K20P 1252

Reg. No. : .....

Name : .....

V Semester Master of Computer Application (M.C.A.)/M.C.A. (Lateral Entry) Degree (CBSS-Reg./Suppl. (Including Mercy Chance)/Imp.) Examination, November 2020

(2014 Admission Onwards)

MCA5C25 : INFORMATION SECURITY

Time : 3 Hours

Max. Marks : 80

SECTION – A

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

1. Define confidentiality and authentication.
2. State the importance of Euclid's algorithm in cryptography.
3. Differentiate MAC and Hash function.
4. Compare transposition and substitution technique.
5. Compare stream cipher and block cipher with example.
6. List the design goals of firewalls.
7. What are the significant features of prime number in information security ?
8. What are the common techniques used to protect a password file ?
9. What are the roles of key expansion in AES ?
10. How IP security does offer the authentication and confidentiality services ?
11. What is an elliptic curve ?
12. What is MIME content type ?

(10×3=30)

P.T.O.

SECTION – B

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

13. a) List the available algebraic structures required for cryptography. Explain each one of them using suitable example. **10**

OR

b) Define cryptography. Discuss the various classical encryption techniques with suitable examples. **10**

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

OR

b) List out the design principles of block cipher, explain the merits of each one. **10**

15. a) Explain the key management of public key encryption in detail. **10**

OR

b) Describe the performance and applications of cryptographic hash using suitable example. **10**

16. a) Discuss about the objectives of HMAC and its security features. **10**

OR

b) Explain secure socket layer protocol stack with a neat diagram and define the different parameters used in session and connection states. **10**

17. a) How does PGP provide confidentiality and authentication service for e-mail and file storage applications ? Draw the block diagram and explain its components. **10**

OR

b) i) Explain in detail about Kerberos and its servers. **5**

ii) What are the positive and negative effects of firewall ? **5**

(5×10=50)