Seat No.: _____ Enrolment No._____

# GUJARAT TECHNOLOGICAL UNIVERSITY

**BE(MINOR) - SEMESTER–IV EXAMINATION – SUMMER 2023**

**Subject Code:114AH01 Date:14-08-2023**

**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)** | **List out Possible sources of Uncertainty.** | **03** |
| | **(b)** | Explain marginal Probability & Conditional Probability. | **04** |
| | **(c)** | Explain Shannon's Source Code theorem Briefly. | **07** |
| **Q.2** | **(a)** | Explain Probability Distributions | **03** |
| | **(b)** | What does quantification of leakage mean? | **04** |
| | **(c)** | Explain Side channel Attack. | **07** |
| | | **OR** | |
| | **(c)** | Explain Diffie-Hellman key exchange | **07** |
| **Q.3** | **(a)** | Does Key length and Security coincide? Justify | **03** |
| | **(b)** | Explain Light Weight cryptography in context to IOT Devices. | **04** |
| | **(c)** | What is elliptic curve cryptography? | **07** |
| | | **OR** | |
| **Q.3** | **(a)** | What is the difference between digital forensic and Network Forensic | **03** |
| | **(b)** | Explain Semantic Security | **04** |
| | **(c)** | What is AES Encryption and how does it work? | **07** |
| **Q.4** | **(a)** | Explain different types of attacks in Cyber Security. | **03** |
| | **(b)** | What are the types of parity check codes? | **04** |
| | **(c)** | What is Hamming code? | **07** |
| | | **OR** | |
| **Q.4** | **(a)** | What is Symmetric cipher? | **03** |
| | **(b)** | How do you find the probability distribution of a random variable? | **04** |
| | **(c)** | Explain polyalphabetic cipher encryption. | **07** |
| **Q.5** | **(a)** | What is linear block codes? | **03** |
| | **(b)** | Explain Cyclic code and give Example. | **04** |
| | **(c)** | Explain Data Masking in Cyber Security. | **07** |
| | | **OR** | |
| **Q.5** | **(a)** | Explain provable security in short. | **03** |
| | **(b)** | What is rate distortion? | **04** |
| | **(c)** | Explain monoalphabetic cipher encryption. | **07** |

**********