B.E. Sem VII (CBSGS) 7/6/17
ExTC

T4927 / T1339 ELECTIVE I 1)DATA COMPRESSION & ENCRYPTION

OP Code : 788900

(3 Hours) [Total Marks : 80

N. B. : (1) Question No. **1** is **compulsory**.
(2) Solve any **three** from remaining.
(3) Assume suitable data if necessary with proper justification.

1. Answer the following in brief :– **20**
   (a) Classify data compresion techniques and give example for each.
   (b) What are one way trap door functions? What is their importance in cryptography?
   (c) State :–
      (i) Fermat's little theorem
      (ii) Euler's theorem
      (iii) Chinese Remainder theorem
      (iv) Difinition of primitive root
   (d) What do you mean by "auditory masking" and "temporal masking"?

2. (a) A source with alphabet A = {a,b,c,d,e} with probabilities P = {0.15, 0.05, 0.25, 0.35, 0.2} respectively, calculate **10**
   Standard Huffman code.
   Minimum variance Huffman code.
   Avg length & variance for both codes.
   Draw binary tree for both.
   (b) What are private key cryptosystems? What are their advantages & disadvantages? Explain DES with neat block diagram. **10**

3. (a) What are dictionary based comprension schemes? Explain the LZ-77 technique with an example. **10**
   (b) Alice and Bob choose p = 13 and q = 5 as prime numbers for RSA encryption. Alice chooses e = 7 as public key. Derive her private key. She wants to send plain text 17 to Bob using RSA. Compute the encrypted text and show how Bob will decrypt it. **10**

4. (a) Explain the principle of working of MP-III audio compression standard, with a neat block diagram. **10**
   (b) What are elliptic curves? Explain the "Elliptic curve Discrete Log" problem and hence explain ECC key exchange algorithm. **10**

[TURN OVER

5. (a) Explain any one lossless technique for image compression in detail.
   (b) What are digital signatures? Explain any one technique in detail.

6. Write short notes on **any two** :–
   (a) MPEG video compression standard
   (b) Hash and MAC functions
   (c) Digital Immune System
   (d) Diffie-Hellman key exchange
