Seat No./Enrollment No.: _____

GUJARAT TECHNOLOGICAL UNIVERSITY
BACHELOR OF ENGINEERING – SEMESTER 7 – EXAMINATION – SUMMER 2026

Subject Code: 3174902 **Date: 22/05/2026**

Subject Name: NETWORK SECURITY AND CRYPTOGRAPHY

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.**

Q.1	**(a)**	Define the following terms: (i) Security Attack (ii) Security Services (iii) Security Mechanism.	**03**
	(b)	List advantages of asymmetric cryptography over symmetric key cryptography.	**04**
	(c)	List and explain various types of attacks on encrypted messages.	**07**
Q.2	**(a)**	Explain avalanche effect.	**03**
	(b)	Explain Vigenere cipher algorithm with example.	**04**
	(c)	Explain steps in the various rounds of DES.	**07**
		OR	
Q.2	**(c)**	Elaborate AES encryption with neat sketches.	**07**
Q.3	**(a)**	Discuss meet-in-the-middle attack.	**03**
	(b)	What is limitation of ECB? How CBC overcomes it?	**04**
	(c)	Explain RSA algorithm and compute keys with p=53, q=59, e=3.	**07**
		OR	
Q.3	**(a)**	List uses of public key cryptography.	**03**
	(b)	Discuss Cipher Feedback (CFB) block cipher mode with diagram.	**04**
	(c)	For Diffie-Hellman: prime=23, g=9, A=4, B=3: compute public keys and secret key.	**07**
Q.4	**(a)**	Define weak collision resistance and strong collision resistance.	**03**
	(b)	What are requirements for a cryptographic hash function?	**04**
	(c)	Explain with diagrams basic uses of MAC.	**07**
		OR	
Q.4	**(a)**	Why is SHA more secure than MD5?	**03**
	(b)	Explain pre-image resistance and second pre-image resistance.	**04**
	(c)	Explain Message Digest Generation Using SHA-512.	**07**
Q.5	**(a)**	Explain authentication mechanism of Kerberos.	**03**
	(b)	Discuss the security of digital signature.	**04**
	(c)	What is key distribution? Give one method with illustration.	**07**
		OR	

Q.5

(a) Role of Key Distribution Centre and techniques for public key distribution. **03**

(b) How can public key cryptography be used for digital signature? Explain. **04**

(c) Discuss X.509 Certificates. **07**

*****