K25U 2475

Reg. No. : .....

Name : .....

V Semester B.C.A. Degree (CBCSS – OBE – Regular/Supplementary/ Improvement) Examination, November 2025
(2019 to 2023 Admissions)
Core Course
5B16BCA-E01 : INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

PART – A
(Short Answer) **(6×1=6)**

Answer **all** questions.

1. Define integrity in the context of security services.
2. What is a substitution cipher ?
3. Define active attack with example.
4. What is the function of the initial permutation in DES ?
5. Mention two types of key cryptosystems.
6. What is the significance of digital certificate ?

PART – B
(Short Essay) **(6×2=12)**

Answer **any 6** questions.

7. Explain the need for security in digital communication systems.
8. Differentiate between keyed and keyless ciphers with examples.
9. Describe the functions of the final permutation in DES.
10. Explain linear cryptanalysis and its relevance to DES.

P.T.O.

11. What do you mean by signing a digest in digital signatures ?

12. List the requirements of a secure public key cryptosystem.

13. Explain the purpose of message authentication and non-repudiation.

14. Describe the computational aspects of RSA algorithm.

PART – C
(Essay) **(4×3=12)**

Answer **any 4** questions.

15. Compare the structure and usage of monoalphabetic and polyalphabetic ciphers.

16. Explain differential cryptanalysis with reference to symmetric key encryption.

17. Describe the key services provided by digital signatures.

18. Explain the concept and components of RSA digital signature schemes.

19. How does a public key ensure message confidentiality and integrity ?

20. Explain the various categories of cryptanalysis attacks.

PART – D
(Long Essay) **(2×5=10)**

Answer **any 2** questions.

21. Explain the cryptanalysis techniques used to break DES encryption.

22. Explain RSA algorithm.

23. Write an essay on the digital signature schemes.

24. Explain symmetric cipher design using substitution and transposition techniques.