Enrolment No./Seat No_______________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE(MINOR)- SEMESTER–I&II EXAMINATION – SUMMER 2025

Subject Code:114AH01 **Date:03-06-2025**

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)** Explain symmetric cipher in brief. **03**

(b) Describe how the lower bound on key size is related to secrecy and authentication. **04**

(c) Analyze Shannon’s foundation of information theory and its impact on modern cryptography. **07**

Q.2 **(a)** What are block codes in coding theory? **03**

(b) Differentiate between randomized ciphers and deterministic ciphers. **04**

(c) Evaluate the importance of secret sharing schemes in secure communication. How does secret sharing enhance the robustness of secure systems? **07**

OR

(c) Assess the use of masking techniques in cryptographic security. How do they contribute to the prevention of side-channel attacks? **07**

Q.3 **(a)** What is a shared secret in cryptography? **03**

(b) How does AES (Advanced Encryption Standard) work in securing data? **04**

(c) Analyze the strengths and weaknesses of the Diffie-Hellman key exchange. Discuss potential vulnerabilities and how they can be mitigated. **07**

OR

Q.3 **(a)** Explain information-theoretic security in brief. **03**

(b) How do side-channel attacks exploit vulnerabilities in cryptographic systems? **04**

(c) Compare and contrast the principles of information-theoretic security and computational security in cryptographic systems. **07**

Q.4 **(a)** Define differential privacy in brief. **03**

(b) What is distributed channel synthesis in the context of secure communication? **04**

(c) Evaluate the role of rate-distortion theory in secure source coding. How does it balance compression and secrecy? **07**

OR

Q.4 **(a)** Define strong secrecy and weak secrecy in cryptography. **03**

(b) Explain the concept of partial secrecy in cryptography. **04**

(c) Analyze the differences between strong secrecy and weak secrecy in cryptography. Which is more practical in real-world scenarios? **07**

Q.5 **(a)** List applications of Public Key Infrastructure (PKI). **03**

(b) Describe common application of lightweight cryptography. **04**

(c) Analyze the importance of digital and network forensics in incident response. How can effective forensics practices improve security measures? **07**

OR

Q.5 **(a)** Briefly explainprimary goal of digital forensics. **03**

(b) How does Public Key Infrastructure (PKI) ensure secure communications? **04**

(c) Assess the impact of Elliptic Curve Cryptography (ECC) on modern encryption practices. How has it changed the landscape of secure communications? **07**

****