Enrolment No. /Seat No.: _______________

GUJARAT TECHNOLOGICAL UNIVERSITY

M.SC(CS)- INTEGRATED– SEMESTER VI- EXAMINATION –SUMMER-2024

Subject Code: 1360305 **Date: 13/05/2024**

Subject Name: IT Security and Audit

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.**

			Marks
Q.1	**(a)**	Differenatiate substitution techniques and transposition techniques.	**03**
	(b)	Describe Rail-Fence cipher algorithm with an example.	**04**
	(c)	Explain Mathematical and Side-channel attacks in detail.	**07**
Q.2	**(a)**	Differenatiate Block cipher and Stream cipher.	**03**
	(b)	Explain sub bytes in AES algorithm.	**04**
	(c)	Explain four different stages of AES structure.	**07**
		OR	
	(c)	Explain hoe DES algorithm observes Fiestel structure. Explain key generation and use of S-box in DES algorithm.	**07**
Q.3	**(a)**	What do you mean by Confidentiality, Integrity and Availability.	**03**
	(b)	What is web security? How can we achieve web security?	**04**
	(c)	Explain the Transport Layer security in detail.	**07**
		OR	
Q.3	**(a)**	What are some key regulations that organization should consider when conducting a security audit?	**03**
	(b)	List out the types of security Audit.	**04**
	(c)	What are some common techniques used during Security audits?	**07**
Q.4	**(a)**	Explain Cipher feedback mode of DES operation.	**03**
	(b)	What are the weakness of ECB mode?	**04**
	(c)	Explain RSA algorithm with suitable example.	**07**
		OR	
Q.4	**(a)**	How encryption is done using triple DES with two keys.	**03**
	(b)	Discuss the Man in Middle attack.	**04**
	(c)	Which principles should be keep in mind during the firewall design?	**07**
Q.5	**(a)**	Explain Public key cryptosystems with applications.	**03**
	(b)	Explain required property of Hash code.	**04**
	(c)	Explain SHA algorithm in detail.	**07**
		OR	
Q.5	**(a)**	Explain counter mode of DES operation.	**03**
	(b)	Write a short note on SSL.	**04**
	(c)	Perform Encryption and Decryption using RSA algorithm for this: p=3; q=13; e=5; M=10.	**07**
