Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI EXAMINATION – SUMMER 2025

Subject Code: 3161606 Date: 22-05-2025

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 the following (i)Denial of Service (ii)Masquerade (iii) Non-repudiation	**03**
	(b)	Differentiate between Brute force and cryptanalysis.	**04**
	(c)	What are the various types of security attacks? Explain them in detail.	**07**
Q.2	**(a)**	Use play fair cipher technique to encrypt the message “beauty lies in the eyes of a beholder” with the key “Monarchy”	**03**
	(b)	Hill cipher key is |17 17 5 | |21 8 21 | |2 2 19 | Encrypt “paymoremoney”	**04**
	(c)	Distinguish between transposition and substitution methods with examples	**07**
		OR	
	(c)	List down various modes of operations of block cipher and Explain ECB, OFB and COUNTER modes briefly.	**07**
Q.3	**(a)**	On what criteria the strength of DES algorithm depends? Explain with reason.	**03**
	(b)	Compare public key cryptography with private key cryptography in detail.	**04**
	(c)	Explain Key Expansion in AES algorithm.	**07**
		OR	
Q.3	**(a)**	Explain meet in the middle attack in DES.	**03**
	(b)	Explain timing attack in RSA.	**04**
	(c)	Explain single round function in DES algorithm.	**07**
Q.4	**(a)**	What is SHA? Why it is needed in cryptography? Explain.	**03**
	(b)	In RSA system, the public key of a user is e=7, p=17, q=11. What is the private key of this user? Also decrypt the message 11 using private key.	**04**
	(c)	Explain Diffie Hellman algorithm with example.	**07**
		OR	
Q.4	**(a)**	Define unconditionally secure cipher? Why one-time pad cipher is unconditionally secure?	**03**
	(b)	Write the Euclid’s algorithm and show the steps of Euclid’s algorithm to find gcd(1970,1066).	**04**
	(c)	Define KDC? Explain key distribution with diagram.	**07**
Q.5	**(a)**	Explain X.509 authentication service in brief.	**03**
	(b)	Explain Secure Socket Layer.	**04**

	(c)	Explain SHA1 hashing algorithm in detail.	**07**
		OR	
Q.5	**(a)**	Differentiate MAC and Hash function?	**03**
	(b)	Explain Digital signature. What requirements should a Digital signature scheme satisfy?	**04**
	(c)	Explain Kerberos protocol in details.	**07**

****