K17P 0207

Reg. No. : .....

Name : .....

Fifth Semester M.C.A. Degree (Regular) Examination, January 2017
MCA 5C25 : INFORMATION SECURITY
(2014 Admission)

Time : 3 Hours Max. Marks : 80

PART – A

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

1. What are the concepts of ciphers in cryptography ?
2. List out the merits of transposition techniques.
3. Discuss the merits of Linear congruence.
4. What are the strength of DES ?
5. What are the roles of key expansion in AES ?
6. Define block cipher operations.
7. Mention the uses of elliptic curve arithmetic in public key cryptography.
8. Define cipher block chaining.
9. What are the requirements of message authentication codes ?
10. What are the merits of secure hash function ?
11. Define digital signature.
12. What are the properties of MAC security ? **(10×3=30)**

PART – B

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

13. a) List out the security attacks and services, explain the importances of each one. **10**

OR

b) i) Define steganography, explain the properties and goals of steganography. **5**

ii) Explain the groups, rings and fields significance in cryptography. **5**

P.T.O.

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

OR

b) Explain the properties of block cipher operations with suitable examples. 10

15. a) i) Discuss the properties and goals of discrete logarithms briefly. 5

ii) Compare and contrast elliptic curve arithmetic and elliptic curve cryptography. 5

OR

b) Mention the goals and applications of various hash functions briefly. 10

16. a) Describe the concepts of MAC security in message authentication requirements, briefly. 10

OR

b) What are the design issues of key management and distribution neatly ? 10

17. a) Distinguish between IP and Web security protocols uses in cryptography. 10

OR

b) i) Explain importance of S/MIME. 5

ii) Discuss the properties of Firewall and Intrusion detection. 5

(5×10=50)