rgpvonline.com

MCSE-202

M.E./M.Tech., II Semester

Examination, June 2013

Information Theory, Coding and Cryptography

Time : Three Hours

Maximum Marks : 70

Note: Attempt any five questions. All questions carry equal marks.

1. a) Prove that the entropy for a discrete source is a maximum when the output symbols are equally probable.   7

   b) Consider a DMS with source probabilities {0.35, 0.25, 0.20, 0.15, 0.05}
      i) Determine the Huffman code for this source
      ii) Determine the average length $\bar{R}$ of the code words.
      iii) What is the efficiency η of the code?   7

2. a) Let X and Y be random variables that take on values $x_1, x_2, \ldots\ldots x_r$ and $y_1, y_2, \ldots\ldots y_s$ respectively. Let $z = x + y$.
      i) Show that $H(z/x) = H(y/x)$
      ii) Under what condition will $H(z) = H(x) + H(y)$?   7

   b) Discuss Shannon's theorem & its application?   7

3. a) Write short note on :
      i) Renewal process
      ii) Bernoulli process   7

   b) Explain Hidden Markov model? What is the use of this model? Also discuss its properties?   7

4. a) Show that if C is a binary linear code, then the code obtained by adding an overall parity check bit to C in also linear.   7

rgpvonline.com

MCSE-202   PTO

   b) Consider the following generator matrix over GF(2)

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

   rgpvonline.com

      i) Generate all possible code words using this matrix
      ii) Find the parity check matrix, H.
      iii) Find the generator matrix of an equivalent systematic code.   7

5. a) Show that $g(x) = (x^n + 1)(x^6 + x + 1)$ is a valid generator polynomial of a fire code. What is the burst error correction length for this code?   7

   b) What are BCH codes? Discuss the steps for decoding BCH codes.   7

6. i) Use the prime number 29 and 61 to generate keys using RSA algorithm.

   ii) Represent the latter 'RSA' in ASCII and encode them using the key generated above.

   iii) Next generate keys using the poor of primes 37 and 67. Which is more secure, the keys in part (i) or Part (iii)? Why?   14

7. a) Explain the main concepts in DES. How can the same key be reused in triple DES?   7

   b) i) Explain the principles of the IDEA algorithm.
      ii) Explain the usage of the S array in the case of the RC4 algorithm.   7

8. Write short notes on :- (Any Three)   14
   i) Reed-solomon codes
   ii) LDPC codes
   iii) Convolution channel coding
   iv) Viterbi Algorithm.

   rgpvonline.com

MCSE-202   ******