K18U 0097

Reg. No. : ....

Name : ....

VI Semester B.Sc. Degree (CBCSS – Reg./Supple./Imp.) Examination, May 2018
CORE COURSE IN COMPUTER SCIENCE
(Elective)
6B16CSC : E06 : Information Security
(2014 Admn. Onwards)

Time : 3 Hours | Max. Marks : 40

SECTION – A

1. **One** word answer : **(8×0.5=4)**

a) ______________ is a standalone malware computer program that replicates itself in order to spread to other computers.

b) ______________ is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

c) ____________ is a method of encrypting text in which a cryptographic key and algorithm are applied to a block of data.

d) DES stands for ____________

e) Vignere table is an example of ________________

f) _____________ uses fixed substitution over the entire message.

g) _______________ is a mathematical scheme for demonstrating the authenticity of digital message or documents.

h) ___________ is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions.

SECTION – B

Write short notes on **any seven** of the following questions : **(7×2=14)**

2. Define worms.

3. Explain cryptography.

4. Define stream cipher.

P.T.O.

5. Define mono alphabetic cipher.

6. Explain DES structure.

7. What is known as linear cryptanalysis ?

8. Explain the security of RSA.

9. Explain triple DES.

10. Define integrity.

11. Explain the term duplicity.

SECTION – C

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

12. Difference between cryptography and steganography.

13. What is known as transposition ciphers ?

14. Explain the requirement for public key cryptosystem.

15. Explain the weakness of DES.

16. Difference between double DES and triple DES.

17. Explain :
    a) Message Authentication
    b) Message Integrity.

SECTION – D

Answer **any two** of the following questions : **(2×5=10)**

18. Explain Kirchhoff's principle.

19. Explain Substitution Ciphers.

20. Define initial permutation, final permutation and key generation in DES.

21. Explain Brute-Force attack.