K23U 2302

Reg. No. : .....

Name : .....

V Semester B.C.A. Degree (C.B.C.S.S. – O.B.E. – Regular/ Supplementary/ Improvement) Examination, November 2023
(2019-2021 Admissions)
Core Course
5B16BCA-E01 : INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

PART – A

Short Answer

Answer **all** questions. **(6×1=6)**

1. What is an affine cipher ?
2. What do you mean by DES ?
3. List the four possible approaches to attack RSA algorithm.
4. What is Avalanche effect ?
5. What are the security services provided by a digital signature ?
6. What is a CCA ?

PART – B

Short Essay

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

7. Distinguish between passive attacks and active attacks.
8. What is the difference between asymmetric and symmetric cryptography ?
9. Explain why all block ciphers are polyalphabetic.

P.T.O.

10. Write a note on Kirchhoff's principle.

11. What is double DES ?

12. What is blinding ?

13. Distinguish between key only attack and known message attack on digital signature.

14. What is the difference between existential and selective forgery ?

PART – C
Essay

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

15. Briefly explain the basic information security principle.

16. Explain cryptanalysis and its common types.

17. Briefly explain the RSA digital signature scheme.

18. Write down the applications and requirement for public key cryptosystem.

19. What is a digital signature ? Explain the difference between conventional and digital signature.

20. Describe the cipher and reverse cipher generation in DES.

PART – D
Long Essay

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

21. Explain various types of information security attacks.

22. What is a substitution cipher ? Explain various monoalphabetic and polyalphabetic ciphers.

23. Briefly explain the structure of DES.

24. With an example explain the RSA algorithm.
