BE - Sem VII - CBSGS - EXTC - DCE

2

06/06/16

QP Code : 31586

(3 Hours) [Total Marks :80

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

1. Answer the following (Any **five**)
   - (a) What are the measures of performances for lossy and lossless compression techniques? 4
   - (b) Illustrate the worst cast in LZ- 77 dictionary compression technique. 4
   - (c) What is "frequency/auditory masking" temporal mashing ? 4
   - (d) Which redundancies are exploited in JPEG lossy standard? Which are the processes using these redundancies? 4
   - (e) State fermat's little theorem (FLT) and Euler's theorem. Illustrate with an example how FLT can be used to find modular inverse. 4
   - (f) Using modular arithmetic and theorems, prove that decypted text is same as plain text in the RSA algorithm. 4
   - (g) What do you mean by "confusion" and "diffusion" ? Which components are used in ciphers to introduce confusion and diffusion? 4

2. (a) Generate a binary tag using arithmetic coding technique for the sequence : a b a c a b b 10

symbol	count
a	37
b	38
c	25

(b) Perform LZW dictionary compression on the following text string : wabba-wabba-wabba-wabba-woo-woo-woo Initial dictionary:- 10

Index	1	2	3	4	5
Entry	-	a	b	o	w

3. (a) Explain MP-III audio compression standard with a neat block diagram. 10
(b) What are different approaches for compressing an image? Explain JPEG-LS standard. 10

4. (a) Explain double DES and the need for it. Also explain the "meet-in-the-middle" attack. 10
(b) Explain any one digital signature algorithm in detail. 10

[TURN OVER

5. (a) Encrypt the plain text 63 using RSA algonithm which uses prime numbers $p = 7$ and $q = 11$. The public key $e = 13$. Verify that the deaypted text is same as the plain text. 10

(b) Alice chooses her private key $x = 3$ and Bob chooses $y = 6$. If both of them use the primitive root $g = 7$ for prime $p = 23$, what is the key exchanged between Alice and Bob using diffie. Hellman key exchange? 10

6. Write short notes on two. 20

(a) Adaptive Huffman coding

(b) H.264 encoder-decoder

(c) Eliptic curve cryptography

(d) Intrusion detection system