K18P 0052

Reg. No. : .....

Name : .....

Fifth Semester M.C.A. Degree (Regular/Supplementary/Improvement) Examination, January 2018
(2014 Admission Onwards)
MCA 5C25 : INFORMATION SECURITY

Time : 3 Hours

Max. Marks : 80

PART – A

Answer **any ten** questions, **each** question carries **three** marks.

1. List out the various security attacks.
2. What are the key roles of modular arithmetic ?
3. Compare rings and fields related to cryptography.
4. Compare and contrast differential and linear cryptanalysis.
5. Discuss the key expansion in AES requirements for any specific application.
6. Define multiple encryption.
7. What are the significant of factoring large numbers ?
8. What are the merits of hash function ?
9. What are the key roles of prime numbers in public key cryptography ?
10. How to make use elliptic curve arithmetic in cryptography
11. Mention the uses of MAC Security.
12. Define user authentication.

(10×3=30)

P.T.O.

PART – B

Answer **all** questions, **each** question carries **ten** marks.

13. a) List out the different encryption techniques. Explain each one with suitable examples. **10**

OR

b) Discuss the importance of Euclid's algorithm and their merits briefly. **10**

14. a) Compare and contrast DES and AES structure and design principles briefly. **10**

OR

b) List out various multiple encryption. Explain the significance of each one. **10**

15. a) What are the various steps involved in performing the operations of public key cryptography ? **10**

OR

b) Mention the principles of public key crypto systems and explain the importance of each of them. **10**

16. a) Explain the importance of Message authentication requirements and functions briefly. **10**

OR

b) How to manage symmetric key management using symmetric and asymmetric encryption ? **10**

17. a) Discuss importance and design issues of electronic mail security tools. **10**

OR

b) i) Explain the design issues of firewall. **5**

ii) Compare and contrast virus and related threats. **5**