Seat No./Enrollment No.: _____

GUJARAT TECHNOLOGICAL UNIVERSITY
MASTER OF COMPUTER APPLICATIONS – SEMESTER 3 – EXAMINATION – SUMMER 2026

Subject Code: MC03094101 **Date: 07/05/2026**

Subject Name: INFORMATION 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. **Use of simple calculators and non-programmable scientific calculators are permitted.**

Q.1	**(a)**	Give full form of CIA and AAA. Explain both in detail with suitable examples.	**07**
	(b)	Explain difference between substitution ciphers and transposition ciphers. Explain two methods of transposition cipher.	**07**
Q.2	**(a)**	Compare stream cipher and block cipher.Write a short note on AES with suitable diagrams.	**07**
	(b)	Explain double DES and triple DES (with two keys and three keys) with neat diagrams.Also explain avalanche effect in DES.	**07**
		OR	
Q.2	**(b)**	List out modes of operation for block cipher.Compare encryption and decryption block diagrams of any three modes.	**07**
Q.3	**(a)**	Compare private key encryption and public key encryption. Write a short note on man in the middle attack.	**07**
	(b)	Briefly explain Diffie Hellman Key exchange. Calculate the shared secret (KA and KB) key using Diffie Hellman Key Exchange Algorithm. Take Prime number(q)=13, Primitive root(α)=6, Private key for party A(XA)=5 and Private key for party B(XB)=4.	**07**
		OR	
Q.3	**(a)**	Explain cryptanalysis. Enlist and explain the requirements of Public Key Cryptography.	**07**
	(b)	Discuss RSA Algorithm. P and Q are two prime numbers.P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 10, then what will be cipher text value according to RSA algorithm?	**07**
Q.4	**(a)**	Compare Hash function, Message authentication code and Digital signature.Write a short note on basics of Hash function and its properties.	**07**
	(b)	Give full form of HMAC. Discuss HMAC structure in detail with required diagrams and equations..	**07**
		OR	
Q.4			

	(a)	Write a short note on Digital Signature and its properties. Explain with block diagram.	**07**
	(b)	Explain SHA-1 message digest algorithm with required diagram and equations.	**07**
Q.5	**(a)**	Explain ESP and AH protocol with tunnel mode and transport mode in IPSec.	**07**
	(b)	Write short note on possible states of port determined by NMap.	**07**

OR

Q.5	**(a)**	Explain need of DHCP. Also explain its working with example.	**07**
	(b)	Write a short note on firewall and its types and compare working of packet filtering firewall and stateful packet inspection firewall .	**07**

*****