K19P 0002

Reg. No. : ....

Name : ....

Fifth Semester M.C.A. Degree (Reg./Supple./Imp.) Examination, January 2019 (2014 Admn. Onwards) MCA5C25 : INFORMATION SECURITY

Time : 3 Hours

Max. Marks : 80

SECTION – A

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

1. Differentiate symmetric and asymmetric encryption.
2. What are the significant features of prime number in information security ?
3. Why network need security, justify.
4. Find gcd (56, 86) using Euclid's algorithm.
5. What are the security options PGP allows when sending an email message ?
6. What is cryptanalysis and cryptography ?
7. What are the properties of digital signature ?
8. What is message authentication ?
9. Define digital signature.
10. What are the essential ingredients of the public key directory ?
11. Mention the scenario where Kerberos scheme is preferred.
12. What are the properties of MAC security have ? **(10×3=30)**

SECTION – B

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

13. a) Define encryption. Describe the various classical encryption techniques with suitable example. **10**

OR

b) Define Steganography. Discuss the various classical encryption techniques with suitable example. **10**

P.T.O.

14. a) What requirements must a public key cryptosystem to fulfil to a secured algorithm ? 10

OR

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

15. a) Discuss the discrete logarithm and Diffi-Hellman key exchange algorithm with its merits and demerits. 10

OR

b) Explain the Kerberos version 4 -message exchanges. 10

16. a) Describe HMAC algorithm in detail. 10

OR

b) Write the digital signature algorithm. With a block diagram explain functions of signing and verification of digital signature. 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 the types of Host based intrusion detection. List any two IDS software available. 10

ii) Explain in detail about various schemes of digital signature.