Duration: 3Hrs **Marks: 80**

Instructions:
(1) Question no 1 is Compulsory
(2) Write any Three from Remaining
(3) Assume suitable data if necessary

1. a) Write a note on convolution code. [4]
   b) State Fermat's little theorem and its applications. [4]
   c) Define Source entropy and destination entropy. [4]
   d) Explain cyclic and Hamming codes. [4]
   e) Describe properties of prefix coding with example. [4]

2. a) Name the source coding technique used in the following types of files and Classify them as lossy or lossless. [10]
   i).Zip ii).jpg iii).mpg iv).bmp v).gif
   b) For (7,4) cyclic code, find out the generator matrix if $G(D)=1+D+D^3$ [10]

3. a) Explain Diffie-Hellman algorithm. Which attack is it vulnerable to? [10]
   b) Construct Huffman code for the given symbols{x1,x2..x8} with probabilities P(x)= {0.1,0.05,0.04,0.01,0.04,0.06,0.3,0.4}Find coding efficiency. [10]

4. a) Explain LZW compression algorithm with example. [10]
   b) State Chinese Remainder theorem. Using it solve for X.
   X=1 MOD 2
   X=2 MOD 3
   X= 2 MOD 5 [10]

5. a) What do you mean by symmetric key cryptography? Explain DES in detail. [10]
   b) The generator polynomial for a (7, 4) cyclic code is given by $G(D)= 1+D+D^3$.
   Compute all systematic codewords. [10]

6. Write short notes on [20]
   a) RSA
   b) RLE
   c) Security Goals
   d) Digital signature.

****

73037