K17U 0343

Reg. No. : .....

Name : .....

**VI Semester B.Sc. Degree (CBCSS – Regular) Examination, May 2017**
**CORE COURSE IN COMPUTER SCIENCE**
**(Elective)**
**6B16CSC : E06. Information Security**
**(2014 Admn.)**

Time : 3 Hours Max. Marks : 40

SECTION – A

1. **One** word answer : **(8×0.5=4)**
   a) _____ is any malicious computer program which is used to hack into a computer by misleading users of its true intent.
   b) _____ is the science of hiding information.
   c) _____ is a symmetric key cipher, each plain text digit is encrypted one at a time with the corresponding digit of the key stream.
   d) DES stands for _____
   e) _____ is a trial and error method used by application programs to decode encrypted data.
   f) In cryptography, _____ is a general form of cryptanalysis based on finding affine approximations to the action of a cipher.
   g) _____ is a mathematical scheme for demonstrating the authenticity of digital message or documents.
   h) _____ refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document.

SECTION – B

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

2. Define passive attacks.
3. What is known as virus ?
4. Define block cipher.

P.T.O.

5. Define polyalphabetic cipher.
6. Explain the properties of DES.
7. What is known as differential cryptanalysis ?
8. Explain the security of RSA.
9. Explain the principles of public key cryptosystems.
10. Define message authentication.
11. What does the term confidentiality means ?

SECTION – C

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

12. Difference between virus and worms.
13. What is known as traditional symmetric key ciphers ?
14. Define RSA algorithm.
15. What is meant by public key cryptanalysis ?
16. Define the term inclusion.
17. Needs for keys in digital signature.

SECTION – D

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

18. Explain various types of attacks.
19. Difference between block cipher and stream cipher.
20. Define RSA digital signature scheme.
21. Explain the applications of key crypto systems.

---