K21U 0190

Reg. No. : .....

Name : .....

VI Semester B.C.A. Degree (CBCSS – Reg./Supple./Improv.) Examination, April 2021
(2014-2018 Admissions)
Core Course (Elective)
6B19BCA:E01 : INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

SECTION – A

1. **One** word answer : (8×0.5=4)
   a) The service that makes sure that only authorized users can access the data is called _____
   b) _____ helps in non-repudiation.
   c) Breaking of code without knowledge of the key and plaintext is also known as _____
   d) DES stands for _____
   e) In double DES data encryption is done _____ times.
   f) RSA uses _____ key length.
   g) A condensed version of data is called _____
   h) The key length for a secure RSA transmission is typically _____ bits.

SECTION – B

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

2. Define plaintext.
3. What is cryptography ?
4. What is symmetric encryption ?
5. What is a Trojan Horse ?

P.T.O.

6. List four examples for block ciphers.

7. Give any four weakness of DES.

8. State the weaknesses of public keys.

9. What is non-repudiation ?

10. What is a stream cipher ?

11. What is brute force attack ?

12. What is a parasitic virus ?

13. What are advantages of using Digital Signatures ?

14. What is linear cryptanalysis ?

15. How is key length related to encryption strength ?

SECTION – C

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

16. Compare symmetric and asymmetric encryption.

17. Differentiate between passive and active attacks.

18. Explain public key encryption.

19. Explain the RSA algorithm.

20. Explain three reasons why digital signatures are used in communication.

21. Discuss about substitution ciphers.

22. Distinguish between Virus and Worms.

23. Explain the working of symmetric encryption.

SECTION – D

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

24. Explain working of DES.

25. Discuss working of digital signature.

26. Explain about transposition ciphers.

27. Describe the elements in information security.

28. Discuss about Malwares.

29. Explain about
    i) Steganography.
    ii) Differential cryptanalysis.