K22U 2254

Reg. No. : ....

Name : ....

V Semester B.C.A. Degree (CBCSS-OBE-Regular/Supplementary/ Improvement) Examination, November 2022
(2019 Admission Onwards)
Core Course
5B16BCA – E01 INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

PART – A
Short Answer

Answer **all** questions : **(6×1=6)**

1. What do you mean by confidentiality ?
2. What do you mean by substitution cipher ?
3. What do you mean by cryptanalysis ?
4. List out any two private key algorithms.
5. What are the principles of a public key cryptographic algorithm ?
6. What do you mean by message authentication ?

PART – B
Short Essay

Answer **any 6** questions : **(6×2=12)**

7. List out the needs for information security.
8. What is a symmetric key ?
9. List out some weaknesses of DES algorithm.
10. What are the criteria that a cryptographic hash function must satisfy ?

P.T.O.

11. What do you mean by cryptanalysis system ?

12. What are the benefits of RSA digital signature ?

13. What is steganography ?

14. What are the features of Trogan horse ?

PART – C
Essay

Answer **any 4** questions : **(4×3=12)**

15. Briefly explain various principles of security.

16. What are various categories of traditional ciphers ?

17. Explain brute force attack.

18. Differentiate public key and private key cryptographic systems.

19. What do you mean by message digest ?

20. Explain Kirchoff's principle of cryptography.

PART – D
Long Essay

Answer **any 2** questions : **(2×5=10)**

21. Describe various types of security attacks.

22. Explain DES algorithm in detail.

23. Describe RSA algorithm.

24. Compare various digital signature schemes.