MCA.V/11.13.717

MCA DEGREE V SEMESTER EXAMINATION NOVEMBER 2013

CAS 2503/2305 CRYPTOGRAPHY AND NETWORK SECURITY

Time: 3 Hours Maximum Marks : 50

PART A
(Answer *ALL* questions)

(15 x 2 = 30)

I. (a) Mention the strength of DES.
(b) Explain about different security attack.
(c) Write a note on substitution and permutation.

II. (a) What is "one time pad".
(b) Write a note on different stages of AES.
(c) Explain about RC5.

III. (a) Write a note on public key cryptography.
(b) What is Diffie Hellman Algorithm?
(c) What is Primality Testing?

IV. Write about:
(i) Digital signature
(ii) Elliptic curve cryptography
(iii) Message digest

V. (a) Write about electronic payment system.
(b) Write a note on Kerberos.
(c) Write about digital watermarking.

PART B

(5 x 4 = 20)

VI. A. Write Euclid's and Mention its application in security.
OR
B. Explain Feistal cipher.

VII. A. Explain the working of IDEA symmetric encryption algorithm.
OR
B. Explain the working of Blowfish algorithm.

VIII. A. Consider a plaintext alphabet G, using RSA algorithm and the values as E = 3, D = 11 and N = 15, find out the encrypted text and verify that upon decryption, it transform back to G.
OR
B. Write about public key cryptography standards.

IX. A. Explain about HMAC.
OR
B. Explain digital certificate creation steps.

X. A. Explain about secure MIME (S/MIME).
OR
B. Write about secure socket layer.

***