Sem - IV / I.T. / CBGS / ITC / NOV-16 / 28-12-16

Q. P. Code : 550000

Information Theory & coding

(3 Hours) [Total Marks -80

N.B.- 1. Question No. 1 is compulsory
2. Attempt any three Questions out of remaining five Questions
3. Figures to right indicate marks.
4 all questions carry equal marks.

---

1. a) What is Entropy? What are its types? [4]
b) Compare Lossy and Lossless compression. [4]
c) Write a note on convolution code. [4]
d) State Fermat's little theorem and its applications. [4]
e) Explain cyclic codes. [4]

2. a) What do you mean by symmetric key cryptography? Explain DES in detail. [10]
b) The generator polynomial for a (7, 4) cyclic code is given by $G(D)= 1+D+D^3$.
Compute all systematic codewords. [10]

3 a) Explain LZW compression algorithm with example. [10]
b) State Chinese Remainder theorem. Using it solve for X. [10]

X=1 MOD 2
X=2 MOD 3
X= 2 MOD 5

4. (a) Consider the symbols {1,1,1,1,1,1,1,2,2,2,2,2,2,3,3,3,3,3,4,4,4,4,5,5,5,6,6,7} [10]
i. Find efficient fixed length code.
ii. Find Huffman code.
iii. Compare 2 codes.
(b) Explain Modular arithmetic with example [5]
(c) Compare MD5 and SHA-1 [5]

5. (a) Explain Diffie- Hellman algorithm. Which attack, is it vulnerable to? [10]
(b) Explain the idea of Message Digest 5 (MD 5) [5]
(c) Explain Speech compression. [5]

6. Write short notes on any **two**: [20]
a) RSA
b) RLE
c) Channel Capacity
d) Data Encryption Standard (DES)
