MITE
Invent Solutions

MANGALORE INSTITUTE OF TECHNOLOGY & ENGINEERING

(A Unit of Rajalaxmi Education Trust®, Mangalore)
Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE, New Delhi
Accredited by NAAC with A+ Grade & ISO 9001:2015 Certified Institution

Model Question Paper

Second Semester MCA Degree Examination

Network Security

Time: 3 Hours **Max. Marks: 100**

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M: Marks, L: RBT (Revised Bloom's Taxonomy) level, C: Course outcomes.

		Module -1	M	L	CO
Q1	a.	A student accesses their bank account using a free campus Wi-Fi network. During this session, an attacker secretly captures the transmitted data packets without altering or modifying the data. Based on the scenario, answer the following: a) Identify the attack. b) Justify your answ er by explaining why this attack falls under that category. c) Suggest any two prevention techniques to protect against such attacks.	10	L3	CO1
	b.	Make use of the Caesar Cipher technique to encrypt the plain text given : Plain Text**:** SECURE YOUR ONLINE DATA a) Show the step-by-step encryption process using a suitable shift value. b) Write down the working principle of the Caesar Cipher technique. c) What type of encryption does it represent? d) Mention its strengths and limitations.	10	L3	CO1
		OR			
Q2	a.	A company uses AES in Cipher Block Chaining (CBC) mode to secure file transmissions over its internal network. Draw and label the block diagram of CBC mode for both encryption and decryption. Describe the role of the Initialization Vector (IV) and explain how ciphertext blocks are generated.	10	L3	CO1
	b.	Encrypt the given plaintext using the Vigenère given the following attributes. Plain Text : MEET ME NOW KEY :KEY Write down the advantages of using Vigenère Cipher over Caesar Cipher for this message in terms of resistance to frequency analysis.	10	L3	CO1
		Module- 2			
Q3	a.	In the Advanced Encryption Standard process, the following state matrix and round key : $\begin{bmatrix} 54 & 68 & 61 & 74 \\ 73 & 20 & 6D & 79 \\ 20 & 4B & 75 & 6E \\ 67 & 20 & 46 & 75 \end{bmatrix}$ $\begin{bmatrix} 0A & 0B & 0C & 0D \\ 0E & 0F & 00 & 01 \\ 02 & 03 & 04 & 05 \\ 06 & 07 & 08 & 09 \end{bmatrix}$ a) Perform the AddRoundKey transformation (XOR operation). b) Show the resulting state matrix.	10	L3	CO2

	B.	A bank is designing a secure online communication system for its customers using public-key cryptography. The system should protect transaction data from unauthorized access while also ensuring that customers can verify that they are communicating with the legitimate bank server and not an attacker. Analyze the key requirements that the cryptographic system must satisfy to ensure both confidentiality and authentication.	10	L3	CO2
		OR			
Q4	a.	Apply the ShiftRows transformation to the given 4×4 state matrix as per the AES encryption standard. $\begin{bmatrix} 9 & 13 & 5 & 2 \\ 1 & 11 & 7 & 6 \\ 3 & 7 & 4 & 1 \\ 6 & 0 & 7 & 10 \end{bmatrix}$ Explain the purpose and working of the **ShiftRows** transformation in the AES encryption process.	10	L3	CO2
	b.	Using the RSA Algorithm, two prime numbers p=3 and q=11 are selected and the plaintext message to be transmitted is M=4. **Based on the above information, answer the following:** a) Generate the public and private keys by computing n, $\phi(n)$, choosing a suitable e, and finding d. b) Encrypt the given message using the RSA encryption process. c) Decrypt the ciphertext and verify that the original message is obtained. d) Show all steps involved in both encryption and decryption processes.	10	L3	CO2
		Module – 3			
Q5	a.	An online learning platform stores student records, including personal and academic details, on cloud servers. With growing concerns about data breaches, the organization wants to implement stronger data protection mechanisms. How backup, encryption, and data masking can be used to secure the data. Mention the approach that balances data security and system efficiency.	10	L3	CO3
	b.	A web application uses HTTPS for most pages, but the login form submits user credentials over HTTP. Analyze the security risks associated with this design. List down the restructuring plan to ensure secure data transmission while maintaining performance and usability.	10	L3	CO3
		OR			
Q6	a.	An organization wants to enforce different levels of network access based on the role of users and the type of device they connect from. Design a policy-driven NAC framework that dynamically adjusts access rights. Justify your approach by explaining how role-based and context-aware access enhances network security.	10	L3	CO3
	b.	A hospital stores patient health records on a cloud infrastructure. Due to rising ransomware threats, the IT team wants to enhance data protection. Mention the role of backup, encryption, and data masking techniques in protecting sensitive health data in cloud environments. Recommend a solution that balances security and performance.	10	L3	CO3
		Module – 4			
Q7	a.	An organization is planning to implement Kerberos for secure authentication across its enterprise network. Explain the key components involved in Kerberos authentication and evaluate how each component contributes to preventing unauthorized access and ensuring secure communication.	10	L3	CO4

	b.	A healthcare provider uses fingerprint authentication on mobile devices for accessing patient records. The staff complain about false rejections and delays. Evaluate the usability and security trade-offs in biometric user authentication. Suggest an alternative or complementary authentication approach that enhances both accuracy and user acceptance.	10	L3	CO4
OR					
Q8	a.	A legacy banking system employs symmetric-key authentication for ATM-user communication. Attackers are suspected to be replaying valid requests to gain unauthorized access. Identify how replay attacks exploit weaknesses in symmetric authentication. Suggest a secure protocol design that addresses authentication freshness and integrity.	10	L3	CO4
	b.	A financial services company provides its clients with online access to manage investments from anywhere in the world. Explain the principles of remote user authentication, assess how these principles help protect against identity theft and session hijacking, and recommend a multi-layered authentication strategy tailored to high-value financial transactions.	10	L3	CO4
Module – 5					
Q9	a.	An organization distributes invoices via email using MIME attachments, but some recipients are unable to open the attachments or receive corrupted files. Analyze the issues related to MIME encoding and client compatibility. How to measures the reliability and security in email attachment delivery.	10	L3	CO5
	b.	A government agency requires a system where emails cannot be altered during transmission and the sender cannot deny sending the message. Examine how digital signatures in S/MIME or Pretty Good Privacy achieve these goals.	10	L3	CO5
Q10	a.	A company's email system is compromised due to DNS spoofing, redirecting users to malicious servers. Evaluate how this attack affects email security. Recommend how DNS Security Extensions can be used to prevent such threats.	10	L3	CO5
	b.	A financial institution transmits sensitive data across an untrusted network. The organization wants to ensure both encryption and integrity of packets. Evaluate how Encapsulating Security Payload (ESP) provides these services. Recommend whether transport mode or tunnel mode is more suitable.	10	L3	CO5

-*****-