QP Code : NP-19886

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

N.B.: (1) Question No.1 is **compulsory**.

      (2) Solve any **three** questions out of the remaining questions.

1. (a) Explain the physical significance of Entropy in Information theory   (2M)
   (b) What is Compression? List different Compression algorithms.   (3M)
   (c) Describe Fermat's Little Theorem.   (3M)
   (d) Find the generator and parity check matrices of a (7, 4) cyclic code with   (3M)
   generator polynomial g (X) = $1 + X + X^3$.
   (e) What is Random Number Generation and when it is needed.   (3M)
   (f) What are the security goals? Define Cryptography.   (3M)
   (g) Write about Convolution Codes.   (3M)

2. (a) Name the source coding techniques used in the following types of files and classify them as lossy or lossless.
   (i) .zip   (ii) .jpg   (iii) .mpg   (iV) .bmp   (v) .gif   (10M)
   (b) Define generator and parity check matrices of a (7, 4) linear block code.   (10M)
   Explain how to generate a linear block code using G-matrix. Explain with an example.

3. (a) Describe about Discrete probability and logarithms.   (10M)
   (b) Given x_i={$x_1, x_2, x_3, x_4, x_5, x_6$} with probabilities as below: (10M)

        $p(x_i)$= {0.3, 0.25, 0.2, 0.12, 0.08, 0.05}.

   Make Huffman code. Find efficiency of this code.

4. (a) What do you mean by Symmetric key cryptography? Explain DES in detail.   (10M)
   (b) A (7, 4) cyclic code has a generator polynomial: g(X) = $X^3 + X + 1$.   (10M)

   (i) Draw the block diagram of encoder and syndrome calculator.

   (ii) Find generator and parity check matrices in systematic form.

5. (a) Describe with example Modular Arithmetic, Exponentiation and Congruences.   (10M)
   (b) Explain Diffie-Hellman Algorithm. Which attack, is it vulnerable to?   (10M)

6. Write Short notes on: (20M)
   (a) Types of Entropy   (b)Digital Signature   (c) RLE
   (d)Prime Number Generation

Con. 13847-14.