MCSE-202

M.E. / M.Tech. (second semester)
(computer science & engineering)
EXAMINATION, june, 2012
(Garding/Non-Grading)
INFORMATION THEORY, CODING AND CRYPTOGRAPHY
(MCSE-202)

Time: three hours   *Maximum Marks: GS: 70*
NGS:100

Note : attempt only one question from each unit, hence total five question are to be attempted. make suitable assumption, as required.

UNIT- 1

1. (a) define information, mutual information and entropy. state and explain various properties of informations.
   (b) find the average codeword length and coding efficiency for the following message using huffman coding with M = 3.

   $[X] = [x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8]$
   $[P] = [0.1, 0.25, 0.15, 0.05, 0.15, 0.1, 0.05, 0.15]$

Or

2. (a) state and discuss shannon's theorem (source coding theorem).
   (b) Write a brief note on random variables, their type and properties.

Unit - 2

3. (a) Discuss hidden-markov model. what are its properties? list is applications.
   (b) describe the discrete birth death processes. what are its properties? using an example, show, how the process may be applied to queuing theory?

Or

4. (a) differentiate between bernoulli processes and poisson processes.
   (b) write the characteristics of markov chain.
       two products A and B are available in market. customer are using product A, 80% of the
       time. also former customers using the product B have switched back to product A 60% of
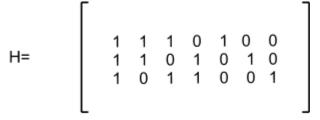   the time:
       (1) construct the transition matrix in terms of (a) retention and loss,
            (b) retention and gain.
        (2) calculate the probability of a customer purchasing A's product at
           the end of the second period (n=2).

Unit – 3

5. (a) The parity check matrix of a particular (7, 4) linear block code is given by ahead :

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

    (1) find the generator matrix G.

    (2) list all the code vectors.

    (3) what is the minimum distance between the code vectors?

    (4) how many error can be detected ? how many errors can be corrected?

  (b) write a brief note on CRC.

Or

6. (a) discuss BCH code and write its properties. show using an example, the decoding steps of the code.

  (b) A (15, 5) linear cyclic code has generator polynomial :

    $g(x) = 1+x+x^2+x^4+x^5+x^8+x^{10}$

    find the code polynomial for the message polynomial :

    $D(x) = 1+x^2+x^4$

    (in a systematic form).

Unit - 4

7. (a) differentiate between the following terms:

    (1) confusion and diffusion

    (2) substitution cipher and transposition cipher

  (b) discuss in brief, the basic principles of data encryption standard (DES).

Or

8. (a) briefly discuss the diffie-hellman key exchange. it is used to establish a secret key between alice and bob. assuming prime number n=11, base g=5 and secret integers as x=2 and y=3, find out the values of messages A,B and secret key (K1 or K2).

  (b) explain RSA algorithm, with an example.

Unit-5

9. (a) what is reed-solomon code? describe its decoding process.

  (b) discuss soft decision viterbi algorithm.

Or

10. (a) how encoding is done in convolutional codes? explain.

  (b) discuss briefly, the coding and decoding of LDPC codes.