Paper / Subject Code: 42405 / Elective - I 1)Data Compression & Encryption

Duration: 3 Hours **Marks: 80**

Note:

1) Q.1 is **compulsory**.
2) Attempt any **three** questions from the remaining **five** questions.
3) Assume Suitable data wherever necessary

Q1. Answer any four **20**

a) What are different security goals? Describe various attacks compromising these goals.
b) State Fermat's Little Theorem, Euler's Theorem in modular arithmetic.
c) What is significance modeling and coding in data compression?
d) Illustrate worst case in LZ-77 dictionary compression technique
e) What are the measures of performances for lossy and lossless compression techniques

Q2. a) A source with alphabet A={a,b,c,d,e} with probabilities P={0.2, 0.4, 0.2, 0.1, 0.1} respectively calculate standard Huffman code, average code word length and draw binary tree **10**

b) Explain Diffie Hellman Key exchange with the help of an example. **10**

Q3. a) Explain RSA algorithm in detail and discuss attacks on RSA **10**

b) Explain Arithmetic coding Tag generation using a suitable example **10**

Q4 a) Explain Triple DES with two keys and 'Meet in the Middle Attack' **10**

b) Explain Standard JPEG with neat diagram, what are the advantages of JPEG 2000 over standard JPEG? Justify use of DCT in JPEG **10**

Q5 a) Explain Frequency and Temporal masking with respect to audio compression. Also explain how MP3 encoder works **10**

b) What are digital signatures? Explain any one technique in detail. **10**

Q6. Write short notes on any two **20**

a) MPEG video compression standard
b) Elliptic Curve Cryptography
c) Fire walls, Intrudes and viruses
d) Adaptive Huffman Coding

____