SARVAJANIK UNIVERSITY
INCLUSIVE | INTEGRATED | INNOVATIVE

# SARVAJANIK UNIVERSITY
## Sarvajanik College of Engineering and Technology
## Bachelor of Technology

## Year: B. Tech II (Semester IV)

**Subject Name**: Information Theory for Cyber Security **Subject Code:** BTEA19453
**Type of course:** Minor (Group: Cyber Security)
**Prerequisite (if any):** Computer Network, Probability Theory
**Rational:** The objective of this course is to provide an insight to information coding techniques, error correction mechanism for cyber security.
**Teaching and Examination Scheme:**

| Teaching Scheme | | | | Theory Marks | | | Practical Marks | | Total |
|---|---|---|---|---|---|---|---|---|---|
| L | T | P | C | TEE | CA1 | CA2 | TEP | CA3 | |
| 3 | 0 | 2 | 4 | 60 | 25 | 15 | 30 | 20 | 150 |

CA1: Continuous Assessment (assignments/projects/open book tests/closed book tests) CA2: Sincerity in attending classes/class tests/ timely submissions of assignments/self-learning attitude/solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work/Quality of work submitted/Active participation in lab sessions/viva on practical skills learned in course

**Content:**

| Sr. No. | Contents | Total Hours |
|---|---|---|
| 1. | Shannon's foundation of Information theory, Random variables, Probability distribution factors, Uncertainty/entropy information measures, Leakage, Quantifying Leakage and Partitions, Lower bounds on key size: secrecy, authentication and secret sharing. provable security, computationally-secure, symmetric cipher. | 08 |
| 2. | Secrecy, Authentication, Secret sharing, Optimistic results on perfect secrecy, Secret key agreement, Unconditional Security, Quantum Cryptography, Randomized Ciphers, Types of codes: block codes, Hamming and Lee metrics, description of linear block codes, parity check Codes, cyclic code, Masking techniques. | 10 |
| 3. | Information-theoretic security and cryptograph, basic introduction to Diffie-Hellman, AES, and side-channel attacks. | 08 |
| 4. | Secrecy metrics: strong, weak, semantic security, partial secrecy, Secure source coding: rate-distortion theory for secrecy systems, side information at receivers, Differential privacy, Distributed channel synthesis. | 10 |
| 5. | Digital and network forensics, Public Key Infrastructure, Light weight cryptography, Elliptic Curve Cryptography and applications. | 09 |

**Reference Text Books:**

| Sr. No. | Title of book /article | Author(s) | Publisher and details like ISBN | Year of publication |
|---|---|---|---|---|
| 1. | Information Theory and Coding | Muralidhar Kulkarni K S Shivaprakasha | John Wiley & Sons | 2014 |
| 2. | Communication Systems: Analog and digital | Singh and Sapre | Tata McGraw Hill | 2008 |
| 3. | Fundamentals in information theory and coding | Monica Borda | Springer | 2011 |
| 4. | Information Theory, Coding and Cryptography | R. Bose | Tata McGraw Hill | 2008 |
| 5. | Multi-media System Design | Prabhat K Andleigh Kiran Thakrar | Prentice Hall PTR | 1996 |

**Course Outcome:**

| Sr. No. | CO Statements |
|---|---|
| CO-1 | Explain the principles and applications of information theory. |
| CO-2 | Describe how information is measured in terms of probability and entropy. |
| CO-3 | Describe coding schemes, including error correcting codes. |