K21U 4675

Reg. No. : .....

Name : .....

V Semester B.C.A. Degree CBCSS (OBE) Regular Examination, November 2021
(2019 Admn. Only)
Core Course
5B16BCA-E01 – INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

PART – A

Short Answer

Answer **all** questions : (6×1=6)

1. List the goals of Information security.
2. Define Cryptography.
3. A cryptanalyst may use _____ attack to break the cipher.
4. DES is a block cipher. State True or False.
5. Expand RSA.
6. Name any two attacks on RSA signature.

PART – B

Short Essay

Answer **any 6** questions : (6×2=12)

7. Differentiate Active and Passive attacks.
8. Explain about Known plain text attack with neat sketch.
9. Write short note on encryption and decryption with DES.
10. Mention some weaknesses found in the cipher design of DES.

P.T.O.

11. What is the principle of public key cryptosystems ?

12. What are the applications of key cryptosystems ?

13. Explain about adding confidentiality to a digital signature.

14. Define forgery. Explain its types.

PART – C

Essay

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

15. Write short note on Principles of Security.

16. Explain about polyalphabetic ciphers with example.

17. Explain about the key generation in DES with diagram.

18. Write and explain the RSA algorithm.

19. Explain the differences between the conventional signature and digital signature.

20. Write note on public key cryptosystems.

PART – D

Long Essay

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

21. Explain in detail about the attacks threatening confidentiality, integrity and availability.

22. Explain in detail about the classifications of transposition ciphers with example.

23. Explain about Multiple Data Encryption Standard (Multiple DES).

24. Explain in detail about RSA digital signature scheme.