GUJARAT TECHNOLOGICAL UNIVERSITY

Minor Degree: Cyber Security
Subject Code: 115AH01
Semester – V
Subject Name: Data Encryption

Prerequisite: Linear Algebra, Cryptography

Rationale: To prevent unauthorized users from accessing your precious data one of the way is Data encryption. On the other hand compressing data can save storage capacity, speed up file transfer, and decrease costs for storage hardware and network bandwidth. This course focus on various encryption techniques for securing data. The subject also covers various compression methods to decrease the file size.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
L	T	P	C	Theory Marks		Practical Marks		
				ESE (E)	PA (M)	ESE (V)	PA (I)	
3	0	2	4	70	0	30	0	100

Content:

Unit No	Course Content	No of Hours
1	**Introduction to Security:** Need for security, Security approaches, Principles of security, Types of attack **Encryption Techniques: Plaintext**, Cipher text, Substitution & Transportation techniques, Encryption & Decryption, Types of attacks, Key range & size.	8
2	**Symmetric & Asymmetric Key Cryptography:** Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, RSA, Symmetric & Asymmetric key together, Digital signature, Knapsack algorithm.	6
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.	9
4	**Introduction 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—Loss less & Lossy	7
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).	8

6	Recent trends in encryption and data compression techniques.	4
	Total Hrs.	**42**

Suggested Specification table (Theory):

Distribution of Theory Marks (%)					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
30	30	15	20	5	-

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

Reference Books:

1. Cryptography and Network Security, Mohammad Ajmad, John Wiley & Sons.
2. Cryptography and Network Security by Atul Kahate, TMH.
3. Information Theory and Coding, Muralidhar Kulkarni, K S Shivaprakasha, John Wiley & Sons
4. Cryptography and Network Security by B.Forouzan, McGraw-Hill.
5. The Data Compression Book by Nelson, BPB.

Course Outcomes: At the end of this course the student will have the knowledge of plain text, cipher text, RSA and other cryptographic algorithm,, Key Distribution ,Communication model, Various models for data compression.

No	Course Outcomes	% weightage
01	To understand basic terminologies used in information security.	10
02	To analyze substitution & transposition techniques.	10
03	To learn RSA and other cryptographic algorithms.	25
04	To understand key distribution and communication model.	20
05	To study various models for data compression.	35

List of Practical:

1. Write a program to perform encryption and decryption using Data Encryption Standard (DES).
2. Write a program to perform encryption and decryption using Advance Encryption Standard (AES).
3. Write a program to perform encryption and decryption using IDEA.
4. Implement RSA algorithm.
5. Implement knapsack algorithm.
6. Study and prepare comparative analysis of SHA-1 and MD5.
7. Prepare case study on Digital Signature.

8. Implement Huffman coding.
9. Prepare case study on recent trend in Encryption.
10. Prepare case study on various data compression techniques.