IT

SE sem IV CBGS IT 22/12/15

Info Theory & ~~[illegible]~~ Coding

QP Code : 5541

(3 Hours) [Total Marks : 80

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

(2) Attempt any **three** questions from remaining five questions.

(3) Make **suitable assumption** if **necessary** and **state** it **clearly**.

1. (a) Derive expression for entropy ? 5

(b) What is lossless compresion ? 5

(c) List attacks threatening security goals. 5

(d) Explain the role of digital signature. 5

2. (a) Explain LZW compression algorithm with example. 10

(b) For DES symmetric algorithm, explain main steps involved showing block size, cipher key size and round key size. 10

3. (a) For (7, 4) cyclic code, find out the generator matrix if $G(D) = 1 + D + D^3$. 10

(b) Describe Huffman decoding procedure with example. 10

4. (a) Explain Diffie-Hellman algorithm. Which attack is it valnerable to ? 10

(b) Describe convolution code in brief. 10

5. (a) State Fermat's Little Theorem with example and its applications. 10

(b) Describe lossy compression methods. Where we use lossy compression methods ? How do we are it ? 10

6. (a) Describe Chinese-Remainder Theorem and its applications. 10

(b) Define : (i) Hamming distance 10

(ii) Hamming Weight

(iii) Syndrome

(iv) Linear properties of code

(v) Code rate

———v———

MD-Con.-12236 -15