Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE(Minor) - SEMESTER– IV EXAMINATION – WINTER 2023

Subject Code:114AH01 Date:08-02-2024

Subject Name: Information Theory for Cyber Security

Time: 02:30 PM TO 05:00 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)**	Describe the term: Strong Secrecy, Authorization and Integrity.	**03**
	(b)	List out various security measures for computer.	**04**
	(c)	Explain Shamir's Secret Sharing Algorithm with suitable example.	**07**
Q.2	**(a)**	What are the different internet security threats?	**03**
	(b)	Discuss LRC with suitable example.	**04**
	(c)	Write a short note on Quantum Cryptography.	**07**
		OR	
	(c)	Explain Caesar Cipher with example.	**07**
Q.3	**(a)**	Explain Elliptic Curve Cryptography?	**03**
	(b)	What is Hamming Code?	**04**
	(c)	Describe Digital Forensics in detail.	**07**
		OR	
Q.3	**(a)**	Explain perfect secrecy in the symmetric cipher model.	**03**
	(b)	Explain Key Management in Cryptosystem.	**04**
	(c)	What is linear block code? Explain in detail with suitable example?	**07**
Q.4	**(a)**	Explain Different types of network forensics in brief.	**03**
	(b)	Explain the difference between uncertainty and risk for a probability distribution.	**04**
	(c)	Explain Passive Attack and its types.	**07**
		OR	
Q.4	**(a)**	What is Diffie-Hellman algorithm?	**03**
	(b)	Explain rate distortion.	**04**
	(c)	Explain Side channel attack	**07**
Q.5	**(a)**	Explain Public Key Infrastructure.	**03**
	(b)	Write down difference between cyclic code and linear code.	**04**
	(c)	Write a short note on probability distribution.	**07**
		OR	
Q.5	**(a)**	Explain secret sharing and its importance in network security.	**03**
	(b)	Comment on the importance of Digital Certificates.	**04**
	(c)	Briefly explain perfect secrecy with One Time Pad using suitable example.	**07**

****