K17U 0428

Reg. No. : ....

Name : ....

VI Semester B.C.A. Degree (CBCSS – Regular) Examination, May 2017
(2014 Admn.)
Core Course in BCA (Elective)
6B19BCA : E01. INFORMATION SECURITY

Time : 3 Hours Max. Marks : 40

SECTION – A

1. **One** word answer: (8×0.5=4)

   a) In cryptography an encrypted text is called ______________

   b) The order of the letters in a message is rearranged by ___________

   c) ElGamal encryption system is an example for ___________

   d) MD5 Developed by _____________

   e) Digest size of SHA 1 is _____________

   f) The success of RSA is based on ____________

   g) Meet in the middle attack introduced by ___________

   h) DES consists of _________ rounds to perform the substitution and transposition.

SECTION – B

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

2. List essential ingredients of Symmetric Key Cryptography.

3. Differentiate Virus and Worm.

4. Define Mono alphabetic cipher.

5. Construct a play fair matrix using the key "LARGEST".

6. What is the purpose of S-Box in DES ?

P.T.O.

7. Explain Differential Cryptanalysis in DES.

8. Give one trap door function for Public key cryptography.

9. Evaluate phi(30).

10. What is Message Integrity Checksum ?

11. What is nonrepudiation ?

SECTION – C

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

12. With a suitable diagram explain Access control security model.

13. Encrypt "WE ARE DISCOVERED SAVE YOURSELF" with key "DECEPTIVE" and Vignere ciphering.

14. Write notes on :

    Avalanche effect

    Completeness effect.

15. With a suitable block diagram explain key generation in DES.

16. Briefly explain the components of Public key system.

17. What is a Digital Signature Standard ?

SECTION – D

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

18. List and briefly explain categories of Passive and Active attacks.

19. What is a P – Box ? Explain the uses of P-boxes in a round of DES.

20. If the received cipher text C = 8 and know the public key of user as [n = 33 and e = 13]. Find decryption key d and recover the message.

21. Explain RSA digital signature scheme.