K23U 0484

Reg. No. : ....

Name : ....

VI Semester B.Sc. Degree (CBCSS – OBE – Regular/Supplementary/ Improvement) Examination, April 2023
(2019 and 2020 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 Cryptography ?
2. What is Digital Signature ?
3. What is Substitution cipher ?
4. What is Block cipher ?
5. What is confidentiality ?
6. What is Trapdoor One-Way Function ?

PART – B
(Short Essay)

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

7. List the security services provided by a digital signature.
8. Differentiate between symmetric cipher and asymmetric cipher.
9. Distinguish between passive and active security attacks.

P.T.O.

10. What is brute-force attack ?

11. What is non-repudiation ?

12. What is linear cryptanalysis ?

13. What is DES ?

14. What is Trojan horse ?

PART – C

(Essay)

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

15. Compare and contrast a conventional signature and a digital signature.

16. What is Kerckhoff's principle ?

17. Explain multiple DES.

18. What is signing the digest ?

19. Explain various attacks on block ciphers.

20. Briefly explain the idea behind the RSA cryptosystem.

PART – D

(Long Essay)

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

21. Explain the different security attacks on confidentiality, integrity and availability.

22. Explain the security of RSA.

23. What is block cipher ? Explain various modes of operation of a block cipher.

24. Compare and contrast a conventional signature and a digital signature.