

Day & Date:19/09/2025, Friday

Time: 10.15 am-12.15 pm

Max Marks-50

Instructions: 1) All questions are compulsory.

2) Figures in rounded () brackets within the question, indicate the scheme of marking for respective part of the question, whereas, figures in the first right column indicate total marks for that whole question.

3) CO is the index number of the Course Outcome statement.

4) The Bloom's taxonomy level (BL) for 1,2,3,4,5 and 6 is remember, understand, apply, analyze, evaluate and create respectively.

5) Assume suitable data if necessary.

6) Use of non-programmable calculators is allowed

			Marks	BT Level	COs
Q.1	A	Differentiate between the Substitution & Transposition Techniques. (4M+4M)	08	BL4	CO3
	B	What is a Caesar Cipher (2M)? Explain Caesar Cipher with a suitable example (3M). Describe the advantages and disadvantages of using the Caesar Cipher in cryptography (3M)	08	BL2	CO1
		OR			
	B	Explain with examples the types of attack, insider and outsiders. (4M+2M+2M)			
Q.2	A	Explain the Symmetric Cipher Model.	08	BL2	CO1
		OR			
	A	Explain Following modes of Operation - Electronic Codebook Mode (ECB) (4M) - Cipher Block Chaining Mode (CBC) (4M)			
	B	Differentiate between Data Encryption Standard (DES) and Advanced Encryption Standard (AES) (4M+4M).	08	BL4	CO3
Q.3	A	Explain RSA Algorithm (3M). Using the RSA algorithm with p=3 q=11, and e=3, generate the public and private keys.	10	BL3	CO5



Then, encrypt the message $M=4$ and show the decryption process step by step to recover the original message (7M)

OR

- A Explain Diffie Helleman Key exchange algorithm (3M). Using the Diffie–Hellman key exchange algorithm, let the prime number $p=7$ and primitive root $g=3$. If user A chooses a private key $a=6$ and user B chooses a private key $b=4$, compute the public keys of A and B, and then show how both arrive at the same shared secret key (7M)
- B What is Public Key Cryptography(2M)? Explain how to apply the Public key Cryptography to achieve the Confidentially, Authentication and Both (6M). **08** BL4 CO2

