(3 Hours)   **[Total Marks: 80]**

N.B. : (1) Question No.1 is compulsory
       (2) Answer any 3 questions from Q.No. 2 to Q.No. 6
       (3) Figures to the right indicate full marks
       (4) Assume suitable data if required

1. (a) Explain Digital signature   5
   (b) Compare Lossy and Lossless compression.   5
   (c) Explain Security goals.   5
   (d) Compare Symmetric and Asymmetric key cryptography   5

2. (a) Explain convolution code with example. Draw code tree, code trellis and state diagram.   10
   (b) What is Entropy? What are its types?   5
   (c) Explain JPEG encoder.   5

3. (a)   10

For a (6,3) linear block code, the coefficient matrix [p] is as follows:

$$P = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

The received code words at the receiver are :
1) 0 0 1 1 1 0   2) 1 1 1 0 1 1
Check whether they are correct or contains some errors.

   (b) Explain RSA algorithm with example   5
   (c) Explain BCH codes.   5

4. (a) Consider the symbols {1,1,1,1,1,1,1,2,2,2,2,2,2,3,3,3,3,3,4,4,4,4,5,5,5,6,6,7}   10
     i. Find efficient fixed length code.
     ii. Find Huffman code.
     iii. Compare 2 codes.

   (b)   Explain Cyclic and Prefix code   5
   (c)   Compare MD5 and SHA-1   5

5. (a) Explain Diffie- Hellman algorithm. Which attach, is it vulnerable to?   10
   (b) Explain Chinese Remainder theorem.   5
   (c) Explain Speech compression.   5

6. (a) Explain DES in detail.   10
   (b) Explain Channel capacity   5
   (c) Use Euclidean's algorithm to find GCD (1819,3587)   5

60238