Enrolment No. /Seat No.: _____________

GUJARAT TECHNOLOGICAL UNIVERSITY

M.SC(CS)- INTEGRATED – SEMESTER VI- EXAMINATION –SUMMER-2025

Subject Code: 1360305 **Date: 19/05/2025**

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)**	Explain cryptanalytic attacks with example of any encryption algorithm.	**03**
	(b)	Distinguish between Symmetric encryption and Asymmetric encryption using suitable example.	**04**
	(c)	Explain the VERNAM Cipher method.	**07**
Q.2	**(a)**	Explain data confidentiality, data authentication and data Integrity.	**03**
	(b)	Explain the difference between diffusion and confusion.	**04**
	(c)	Explain how DES (Data Encryption standard) algorithm observes Fiestel structure. Explain single round in detail.	**07**
		OR	
	(c)	Explain playfair cipher with example.	**07**
Q.3	**(a)**	Explain the process of key generation in DES.	**03**
	(b)	List out the various web security threats.	**04**
	(c)	Explain Cipher Feedback (CFB) and Output Feedback mode (OFB) block cipher modes of operation with the help of diagram	**07**
		OR	
Q.3	**(a)**	Differentiate between hashing and encryption.	**03**
	(b)	Elaborate AES encryption with neat sketches.	**04**
	(c)	Explain Hash functions based on Cipher Block Chaining	**07**
Q.4	**(a)**	What is Security audit?what is the need of security audits??	**03**
	(b)	Explain triple DES with two keys.	**04**
	(c)	Write a detailed note on SSL architecture and protocol.	**07**
		OR	
Q.4	**(a)**	How does secure socket layer protocol work?	**03**
	(b)	Explain Intrusion Detection Systems.	**04**
	(c)	Explain Types of Security Audits.	**07**
Q.5	**(a)**	Discuss HASH function and its application in Crypto System.	**03**
	(b)	Explain the following properties of hash function (i) One way property (ii) Weak collision resistance	**04**
	(c)	Discuss Diffie-Hillman key exchange algorithm in detail.	**07**
		OR	
Q.5	**(a)**	Discuss Man-in-the-Middle Attack	**03**
	(b)	Discuss Secure Hash Algorithm (SHA)	**04**
	(c)	Explain RSA algorithm in detail with suitable example.	**07**
