

Data Compression and Encryption

(Elective – I)

B.E. Sem. VII [EXTC]

EVALUATION SYSTEM

	Time	Marks
Theory Exam	3 Hrs.	100
Practical Exam	–	–
Oral Exam	–	25
Term Work	–	25

Objective : The objective of this course is to introduce to the students the fundamentals of data compression, data encryption and data security.

SYLLABUS

1. Text Compression

Shannon Fano Coding, Huffmann coding, Arithmetic coding and dictionary techniques-LZW, family algorithms. Entropy measures of performance and Quality measures.

2. Audio Compression

Digital Audio, Lossy sound compression, M-law and A-law companding, DPCM and ADPCM audio compression, MPEG audio standard, frequency domain coding, format of compressed data.

3. Image and Video Compression

Loss less techniques of image compression, gray codes, Two dimensional image transforms, JPEG, JPEG 2000, Predictive Techniques PCM and DPCM. Video compression and MPEG industry standard.

4. Conventional Encryption

Introduction, Types of attacks, Steganography, Data Encryption Standard, Block Cipher Principle, S-box design, triple DES with two three keys, introduction to international data encryption algorithm and key distribution.

5. Public Key Encryption and Number Theory

Euler's theorems, Chinese remainder theorem, Principles of public key cryptography, RSA algorithm, Diffie-Hellman Key Exchange. Elliptic curve cryptology, message authentication and Hash functions, Hash and Mac algorithms, Digital signatures.

6. System Security & Case Studies

Intruders, Viruses, Worms, firewall design, antivirus techniques, digital Immune systems, Certificate based & Biometric authentication, Secure Electronic Payment System.

References :

1. Data Compression (*David Salomon*) Springer Publication, 4th Edition.
2. Introduction to Data Compression (*Khalid Sayood*) Morgan Kaufmann Series, 3rd Edition
3. Cryptography and Network Security (*William Stallings*) Pearson Education Asia Publication, 5th Edition.
4. Cryptography and Network Security (*Behrouz Forouzan*), McGraw-Hill, 1st Edition.
5. The Data Compression Book (*Mark Nelson*), BPB publication, 2nd Edition
6. Applied Cryptography (*Bruce Schneier*) John Willey & Sons Inc. Publication, 2nd Edition
7. Cryptography & Network Security (*Atul Kahate*) Tata McGraw Hill, 2nd Edition

