Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER–V EXAMINATION – WINTER 2025

Subject Code:3154501 Date:02-12-2025

Subject Name:Cryptography and Network security

Time:10:30 AM TO 01:00 PM Total Marks:70

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

			MARKS
Q.1	**(a)**	Define Cryptography and Cryptanalysis. Draw conventional cryptosystem.	**03**
	(b)	List and explain various types of attacks on encrypted message.	**04**
	(c)	Explain single round function of DES with suitable diagram.	**07**
Q.2	**(a)**	Differentiate Symmetric and Asymmetric key cryptography.	**03**
	(b)	Use playfair algorithm with key “monarchy” and encrypt the text “crypt tool”.	**04**
	(c)	Explain various steps of AES with diagram.	**07**
		OR	
	(c)	Which security goal is achieved with SHA-1 algorithm? Explain steps of SHA-1.	**07**
Q.3	**(a)**	Explain rail fence Cipher technique	**03**
	(b)	Explain the terms diffusion and confusion.	**04**
	(c)	Explain NIST digital Signature algorithm	**07**
		OR	
Q.3	**(a)**	Differentiate session key and master key.	**03**
	(b)	Explain different characteristics of hash function.	**04**
	(c)	List various modes of operations in block cipher encryption and explain any two.	**07**
Q.4	**(a)**	Explain Euler’s totient function with example.	**03**
	(b)	P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm?	**04**
	(c)	What is a nonce? Explain the key distribution scenario if A wishes to establish logical connection with B (A and B both have a master key shared with KDC).	**07**
		OR	
Q.4	**(a)**	Discuss the triple DES scheme with two keys and its limitations.	**03**
	(b)	Explain Encryption and decryption in RSA algorithm.	**04**
	(c)	Explain Deffie Hellman key exchange scheme in detail.	**07**
Q.5	**(a)**	Write the elements of X.509 certificates.	**03**
	(b)	What steps sending PGP(pretty good privacy) perform?	**04**
	(c)	Explain Kerberos in detail.	**07**
		OR	
Q.5	**(a)**	Describe various ways to distribute public key in public key cryptography.	**03**
	(b)	Explain the secure socket layer handshake protocol action.	**04**
	(c)	How encapsulating security payload help in IP security? Explain various fields in Encapsulating security payload packet.	**07**

****