K21P 2602

Reg. No. : .....

Name : .....

V Semester M.C.A./M.C.A. (Lateral Entry) Degree (C.B.S.S. – Reg./Suppl./ Imp.) Examination, November 2021
(2016 Admission Onwards)
MCA 5C25 : INFORMATION SECURITY

Time : 3 Hours

Max. Marks : 80

PART – A

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

1. Draw and explain Symmetric Key Cryptography.
2. Discuss Transposition techniques.
3. Explain stegnography and its techniques.
4. Discuss congruence in cryptography with its properties.
5. Explain Euclidean Algorithm.
6. What are the strengths of DES ?
7. Explain the Evaluation criteria of AES.
8. Discuss Meet in the Middle Attack in 2DES.
9. What is ECB and mention its drawback ?
10. Explain RC4 Algorithm.
11. Illustrate and explain Public key Cryptography.
12. What is Kerberos ? Discuss its components.

(10×3=30)

P.T.O.

PART – B

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

13. a) Explain the different substitution techniques in cryptography. **10**

OR

b) i) Discuss field and its properties in cryptography. **5**

ii) Explain finite field and its types briefly. **5**

14. a) Draw and explain AES Algorithm. **10**

OR

b) Distinguish between Double DES and Triple DES briefly. **10**

15. a) i) Discuss the features of Discrete logarithms. **5**

ii) Briefly explain Diffie Helman Key Exchange. **5**

OR

b) i) Describe the concepts of Hash functions in cryptography briefly. **5**

ii) Explain SHA-512 Algorithm. **5**

16. a) i) Explain HMAC Algorithm. **5**

ii) Describe the importance of Digital Signature in cryptography briefly. **5**

OR

b) Explain key management in cryptography. **10**

17. a) i) Explain the importance of PGP. **5**

ii) What is Firewall ? Mention its properties. **5**

OR

b) i) Who is an Intruder ? What is an intrusion detection system ? **5**

ii) Explain IP security briefly. **5**

(10×5=50)