K18U 0184

Reg. No. : .....

Name : .....

VI Semester B.C.A. Degree (CBCSS – Reg./Supple./Imp.) Examination, May 2018
Core Course (Elective)
6B19BCA : E01 : INFORMATION SECURITY
(2014 Admn. Onwards)

Time : 3 Hours Max. Marks : 40

SECTION – A

1. **One** word answer : **(8×0.5=4)**
   a) In asymmetric key Cryptography _____ key is kept as secret.
   b) _____ is used to find some insecurity in a cryptographic scheme.
   c) _____ algorithm is used only for key exchange.
   d) MIC stands for _____
   e) Message block size of SHA 512 is _____
   f) _____ is an example for Digital Signature Standard.
   g) Data Encryption Standard also called as _____
   h) _____ is the first step in DES.

SECTION – B

Write short notes on **any seven** of the following questions : **(7×2=14)**

2. Briefly explain different goals of security.
3. List different categories of virus.
4. What is transposition cipher ?
5. Explain one time padding.
6. List strengths of DES.

P.T.O.

7. Is use of weak keys and semi weak keys are considered as fault in DES ? Why ?

8. Define Eulerstotient phi function.

9. Give any two applications of Public key system.

10. What is Message Authentication code ?

11. How Steganography differs from Cryptography ?

SECTION – C

Answer **any four** of the following questions : **(4×3=12)**

12. With a suitable diagram explain a model for network security.

13. Encrypt "ENEMY MUST BE STOPPED" with key "OCCURRENCE" and play fair ciphering.

14. Explain Triple DES with suitable diagram.

15. Briefly explain any three vulnerabilities identified in DES.

16. Prepare cipher text corresponding to message M = 10 using RSA if public key is [n=39 & e=5].

17. Explain attacks possible on Digital Signatures.

SECTION – D

Write an essay on **any two** of the following : **(2×5=10)**

18. List and briefly explain different categories of security services.

19. With a suitable block diagram explain overall structure of DES.

20. Explain RSA algorithm with a suitable example.

21. What is a Hash function ? Explain the requirements for a secure Hash function.