B.E. Sem 7 (Rev.) EXTC. Data compression and Encryption 29/12/08

ws Oct 08 277

Con. 5827–08. (REVISED COURSE) RC–7334

(3 Hours) [Total Marks : 100

N.B. : (1) Questions No. **1** is **compulsory**.
(2) Attempt any **four** questions out of remaining **six** questions.

1. (a) Briefly explain the significance of modeling and coding with respect to data compression. **5**
   (b) What are the sifting properties in Adaptive Huffman Codes ? **5**
   (c) What is the significance of prime numbers in cryptography ? **5**
   (d) What are 'active' and 'passive' attacks ? **5**

2. (a) With M= {a, b, c, d} and P {0·4, 0·3, 0·1, 0·2}, respectively, we encode the message 'cbdda'. Using arithmetic coding generate the tag for encoding and also decipher the tag to decode the sequence. **10**
   (b) Explain discrete logarithm and Chinese Remainder theorem and its use in security. **10**

3. (a) Given an initial dictionary consisting letters (a, b, c, d, e, f) incode using LZW algorithm 'addaeabccdaceaeafccdeafccde'... Also decode using the incoding sequence to get back the string. **10**
   (b) Explain different types of block cipher modes of operations. **10**

4. (a) Distinguish between scalar and vector quantization. Explain K-Means algorithm. **10**
   (b) Explain RSA algorithm. Using RSA, perform encryption and decryption for p = 7, q = 11, e = 17, M = 8. **10**

5. (a) Why in DCT more popular for image compression ? How is it used in JPEG ? **10**
   (b) What is the role played by KDC in symmetric Encryption ? Explain. **10**

6. (a) Give a suitable scheme for speech compression. Discuss the MPEG audio encoder and decoder systems. **10**
   (b) Suggest a suitable scheme for secure communication between users A and B taking care of message integrity and authentication. Justify your scheme. **10**

7. Write notes on (any **two**) :– **20**
   (a) Fractal Image Compression
   (b) Digital Signatures
   (c) Diffie Huffman Key Exchange
   (d) Extended Huffman Codes.
