

(3 Hours)

QP Code : 29786  
[Total Marks : 100]

N.B 1. Question No. 1 is compulsory.

2. Attempt any four questions out of the remaining six questions

- 1 a What are the various models used for data compression ? 05
- b What are active and passive attacks? 05
- c What is Biometric authentication? Explain with examples. 05
- d What is the need for data compression? 05
- 2 a A source emits letter from an alphabet  $A = \{ a_1, a_2, a_3, a_4, a_5 \}$  with probabilities  $P(a_1) = 0.15$ ,  $P(a_2) = 0.04$ ,  $P(a_3) = 0.26$ ,  $P(a_4) = 0.05$  and  $P(a_5) = 0.50$ . 10
- a) Calculate the entropy of this source
- b) Find the Huffman code for this source.
- c) Find the average length of the code in and its redundancy
- b Explain the working of DES. 10
- 3 a Show the difference in the encoding procedure of LZ78 and LZW with an example. 10
- b How are keys distributed in conventional encryption systems? 10
- 4 a Discuss the various lossless techniques for image compression. 10
- b Explain Chinese Remainder Theorem with an example. 10
- 5 a How is motion compensation used in video compression? 10
- b What are the various aspects of Firewall design? 10
- 6 a Discuss the differences in compression schemes of JPEG and JPEG 2000. 10
- b What are digital signatures and how are they implemented ? 10
7. Write notes on [Any TWO] 20
- a Elliptic Curve Cryptography
- b MPEG Audio System
- c ADPCM Encoder and Decoder