K20U 0190

Reg. No. : .....

Name : .....

VI Semester B.C.A. Degree (CBCSS-Reg./Supple./Improv.) Examination, April 2020
(2014 Admission Onwards)
Core Course (Elective)
6B19 BCA – E01 : INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

SECTION – A

1. **One word** questions. **(8×0.5=4)**
   a) The term cryptography refers to transforming messages to make them secure and immune to
   b) Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not
   c) Additive ciphers are also called as
   d) _____ cipher does not substitute one symbol for another, instead it changes the location of the symbol.
   e) _____ means a change in the plaintext should create a significant change in the ciphertext.
   f) What is the preprocess step before key expansion in a compression ?
   g) Which algorithm accepts the cipher text and the matching key to produce the original plaintext ?
   h) Which type of attack exploits properties of the RSA algorithm ?

SECTION – B

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

2. Define the term worms.
3. Discuss active attacks.

P.T.O.

4. Write short note on Kerckhoff's principle.
5. Distinguish between encryption and decryption algorithm with example.
6. Explain weakness of the cipher key.
7. Write short note on substitution ciphers.
8. What is message integrity ?
9. Explain elliptic curve digital signature scheme.
10. What are the principle elements of a public key cryptosystem ?
11. Explain the concept of trap door one way function.

SECTION – C

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

12. Explain secret sharing.
13. Write short on monoalphebetic cipher.
14. What are the two desired properties of a block cipher ?
15. Discuss DES analysis.
16. Compare and contrast existential and selective forgery.
17. Write short note on RSA data security.

SECTION – D

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

18. What are stream and block ciphers ? Explain how stream ciphers are different from block ciphers.
19. Distinguish between keyless and keyed transposition cipher, in detail.
20. Explain RSA algorithm in detail.
21. Explain the requirements for public key cryptography.
