BE - sem - VII - CBGS - EXTC

DCE

17/12/15

Q.P. Code : 6193

(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. (a) Distinguish between cryptography and steganography 20
(b) A source emits latters A { a_1, a_2, a_3, a_4} with probabilities p (a_1) = 0.5 p (a_2) = 0.15 p (a_3) = 0.25 p (a_4) = 0.10 calculate the entropy of the source. Also find the huffman code with minimum variance.
(c) Define the chinese remainder theorem find the solution to the simultaneous equations.
$x = 2 \bmod 3$
$x = 3 \bmod 5$
$x = 2 \bmod 7$
(d) Define fermat's little theorem find the result of
(i) $3^{12} \bmod 11$
(ii) $3^{10} \bmod 11$

2. (a) Encode and decode the following sequence using Lz -77 and Lz - 78 algorithm. 20
w a b b a b r a r b a r r a c b a c
Give drawbacks of Lz-77 and Lz- 78 assume window size 9 for Lz - 77.
(b) What is MDC and MAC ? Explain HMAC in detail.

3. (a) Write a short note on μ-law and A-law companding 20
(b) Explain diffie hellman key exchange algorithm with an example. Also explain attack on diffie hellman key exchange

4. (a) Explain attack on double DES with example write with neat black diagram triple DES with two keys. 20
(b) Write short note on AES

5. (a) Write short note on H-264 encoder and decoder 20
(b) Explain Intrusion detection system in detail

6. Write short note (Any **three**) 20
(a) Ethical hacking
(b) Attacks on RSA
(c) JPEG - 2000
(d) Biometric Authentication.

MD-Con. 11740-15.