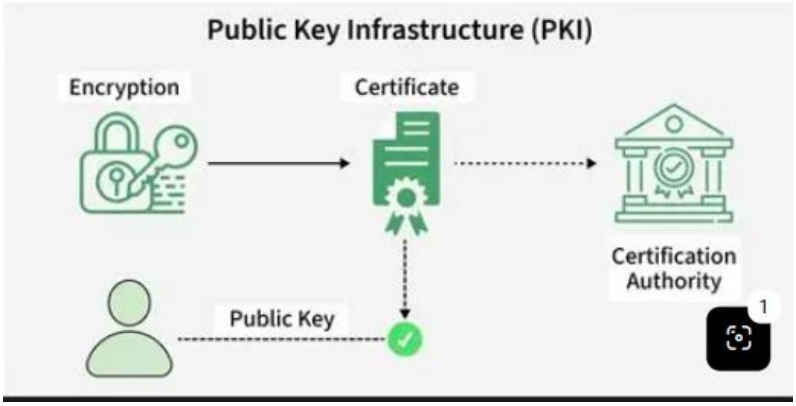
	The *-Property is "no write down"; a Secret-level user cannot write to a Confidential document under the basic model. Therefore both operations are denied. **Marking: purpose – 1; no-read-up – 1; no-write-down – 1; application to both cases – 2.**	
Q.5A	Explain the working of HMAC and CMAC. Differentiate between them based on their construction and use. **ANSWER / KEY POINTS** HMAC uses a cryptographic hash function and a secret key to provide integrity and authentication: HMAC(K,m)=H((K′⊕opad) || H((K′⊕ipad) || m)). HMAC working: hash the message with the key and inner padding; then hash that result with the key and outer padding. The receiver independently computes and compares the tag. CMAC uses a block cipher, commonly AES, and a secret key. It processes message blocks using cipher-based chaining, derived subkeys and suitable final-block handling to output an authentication tag. HMAC is hash-based (e.g. SHA-256); CMAC is block-cipher-based (e.g. AES). Both provide integrity/authentication but neither provides confidentiality alone.	10

Basis	**HMAC (Hash-based Message Authentication Code)**	**CMAC (Cipher-based Message Authentication Code)**
1. Full form	Hash-based Message Authentication Code	Cipher-based Message Authentication Code
2. Based on	Cryptographic hash functions	Symmetric block ciphers
3. Algorithms	Uses SHA-256, SHA-512, etc.	Commonly uses AES
4. Key	Uses a secret key	Uses a secret key
5. Working	Combines the secret key with a hash function to generate a MAC	Uses a block cipher and secret key to generate a MAC
6. Security purpose	Provides message integrity and authentication	Provides message integrity and authentication
7. Confidentiality	Does not provide confidentiality	Does not provide confidentiality
8. Applications	API authentication, secure communication, and message verification	Embedded systems, IoT devices, and secure communication protocols

Marking: HMAC working – 3; formula – 1; CMAC working – 3; comparison – 2; limitation – 1.

OR

Q.5B	Explain the role of X.509 digital certificates and Public Key Infrastructure (PKI) in establishing trust in digital communication	10

	ANSWER / KEY POINTS An X.509 certificate digitally binds an entity's identity to a public key and is digitally signed by a Certificate Authority (CA). Fields include subject, subject public key, issuer, serial number, validity period, signature algorithm, CA signature and extensions such as key usage or subject alternative name. PKI is the framework of policies, roles, procedures and technology used to issue, distribute, validate, renew and revoke certificates and manage public keys. Validation includes checking the certificate chain/signatures, identity or hostname, validity period, key usage and revocation status. PKI supports authentication, digital signatures and trust establishment.  **Marking: X.509 definition/fields – 3; PKI – 2; validation – 3; applications – 2.**	
Q.6A	Analyze packet sniffing, ARP spoofing, and IP spoofing based on their attack mechanisms, security impact, and countermeasures. **ANSWER / KEY POINTS** Packet sniffing captures network packets; unencrypted traffic may reveal credentials or sensitive data. Defenses: TLS, secure protocols and monitoring. ARP spoofing forges local IP-to-MAC mappings, often redirecting traffic through the attacker. Defenses: Dynamic ARP Inspection, DHCP snooping, segmentation and encryption. IP spoofing forges the source IP address. It can hide traffic origin or contribute to certain DoS attacks. Defenses: ingress/egress filtering, source-address validation and firewall controls. Comparison: sniffing observes traffic; ARP spoofing corrupts local IP-to-MAC mappings; IP spoofing forges the source IP field. **Marking: packet sniffing – 3; ARP spoofing – 3; IP spoofing – 3; comparison – 1.**	10
	OR	
Q.6B	Compare ICMP flood, TCP SYN flood, and UDP flood attacks in terms of their effects on network availability and suitable mitigation techniques. **ANSWER / KEY POINTS** DoS attacks attempt to make a system or service unavailable by exhausting resources or disrupting normal operations.	10

	ICMP flood: excessive ICMP packets consume bandwidth/processing. Mitigation: rate limiting, filtering abusive traffic and upstream DDoS protection. TCP SYN flood: many TCP SYN requests remain incomplete and exhaust connection queues. Mitigation: SYN cookies, rate limiting, queue management and DDoS protection. UDP flood: excessive UDP packets consume bandwidth and processing resources. Mitigation: rate limiting, filtering unwanted UDP traffic and upstream traffic scrubbing. The impact depends on whether bandwidth, connection state or processing capacity is exhausted. Combine monitoring, filtering, service hardening and upstream DDoS protection. **Marking: DoS definition – 1; ICMP flood – 2; SYN flood – 2; UDP flood – 2; comparison – 2; conclusion – 1.**	
*********** All the Best***********		