MCA.V/11.15.0902 Reg. No. □□□□□□□□

D

MCA DEGREE V SEMESTER EXAMINATION NOVEMBER 2015

CAS 2504/2305 CRYPTOGRAPHY AND NETWORK SECURITY

(*Regular and Supplementary*)

Time: 3 Hours Maximum Marks: 50

PART A

(Answer *ALL* questions)

(15 × 2 = 30)

I. (a) Anne gives a cheque for ₹100 to buy a book. Later she finds that the cheque was cashed for ₹1000. Determine the type of security attack and the security service that is violated in this case.

(b) "For better security, the use of weak keys and semi weak keys should be avoided in DES algorithm". Do you agree with this statement? Justify your answer.

(c) What is avalanche effect? How is a ciphertext generated in triple DES?

II. (a) List the features of Blowfish algorithm.

(b) What is the significance of session key and master key in a key distribution system?

(c) How is decryption performed in AES algorithm?

III. (a) Explain an algorithm used to factorize large numbers.

(b) Explain how man-in-the-middle attack can happen in Diffie-Hellman key exchange method.

(c) Explain the divisibility algorithm for primality testing.

IV. (a) Give the general form of an elliptic curve. What do you mean by zero point of an elliptic curve?

(b) Differentiate between message authentication code and hash value.

(c) List the basic requirements for a digital signature.

V. (a) What is a Kerberos realm? List the activities involved when a user wishes to access a file server in a different realm.

(b) In PGP, compression is done before/after encryption and before/after generating the signature. Form the correct statement and justify your answer.

(c) Distinguish between transport and tunnel mode of IPSec.

PART B

(5 × 4 = 20)

VI. Determine the gcd(2740,1760).

OR

VII. Explain DES algorithm, with the help of a neat sketch.

VIII. Given, plaintext, P = 00 04 12 14 12 04 12 00 0C 00 13 11 08 23 19 19 and cipher key, K = 24 75 A2 B3 34 75 56 88 31 E2 12 00 13 AA 54 87. Show the value of state array after initial AddRound Key operation of AES algorithm.

OR

IX. Explain RC5 algorithm.

X. Given two prime numbers 23 and 37, public key 5 and private key 317, using RSA determine the ciphertext if the plaintext is 24.

OR

XI. Explain Miller-Rabin primality testing, with the help of an example.

XII. Write short note on Digital Signature Standard.

OR

XIII. Explain how a hash value is generated using HMAC.

XIV. Explain how PGP provides confidentiality and authentication for messages.

OR

XV. Write short note on SSL protocols.

***