Reg. No. : ....

Name : ....

VI Semester B.Sc. Degree (CBCSS – Supple./Improv.) Examination, April 2022
(2016 – 2018 Admissions)
CORE COURSE IN COMPUTER SCIENCE
(Elective)
6B16CSC-E06 : Information Security

Time : 3 Hours   Max. Marks : 40

SECTION – A

1. **One** word answer.   (8×0.5=4)

   a) DES stands for

   b) A _____ attack attempts to learn or make use of information from the system but does not affect system resources.

   c) The encryption method that applies a deterministic algorithm along with a symmetric key is known as

   d) A _____ is a mathematical scheme for verifying the authenticity of digital messages or documents.

   e) _____ is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.

   f) If an input is changed slightly, then the output changes significantly and this consequence is termed as

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

   h) _____ uses the private and the public key of the receiver.

SECTION – B

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

2. Narrate the goals of information security.

3. Define a symmetric key cipher.

4. Write about general structure of DES.

5. List any 4 properties of S box.

6. What is meant by digital signature ?

7. Differentiate between virus and worm. ,

8. What is RSA ?

9. Write about the feebleness in DES.

10. Which are the different types of attack on digital signature ?

11. Define brute force attack.

SECTION – C

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

12. Distinguish between active and passive attacks.

13. Explain Kerckhoffs's principle.

14. How monoalphabetic cipher differs from polyalphabetic cipher ?

15. Write an algorithm for round key generation.

16. Compare and contrast conventional signature and digital signature.

17. Give details about cryptosystem.

SECTION – D

Answer an essay on **any two** of the following questions.   **(2×5=10)**

18. Explain about cryptography and steganography.

19. Describe the different types of symmetric key ciphers.

20. Write about RSA digital signature scheme and attacks on RSA digital signature.

21. Elaborate on DES structure and DES functions.

_____