QP Code :12601

(3 Hours)   Total Marks : 80

N. B. : (1) Question No.1 is **compulsory**.
(2) Solve any **three** questions out of the remaining questions.
(3) Figures to the right indicate **full** marks.

1. (a) Define Chinese Remainder Theorem and its application   5
   (b) Explain Term Entropy in Information Theory and its significance   5
   (c) Describe Fermat's Little Theorem. And its Application   5
   (d) Explain Cyclic Codes   5

2. (a) Explain Adaptive Huffman encoding technique. Encode the data Pattern   10
       "accabbcdaad" using Above technique.
   (b) Compare Symmetric and Asymmetric Cryptography   5
   (c) Explain various Security Goals   5

3. (a) Explain convolution code in Brief.   10
   (b) Consider the source probabilities   10
       {0.20, 0.20, 0.15, 0.15, 0.10, 0.10, 0.05, 0.05,}
       (i)   Determine the efficient fixed length code for the source.
       (ii) Determine Huffman code for this source.
       (iii) Compare the two codes and comment.

4. (a) Explain DES and give an outline of the algorithm.   10
   (b) Which of the following g (x) values guarantees that a single-bit error is caught?   10
       In each case, what is the error that cannot be caught?
       (i)   x+1   (ii) x^3

5. (a) Describe with example Modular Arithmetic, Expontiation and Congruences.   10
   (b) Define -   (i)   Hamming Weight   10
                         (ii)   Hamming Distance
                         (iii) Syndrome
                         (iv)   Linear Code Properties
                         (v)   Code Rate

6. Write Short notes on: 20
   (i)   RSA
   (ii) RLE
   (iii) Speech Compression
   (iv) Random Number Generation