



K20U 0103

Reg. No. :

Name :

VI Semester B.Sc. Degree (CBCSS-Reg./Supple./Improv.)

Examination, April 2020

(2014 Admission Onwards)

CORE COURSE IN COMPUTER SCIENCE

6B16CSC:E06 : Information Security

Time : 3 Hours

Max. Marks : 40

PART – A

1. a) An attack that threatens confidentiality of information is _____
- b) The process of converting cipher text to plain text is _____
- c) The art and science of creating secret code is _____
- d) An example for block cipher is _____
- e) Expand DES.
- f) Give an attack on RSA signature.
- g) RSA stands for _____
- h) Secret key encryption is _____ encryption. **(8×0.5=4)**

PART – B

Answer **any seven**.

2. Define integrity.
3. What are viruses ?
4. What are substitution ciphers ? Give an example.
5. What is a public key ?
6. Mention any two applications of steganography.
7. What are block ciphers ?

P.T.O.

K20U 0103



8. What is message authentication ?
9. What is a brute force attack ?
10. What is Non-Repudiation ?
11. Give an overview of encryption and decryption with DES.

(7×2=14)

PART – C

Answer any four.

12. Which are the keys used in public key cryptosystems ? How are they used ?
13. What are the security goals ?
14. Explain the permutation steps in DES.
15. Explain the properties of a block cipher.
16. Compare conventional signatures and digital signatures.
17. What is the need for keys in digital signatures ?

(4×3=12)

PART – D

Answer any two.

18. Explain transposition ciphers.
19. Write notes on Security of DES.
20. Explain the applications of key cryptosystems.
21. Explain RSA Algorithm.

(2×5=10)