Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE-MINOR - SEMESTER–IV EXAMINATION – WINTER 2022

Subject Code:114AH01 Date:24-02-2023

Subject Name:Information Theory for Cyber 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 Symmetric Cipher.	**03**
	(b)	Write a short note on Lower bounds on key size.	**04**
	(c)	Explain Shannon's information theory in detail.	**07**
Q:2	**(a)**	What important role random number plays in cyber security? Explain in brief.	**03**
	(b)	Define the Terms: • Strong Secrecy • Weak Secrecy • Semantic Secrecy • Partial Secrecy	**04**
	(c)	Write a short note on probability distribution.	**07**
		OR	
	(c)	Explain in detail Elliptical curve cryptography.	**07**
Q.3	**(a)**	What are the different internet security threats?	**03**
	(b)	List out various security measures for computer.	**04**
	(c)	Explain Shamir's Secret Sharing Algorithm with suitable example.	**07**
		OR	
Q.3	**(a)**	What is authentication? List out different authentication techniques.	**03**
	(b)	Discuss quantum cryptography and different photon states.	**04**
	(c)	What is perfect secrecy? Explain perfect secrecy with One Time Pad using suitable example.	**07**
Q.4	**(a)**	What is channel coding? What are its different types?	**03**
	(b)	Discuss LRC with suitable example.	**04**

	(c)	Find out CRC code for the information 100100 given divisor is 1101.	**07**

OR

Q.4	**(a)**	What is VRC? Explain it with example.	**03**
	(b)	Find out hamming code if information bits are 1101.	**04**
	(c)	Explain Defi-Hellman key exchange algorithm with suitable example.	**07**

Q.5	**(a)**	Explain Different types of network forensics in brief.	**03**
	(b)	Write a short note on Lightweight cryptography.	**04**
	(c)	Illustrate the working of public key infrastructure.	**07**

OR

Q.5	**(a)**	Describe the working of certificate authority.	**03**
	(b)	Comment on the importance of Digital Certificates.	**04**
	(c)	Describe Digital Forensics in detail.	**07**