(Affiliated to University of Mumbai)	***End Semester Examination (R-24/R-25) SH 2026 Answer Key with marking scheme***
Branch: AIDS/AIML	Course: Cryptography and Network Security
Year/ Semester: V	Course code: MDMC5042
Time: 03 hours	Marks: 80

		Marks
Q. 1	All questions are compulsory.	
A.	• Passive attack observes/intercepts information without altering system resources; examples: eavesdropping and traffic analysis. [2 M] • Active attack modifies, disrupts, or injects data/system activity; examples: masquerade, replay, message modification and DoS. [2 M] • Clear comparison based on effect on communication/system. [1 M]	5
B.	• Since 7 is prime and gcd(3,7)=1, 3^6 ≡ 1 (mod 7). [2 M] • 100 = 6×16 + 4, so 3^100 ≡ 3^4 (mod 7). [1 M] • 3^4 = 81 ≡ 4 (mod 7). [2 M] **Answer: 4.**	5
C.	• YA = 5^6 mod 23 = 8. [2 M] • YB = 5^15 mod 23 = 19. [1 M] • A computes K = 19^6 mod 23 = 2; B similarly obtains K = 8^15 mod 23 = 2. [2 M] **Common secret key = 2.**	5
D.	• Bind an entity's identity to its public key. [2 M] • Issued/signed by a trusted Certificate Authority. [1 M] • Contain identity, public key, validity, issuer and CA signature information. [1 M] • Support authentication and trusted public-key communication/signature verification. [1 M]	5
E.	• Access Requestor (AR) – 1 M The student, faculty member, or visitor device requesting access to the college network acts as the Access Requestor. • Policy Server – 1 M The Policy Server manages identities and determines the permissions to be granted to the requesting user/device based on the defined security policy. • Network Access Server (NAS) – 1 M The NAS enforces the access decision made by the Policy Server and allows, restricts, or denies network access. • NAC Enforcement Methods – 2 M The access decision can be enforced using the following methods: • Edge Enforcement: Enforcement is performed at the network edge. • Hybrid Enforcement: Combines different enforcement approaches. • In-line Enforcement: The NAC enforcement device is placed directly in the communication path.	5

	• Protocol Enforcement: Access is enforced through network protocols.	
F.	• Application Layer: HTTP session management vulnerability → Session Hijacking. • Application Layer: DNS cache vulnerability → DNS Cache Poisoning. • Transport Layer: TCP connection establishment vulnerability → SYN Flood. • Internet Layer: IP addressing vulnerability → IP Spoofing.	5
Q.2A	Confidentiality → Data Confidentiality → Encipherment: Encrypt the confidential message before transmission so that unauthorized users cannot understand its contents. **2 M** Integrity → Data Integrity → Anti-change / Anti-replay: Ensure that the message is not modified during transmission and prevent replay of an old message. **2 M** Authentication → Peer-Entity / Data-Origin Authentication → Authentication Exchange: Verify the identity of the communicating entity and the origin of the received data. **2 M** Non-repudiation → Proof of Origin / Proof of Delivery → Digital Signature / Notarization: Provide evidence of the message origin and support non-repudiation. **2 M** Access Control → Access Control Mechanism: Ensure that only authorized users can access the communication resources. **1 M** Overall application: Select and relate the above services and mechanisms appropriately to secure the confidential communication over the insecure network. **1 M**	10
	OR	
Q.2B.	• Repeat key KEY over SECURITY: KEYKEYKE. [1 M] • Using A=0,…,Z=25: S+K=C, E+E=I, C+Y=A, U+K=E. R+E=V, I+Y=G, T+K=D, Y+E=C. [2 M] • Ciphertext = CIAEVGDC. [1 M] • Vigenère uses multiple substitution alphabets and has a larger key space than a single Caesar shift. [1 M] • Changing substitutions reduce simple frequency patterns compared with Caesar. [2 M] • Vigenère is more suitable than Caesar for the stated comparison, although classical Vigenère is not secure by modern standards. [3M]	10
Q.3A	• SubBytes: nonlinear S-box substitution; provides confusion. [2 M] • ShiftRows: cyclic row shifts; spreads bytes across columns and contributes to diffusion. [2 M] • MixColumns: combines bytes within each column; increases diffusion. [2 M] • AddRoundKey: XORs state with round key; incorporates secret-key material. [2 M] • Combined transformations provide confusion, diffusion and resistance to cryptanalysis. [2 M]	10

