Enrolment No./Seat No_______________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER–VII (NEW) EXAMINATION – WINTER 2024

Subject Code:3170720 **Date:16-12-2024**

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 following: i. Cryptography ii. Sniffing iii. Spoofing.	**03**
	(b)	Encrypt the following message using playfair cipher. Text: “you keep smiling” and security Keyword: “happiness”.	**04**
	(c)	List and explain various types of attacks on encrypted message.	**07**
Q.2	**(a)**	What is the purpose of S-boxes in DES?	**03**
	(b)	Explain encryption and decryption of RSA algorithm.	**04**
	(c)	DES algorithm is secure or not. Justify your answer.	**07**
		OR	
	(c)	Explain in detail single round of AES algorithm.	**07**
Q.3	**(a)**	What are the problems with one-time pad? Explain with suitable example.	**03**
	(b)	Distinguish between passive and active security attacks.	**04**
	(c)	Explain Diffie-Hellman algorithm with suitable example. What are the limitations of Diffie-Hellman algorithm?	**07**
		OR	
Q.3	**(a)**	Differentiate Stream cipher and block cipher.	**03**
	(b)	What is the limitation of Electronic Codebook Mode (ECB)? How it is overcome by Cipher Block Chaining (CBC) mode.	**04**
	(c)	What do you mean by key distribution? Give at least one method for key distribution with proper illustration.	**07**
Q.4	**(a)**	Discuss Man-in-the-Middle Attack.	**03**
	(b)	Explain rail fence Cipher technique.	**04**
	(c)	Explain Message Digest Generation Using Secure Hash Algorithm (SHA).	**07**
		OR	
Q.4	**(a)**	Discuss Meet-in-the-Middle Attack.	**03**
	(b)	Explain the triple DES scheme with two keys with suitable diagram.	**04**
	(c)	Explain with the diagrams Basic Uses of Message Authentication code (MAC).	**07**
Q.5	**(a)**	What is the role of AS and TGS in Kerberos?	**03**
	(b)	Give the difference between Session key and Master key.	**04**
	(c)	Explain NIST Digital signature algorithm	**07**
		OR	
Q.5	**(a)**	Explain authentication mechanism of Kerberos.	**03**
	(b)	Write a short note on Pretty Good Privacy (PGP).	**04**
	(c)	Explain SSL Architecture with neat diagram.	**07**

****