Enrolment No./Seat No_______________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE MINOR- SEMESTER–IV EXAMINATION – WINTER 2025

Subject Code:114AH01 **Date:03-12-2025**

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)**	Define provable security.	**03**
	(b)	Explain Uncertainty/Entropy information measures.	**04**
	(c)	Explain Shannon’s general secrecy system with block diagram.	**07**
Q.2	**(a)**	Define Quantum Cryptography.	**03**
	(b)	Explain concept of quantification of leakage and partition.	**04**
	(c)	Write a short note on differential privacy.	**07**
		OR	
	(c)	Explain side channel attack in detail.	**07**
Q.3	**(a)**	Explain unconditional security.	**03**
	(b)	Mention various masking techniques and write short description of each.	**04**
	(c)	List out various codes and discuss them in detail.	**07**
		OR	
Q.3	**(a)**	Explain light-weight cryptography in IOT context.	**03**
	(b)	Draw a figure of Diffie-Hellman key exchange mechanism and explain each step.	**04**
	(c)	Explain Shamir’s secret sharing algorithm with example.	**07**
Q.4	**(a)**	Define secret sharing and its importance in network security.	**03**
	(b)	Explain probability distribution in detail.	**04**
	(c)	Briefly explain rate-distortion theory for secrecy systems.	**07**
		OR	
Q.4	**(a)**	What is Randomized Ciphers? Mention its applications and challenges.	**03**
	(b)	Differentiate between uncertainty and risk for a probability distribution.	**04**
	(c)	Explain Elliptic Curve Cryptography and its applications.	**07**
Q.5	**(a)**	What is semantic security?	**03**
	(b)	Differentiate between parity check code and cyclic code.	**04**
	(c)	Discuss key concept, types, techniques and applications of Distributed channel synthesis.	**07**
		OR	
Q.5	**(a)**	Define network forensics.	**03**
	(b)	Draw a diagram of encryption and decryption process in AES.	**04**
	(c)	Write a short note on Public Key Infrastructure.	**07**

****