K19U 0098

Reg. No. : ....

Name : ....

VI Semester B.Sc. Degree (CBCSS – Reg./Supple./Improv.) Examination, April 2019
(2014 Admission Onwards)
CORE COURSE IN COMPUTER SCIENCE
6B16CSC : E06 : Information Security

Time : 3 Hours

Max. Marks : 40

PART – A

1. a) __________ is a principle of security.

   b) __________ means converting plain text to cipher text.

   c) The science and art of breaking secret code is

   d) DOS stands for ________

   e) If each occurrence of a character has different substitution, it is __________ substitution.

   f) Expand NIST.

   g) After parity drop operation, if a key consists of all 0's or 1's or half 0's and half 1's, they are _________ keys.

   h) _________ feistel rounds are present in encryption in DES. **(8×0.5=4)**

PART – B

Answer **any seven** :

2. Define confidentiality.

3. Differentiate passive attacks and active attacks.

4. Define digital signature.

5. Define Kirchhoff's principle.

P.T.O.

6. Give and explain any two properties of a block cipher.
7. What is a private key ?
8. What is steganography ?
9. What do you mean by cipher text ?
10. Explain linear cryptanolysis.
11. What is Trojan Horse ? **(7×2=14)**

PART – C

Answer **any four** :

12. What is public key encryption ? Explain its main elements.
13. Explain security attacks.
14. What are cryptanolysis attacks ?
15. Explain keyless and keyed transposition ciphers.
16. Explain the weaknesses of DES.
17. Explain digital signature process. **(4×3=12)**

PART – D

Answer **any two** :

18. Explain DES structure.
19. Write notes on RSA digital signature scheme.
20. Explain the applications of key crypto systems.
21. Explain the various types of attacks. **(2×5=10)**

———————