Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER– VII EXAMINATION – SUMMER 2026

Subject Code:2170709 Date:03-06-2026

Subject Name:Information and Network Security

Time:02:30 PM TO 05:00 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 Confidentiality, Integrity and Avaibility	**03**
	(b)	Briefly explain any two active security attacks.	**04**
	(c)	Explain playfair cipher substitution technique in detail. Find out cipher text for the following given key and plaintext. Key=ENGINEERING, Plaintext=COMPUTER	**07**
Q.2	**(a)**	Explain one time pad cipher with example.	**03**
	(b)	Explain columnar transposition Cipher technique.	**04**
	(c)	Explain single round of DES algorithm. Support your answer with neat sketches.	**07**
		OR	
	(c)	Briefly describe Mix Columns and Add Round Key in AES algorithm.	**07**
Q.3	**(a)**	State the differences between chosen plain text and chosen cipher text attack.	**03**
	(b)	Write a short note on Man-in-the-middle attack.	**04**
	(c)	Discuss Diffie-Hellman key exchange algorithm in detail.	**07**
		OR	
Q.3	**(a)**	What is the purpose of the S-boxes in DES? Explain the avalanche effect.	**03**
	(b)	Encrypt the message "meet me at the usual place " using the Hill cipher with the key (9 4 5 7)	**04**
	(c)	Explain RSA algorithm in detail with suitable example.	**07**
Q.4	**(a)**	Explain counter mode of DES operation.	**03**
	(b)	Explain public key cryptosystem with neat diagram.	**04**
	(c)	Explain the logic of SHA (Secure Hash Algorithm).	**07**
		OR	
Q.4	**(a)**	Explain cipher feedback mode of DES operation.	**03**
	(b)	Explain key distribution process using Key Distribution Center (KDC).	**04**
	(c)	Write the algorithm for message authentication code (MACs) based on HASH functions.	**07**
Q.5	**(a)**	Which types of security threats are faced by user while using the web?	**03**
	(b)	Explain MAC code generation using block cipher.	**04**
	(c)	Write a short note on “Digital Signature Algorithm”.	**07**
		OR	
Q.5	**(a)**	What is defined by X.509 certificate? Write the process of authentication in X.509.	**03**
	(b)	Explain Difference between Asymmetric and Symmetric Key.	**04**
	(c)	Explain SSL architecture.	**07**

****