	OR	
Q.3B	• Initial Permutation rearranges the 64-bit input block. [2 M] • Feistel structure splits data into 32-bit halves and processes 16 rounds. [2 M] • Round function uses expansion, XOR with round key, S-box substitution and permutation; S-boxes provide nonlinearity. [2 M] • Permutation spreads S-box output and contributes to diffusion. [2 M] • Sixteen rounds repeatedly mix data and subkeys; DES nevertheless has a limited 56-bit effective key. [2 M]	10
Q.4A	**Given:** Branch A public key: $(e_A, n_A) = (7, 247)$ Branch B public key: $(e_B, n_B) = (5, 221)$ Message: M = 5 **i. Private Key of Branch A – 3 M** $n_A = 247 = 13 \times 19$ $\varphi(n_A) = (13 - 1)(19 - 1) = 12 \times 18 = 216$ Private key dA satisfies: $7\,dA \equiv 1 \pmod{216}$ Since $7 \times 31 = 217 = 216 + 1$, dA = 31 Therefore, A's private key = (dA, nA) = (31, 247) **ii. Private Key of Branch B – 3 M** nB = 221 = 13 × 17 φ(nB) = (13 − 1)(17 − 1) = 12 × 16 = 192 Private key dB satisfies: $5dB \equiv 1 \pmod{192}$ Since 5 × 77 = 385 = 2(192) + 1, dB = 77 Therefore, B's private key = (dB, nB) = (77, 221) **iii. Ciphertext sent from A to B – 4 M** Since A is sending the message to B, B's public key is used for encryption: $(e_B, n_B) = (5, 221)$. RSA encryption: $C = M^{e_B} \bmod n_B$ C = 5^5 mod 221 5^5 = 3125 3125 = 221 × 14 + 31 Therefore, C = 31 **Final Answers** A's private key = (31, 247) B's private key = (77, 221) **Ciphertext sent to B = 31**	10
	OR	
Q.4B	• e2 = e1^d mod p = 2^3 mod 11 = 8. [2 M] • C1 = e1^r mod p = 2^4 mod 11 = 5. [2 M] • C2 = P×e2^r mod p = 5×8^4 mod 11 = 9. [2 M] • Shared value S=C1^d mod p = 5^3 mod 11 = 4. [2 M] • S^-1 mod 11 = 3; P=C2×S^-1 mod 11 = 9×3 mod 11 = 5. [2 M] • Ciphertext=(5,9); recovered plaintext=5.	10
Q.5A	• Client requests authentication/service access from Authentication Server(AS). [2 M]	10

	• AS verifies the user and issues a Ticket Granting Ticket (TGT). [2 M] • Client presents TGT to Ticket Granting Server (TGS) for a service ticket. [2 M] • TGS issues a service ticket and session-key information. [2 M] • Client presents service ticket to server; server verifies it and establishes authenticated secure access. [2 M]	
	OR	
Q.5B	• MAC is a general message-authentication mechanism using a secret key; provides integrity and authentication. [2 M] • HMAC is hash-based and combines a secret key with a cryptographic hash function. [2 M] • CMAC is block-cipher-based and is suitable where a secure block cipher such as AES is available. [2 M] • Compare construction: HMAC→hash based; CMAC→block-cipher based; both use secret keys. [2 M] • Recommendation must match the application: HMAC is a strong general choice with a secure hash; CMAC is suitable where block-cipher infrastructure is already used. [2 M]	10
Q.6A	• Need: secure channel for confidentiality, server authentication and integrity of banking communication. [2 M] • ClientHello: proposes protocol/cipher parameters and sends client random. [1 M] • ServerHello: selects parameters, sends server random and certificate. [2 M] • Client verifies certificate and the key-exchange process establishes secret/session-key material. [2 M] • Change Cipher Spec/Finished messages confirm the handshake and both sides use established session parameters. [2 M] • Application data is then protected using the established secure session. [1 M]	10
	OR	
Q.6B	• Individual host-to-host communication → Transport Mode. [2 M] • Transport Mode protects the IP payload while retaining the original IP header. [2 M] • Communication between two complete networks/VPN → Tunnel Mode. [3 M] • Tunnel Mode encapsulates and protects the complete original IP packet inside a new IP packet with an outer IP header. [3 M]	10
	********* **All the Best**********|	