Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER–VII EXAMINATION – WINTER 2025

Subject Code:3170720 Date:01-12-2025

Subject Name:Information 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 substitution technique in cryptography. List various substitution technique and discuss any one with an example.	**03**
	(b)	What is the objective of attacking an encryption system? Write the two approaches to attack a conventional encryption scheme.	**04**
	(c)	List various modes of operations of block cipher. Explain any three of them briefly.	**07**
Q.2	**(a)**	Define 1) Authentication 2) Data integrity 3) Data Confidentiality	**03**
	(b)	Construct a Playfair matrix with the key “engineering”. And encrypt the message “test this process”.	**04**
	(c)	Describe the Diffie-Hellman Key Exchange algorithm and how it enables secure key exchange between two parties. Explain the man-in-the-middle attack and how it can compromise the security of Diffie-Hellman.	**07**
		OR	
	(c)	Discuss RSA algorithm, focusing on its computational aspects and security. Discuss how public and private keys are generated and used in encryption and decryption.	**07**
Q.3	**(a)**	What is the purpose of the State array? How many bytes in State are affected by ShiftRows?	**03**
	(b)	Explain the following properties of hash function (i) One way property (ii) Weak collision resistance	**04**
	(c)	Explain the structure of the Advanced Encryption Standard (AES), its transformation functions, and the key expansion process.	**07**
		OR	
Q.3	**(a)**	How does a Message Authentication Code (MAC) ensure message integrity and authenticity?	**03**
	(b)	What is the difference between direct and arbitrated digital signature?	**04**
	(c)	Briefly describe the main components of the Data Encryption Standard (DES) algorithm.	**07**

Q.4	**(a)**	Briefly define the monoalphabetic cipher.	**03**
	(b)	Describe the Elgamal digital signature schemes.	**04**
	(c)	Discuss Kerberos as a secure authentication protocol. Explain its key components and how it protects against replay attacks.	**07**

OR

Q.4	**(a)**	What are the essential ingredients of a symmetric cipher?	**03**
	(b)	Describe the Schnorr digital signature schemes.	**04**
	(c)	Explain the process of remote user authentication using symmetric encryption. How does it ensure secure communication between parties?	**07**
Q.5	**(a)**	What is a nonce? What is the difference between a session key and a master key?	**03**
	(b)	Discuss key expansion process of DES algorithm.	**04**
	(c)	Discuss the Secure Hash Algorithm (SHA) family. Explain how SHA functions are used in ensuring data integrity and their role in cryptographic applications.	**07**

OR

Q.5	**(a)**	Explain the avalanche effect.	**03**
	(b)	Briefly describe the role of X.509 certificates in secure communication.	**04**
	(c)	What is public key cryptography? Explain the concept behind the public key cryptography and Compare it with conventional cryptography.	**07**

****