Year: B. Tech III (Semester V)

Subject Name: Data Encryption and Compression
Type of course: Minor (Group: Cyber Security)
Subject Code: BTEA19553

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.

Contents:

Sr. No.	Contents	Total Hours
1.	**Introduction to Security:** Need for security, Security approaches, Principles of security, Types of attacks. **Encryption Techniques:** Plaintext, Cipher text, Substitution & Transposition techniques, Encryption & Decryption, Types of attacks, Key range & Size.	08
2.	**Symmetric & Asymmetric Key Cryptography:** Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, RSA, Symmetric & Asymmetric key together, Digital signature, Knapsack algorithm.	07
3.	**Case Studies of Cryptography:** Denial of service attacks, IP spoofing attacks, Conventional Encryption and Message Confidentiality, Conventional Encryption Algorithms, Key Distribution. **Public Key Cryptography and Message Authentication:** Approaches to Message Authentication, SHA-1, MD5, Public-Key Cryptography Principles, RSA, Digital, Signatures, Key Management, Firewall.	09
4.	**Data Compression:** Need for data compression, Fundamental concept of data compression & coding, Communication model, Compression ratio, Requirements of data compression, Classification. **Methods of Data Compression:** Data compression—Lossless &lossy.	08
5.	**Entropy encoding:** Repetitive character encoding, Run length encoding, Zero/Blank encoding; Statistical encoding-- Huffman, Arithmetic & Lempel-Ziv coding; Source encoding, Vector quantization (Simple vector quantization & with error term).	08

6.	Recent trends in encryption and data compression techniques.	05

Suggested Specification table with Marks (Theory): (For B. Tech only)

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
15	20	20	5	-	-

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (Revised Bloom's Taxonomy)

Reference Books:

Sr. No.	Title of book /article	Author(s)	Publisher and details like ISBN
1	Cryptography and Network Security	Mohammad Amjad	John Wiley & Sons
2	John Wiley & Sons	AtulKahate	TMH
3	Information Theory and Coding	MuralidharKulkarni, K S Shivaprakasha	John Wiley & Sons
4	Cryptography and Network Security	B. Forouzan	McGraw-Hill
5	The Data Compression	Nelson	BPB

Note: Students should refer to the latest editions of books

Course Outcomes (CO):

Sr. No.	CO statements	Marks % weightage
CO-1	Demonstrate the knowledge of plain text, cipher text RSA and other cryptographic algorithms.	40%
CO-2	Explain Key Distribution, communication model.	20%
CO-3	Explain methods for data compression.	40%

Lab Work:

- Experiments to be implemented as per curriculum