



K22U 0384

Reg. No. :

Name :

**VI Semester B.Sc. Degree (CBCSS – OBE – Regular) Examination, April 2022
(2019 Admission)
CORE COURSE IN COMPUTER SCIENCE
Discipline Specific Elective
6B15CSC – A : Information Security**

Time : 3 Hours

Max. Marks : 40

**PART – A
(Short Answer)**

Answer **all** questions : **(6×1=6)**

1. What are the characteristics of Information Security ?
2. What is passive attack ?
3. Explain the method of hashing in cryptography.
4. Are all stream ciphers mono-alphabetic and all block ciphers poly-alphabetic ?
5. What is block size and cipher key size in DES ?
6. Explain the requirement of Digital Signatures.

**PART – B
(Short Essay)**

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

7. Differentiate between virus and worms.
8. Discuss the need for security.
9. Differentiate between mono and poly alphabetic substitution ciphers.
10. Define the attacks repudiation and traffic analysis. Are they passive or active attacks ?

P.T.O.



11. Which security mechanism can be utilized, when an instructor demands student identification and password for students to log into a course ?
12. Encrypt the message 'This is a test' using additive cipher with key = 20. Do not consider the space between words.
13. Discuss the properties avalanche effect and completeness effect with respect to DES.
14. Differentiate RSA and DSS approaches to Digital Signatures.

PART – C

(Essay)

Answer **any 4** questions :

(4×3=12)

15. Explain the security goals.
16. Explain Kerckhoff's principle.
17. How symmetric key encipherment differs from asymmetric key encipherment ?
18. Explain the combination of keyless and keyed transposition ciphers.
19. What are the use of keys in cryptography ? Explain the concept of public and private keys.
20. Explain the Digital Signature Services.

PART – D

(Long Essay)

Answer **any 2** questions :

(2×5=10)

21. Compare and contrast between steganography and cryptography in detail.
 22. Write notes on modern block ciphers and modern stream ciphers.
 23. Provide detail explanation on the structure, analysis and security of DES.
 24. What are the properties of a digital signature ? Also provide notes on the threats associated with a direct digital signature scheme.
-