USN | | | | | | | | | | |

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

Sixth Semester B.E Degree Examination Odd Term 2025-26

Model Question Paper

Cryptography and Network Security 23ICPE321

Time: 3 Hours (180 Minutes) **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	C
Q1	a.	Explain Playfair Cipher and list out all the rules. Use **your name** (Ex: Alice, Bob, Eve..) as keyword, encrypt the phrase **"plan and execute"** using Playfair cipher.	7	L3	1
	b.	Encrypt and decrypt the plaintext "**MITE**" using HILL cipher with given key. Show the calculation and cipher text. [Hint: a=0, b=1…….z=25]. Key : $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$	7	L3	1
	c.	Explain how the Vigenère Cipher improves security against frequency analysis compared to a simple Caesar Cipher.	6	L3	1
		OR			
Q2	a.	Explain the General Model for Network Security with a neat diagram. Identify the four basic tasks in designing a particular security service.	7	L3	1
	b.	Describe the overall steps of the Data Encryption Standard (DES) algorithm with a neat diagram.	7	L3	1
	c.	Describe the design of a Traditional Feistel Block Cipher. Explain why the decryption process in a Feistel network is essentially the same as the encryption process.	6	L3	1
		Module- 2			
Q3	a.	Explain the Linear Congruential Generator (LCG) method for generating pseudorandom numbers using the formula Xn+1=(aXn+c)mod m. Discuss the significance of selecting appropriate values for a, c, and m to achieve a long period."	7	L3	2

	b.	Given p = 11, q = 19, and a seed s = 3, calculate the first 4 bits generated by the Blum Blum Shub algorithm. Explain why BBS is considered cryptographically secure compared to LCG.	7	L3	2
	c.	Illustrate with a diagram how a Man-in-the-Middle attack is executed against the Diffie-Hellman protocol.	6	L3	2
OR					
Q4	a.	In an RSA system, a user chooses two prime numbers p = 7 and q = 11. • Determine the public key (e, n) if e = 13. • Find the private key d. • Encrypt the message M = 5	7	L3	2
	b.	Diffie-Hellman Key Exchange Alice and Bob agree on a prime q = 23 and a primitive root α= 5. • If Alice chooses private key X_A = 6, calculate her public key Y_A. • If Bob chooses private key X_B = 15, calculate his public key Y_B. • Calculate the shared secret key K	7	L2	2
	c.	Explain the algebraic structure of an Elliptic Curve over a finite field E_p(a, b). Define the "Elliptic Curve Discrete Logarithm Problem" (ECDLP)	6	L3	2
Module – 3					
Q5	a.	Identify and explain four major applications of cryptographic hash functions in network security. Specifically, discuss how they are used for Password Storage, Data Integrity, Digital Signatures, and Intrusion Detection.	7	L3	3
	b.	Distinguish between Direct Digital Signatures and Arbitrated Digital Signatures. Explain the role of a "Trusted Third Party" in preventing disputes between the sender and receiver.	7	L3	3
	c.	Demonstrate how simple hash functions work by calculating a 4-bit hash for the message `1101 0011 1010` using: Bit-by-bit XOR across blocks.	6	L3	3
OR					
Q6	a.	Illustrate how asymmetric encryption (like RSA) is used to solve the "key exchange problem" for symmetric systems.	7	L2	3
	b.	List and explain the essential fields found in an X.509 Certificate. Focus on the Version, Serial Number, Issuer Name, Validity Period, and the Subject's Public Key information.	7	L2	3
	c.	Define PKI and its core components: The Certificate Authority (CA), Registration Authority (RA), and Certificate Revocation List (CRL).	6	L2	3
Module - 4					

Q7	a.	Explain the five services provided by PGP: Authentication, Confidentiality, Compression, Email Compatibility (Radix-64), and Segmentation. Why does PGP perform compression before encryption?	10	L2	4
	b.	Illustrate the full message exchange between a User, the Authentication Server (AS), and the Ticket Granting Server (TGS). Explain why the TGS is necessary instead of the User just getting a service ticket directly from the AS.	10	L3	4
OR					
Q8	a.	What is S/MIME? Explain the functions it provides, such as Enveloped Data, Signed Data, and Clear-signed Data. How does S/MIME differ from standard PGP in terms of key certification?	10	L2	4
	b.	Identify and explain four major threats to email communication: Message Alteration, Spam, Phishing, and Eavesdropping. How does encryption address these specific concerns?	10	L3	4
Module - 5					
Q9	a.	Explain Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE) with suitable diagrams.	10	L2	5
	b.	Describe ESP header format, encryption process, authentication, and its advantages over AH.	10	L3	5
OR					
Q10	a.	Describe the Internet Key Exchange (IKE) protocol. Explain its phases, key management process, and negotiation mechanism.	10	L3	5
	b.	Compare Transport Mode and Tunnel Mode in IPSec. Illustrate with neat diagrams and suitable examples.	10	L3	5

-*****-