K19P 1363

Reg. No. : ....

Name : ....

V Semester Master of Computer Application (M.C.A.)/ M.C.A. Lateral Entry Degree (Reg./Suppl./Imp.) Examination, November - 2019

(2014 Admission Onwards)

MCA 5C25 : INFORMATION SECURITY

Time : 3 Hours Max. Marks : 80

SECTION - A

Answer any **ten** questions. Each carries **three** marks.

(10 x 3=30)

1. Define steganography.

2. Specify the components of encryption algorithm.

3. Define encryption.

4. What are the functions of hash function?

5. Compare stream cipher and block cipher with example.

6. What is an elliptic curve?

7. Define block cipher operations.

8. Describe in general terms an efficient procedure for picking a prime number.

9. Define the classes of message authentication function.

10. Define virus. Specify the types of viruses

11. What are the common techniques used to protect a password file?

12. What are the key algorithms used in S/MIME?

P.T.O.

SECTION - B

Answer **all** questions. Each questions carries **ten** marks.

13. a) Define Cryptography. Discuss the various classical encryption techniques with suitable example. **(10)**

(OR)

b) Briefly discuss the available algebraic structures required for cryptography using suitable example. **(10)**

14. a) With a neat flowchart, explain the DES algorithm for 64 bit data and 64 bit key size. **(10)**

(OR)

b) Explain in detail, the key generation technique in AES algorithm and its expansion format. **(10)**

15. a) Explain Diffi - Helman key exchange in detail with an example. **(10)**

(OR)

b) Briefly explain the idea behind Elliptic Curve Cryptosystem. **(10)**

16. a) What are the design issues of key management and distribution neatly? **(10)**

(OR)

b) Briefly discuss the concept of PGP message transmission and reception technique. **(10)**

17. a) Explain the architecture of IP security. **(10)**

(OR)

b) i. Explain firewalls and how they prevent intrusions. **(10)**

ii. What is Kerberos? Explain how it provides authenticated service.