Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE-MINOR- SEMESTER–IV EXAMINATION – SUMMER 2022

Subject Code:114AH01 **Date:13-07-2022**

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)**	Describe the term: Authentication, Authorization and Integrity	**03**
	(b)	What is data leakage? Explain Types of data leakage.	**04**
	(c)	Explain Shannon’s general secrecy system with a block diagram	**07**
Q.2	**(a)**	What is Differential Privacy? Give it’s benefits.	**03**
	(b)	Encode a binary word 11001 into the even parity hamming code.	**04**
	(c)	What is the difference between Encryption and Masking? Which is better for data security?	**07**
		OR	
	(c)	How does a side channel attack work? What attacks use side channel analysis?	**07**
Q.3	**(a)**	Differentiate :Data Encryption Vs. Data Masking	**03**
	(b)	What is Lightweight Cryptography? Give its advantages and disadvantages.	**04**
	(c)	A bit stream 10110 is transmitted using the standard CRC method. The code generator is 1101. What is the actual bit string transmitted?	**07**
		OR	
Q.3	**(a)**	What is Parity and How it Works?	**03**
	(b)	Explain Diffie-Hellman algorithm	**04**
	(c)	What is Public Key Infrastructure? Explain Digital Certificate with diagram.	**07**
Q.4	**(a)**	What is Secret Sharing?	**03**
	(b)	Explain Key Management in Cryptosystem.	**04**
	(c)	Explain Caesar Cipher with example.	**07**
		OR	
Q.4	**(a)**	What is Elliptic Curve Cryptography?	**03**
	(b)	Explain Symmetric Cipher Model.	**04**
	(c)	Explain provable security and authentication. Is RSA provably secure? Justify.	**07**
Q.5	**(a)**	Explain secret sharing and its importance in network security.	**03**
	(b)	What is Network Forensics? Write Processes Involved in Network Forensics and Challenges in Network Forensics.	**04**
	(c)	Explain Passive Attack and its types.	**07**
		OR	
Q.5	**(a)**	Explain perfect secrecy in the symmetric cipher model.	**03**
	(b)	Explain the difference between uncertainty and risk for a probability distribution.	**04**
	(c)	What Is Quantum Cryptography? How does it works?	**07**

****