K25U 0129

Reg. No. : .....

Name : .....

Sixth Semester B.Sc. Degree (C.B.C.S.S. – OBE-Regular/Supplementary/ Improvement) Examination, April 2025
(2019 to 2022 Admissions)
DISCIPLINE SPECIFIC ELECTIVE IN COMPUTER SCIENCE
6B15CSC-A : Information Security

Time : 3 Hours Max. Marks : 40

PART – A
(Short Answer)

Answer **all** questions. **(6×1=6)**

1. What is integrity in information security ?
2. Define a worm.
3. What is a passive attack ?
4. What is a substitution cipher ?
5. What are weak keys in DES ?
6. Define message integrity.

PART – B
(Short Essay)

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

7. Explain the principle of authentication.
8. Differentiate between viruses and worms.
9. What is a keyed transposition cipher ?
10. Describe the concept of cryptanalysis.

P.T.O.

11. What is the completeness effect in DES ?

12. Explain differential cryptanalysis.

13. Describe the application of public key cryptosystems.

14. What are the types of digital signature forgery ?

PART – C

(Essay)

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

15. Discuss the need for information security.

16. What is factoring problem in RSA ?

17. What is the structure of a block cipher ?

18. Explain double DES and triple DES.

19. Describe the RSA digital signature scheme.

20. Explain how a digital signature ensures non-repudiation.

PART – D

(Long Essay)

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

21. Explain the principles of information security with examples.

22. Describe mono-alphabetic and polyalphabetic substitution ciphers.

23. Explain the brute-force and linear cryptanalysis techniques used against DES.

24. Discuss the process of creating and verifying a digital signature, including its services.

———————