Roll No. | | | | | | | | | | | | **Total No. of Pages : 02**

Total No. of Questions : 18

B.Tech.(CSE) (2012 to 2017 E-I) (Sem.–6)

INFORMATION SECURITY

Subject Code : BTCS-904

M.Code : 71113

Time : 3 Hrs. **Max. Marks : 60**

INSTRUCTION TO CANDIDATES :

1. **SECTION-A is COMPULSORY consisting of TEN questions carrying TWO marks each.**
2. **SECTION-B contains FIVE questions carrying FIVE marks each and students have to attempt any FOUR questions.**
3. **SECTION-C contains THREE questions carrying TEN marks each and students have to attempt any TWO questions.**

SECTION-A

Answer briefly :

1. Difference between Active and Passive attack.
2. What is Non repudiation?
3. What does CIA stand for?
4. Difference between authorization and authentication.
5. What are digital signatures?
6. Define PGP.
7. What is authentication header?
8. Define Malware.
9. List some firewall design principles.
10. What is Caeser Cipher?

SECTION-B

11. Explain difference public key and private key cryptography mechanisms.

12. Explain different substitution techniques for cryptography.

13. Discuss some benefits and applications of IPsec.

14. Describe Differential Cryptanalysis and Linear Cryptanalysis for DES.

15. What is e-mail security? What are different protocols for e-mail security?

SECTION-C

16. Explain public key cryptography. Discuss RSA public key encryption algorithm with the help of example.

17. What are web security threats? Give countermeasures of web security threats. What is difference between HTTP and HTTPS protocol?

18. Write a Short note on :

    a. Steganography

    b. Trojan horse

    c. Stream cipher

    d. MD5

NOTE : Disclosure of identity by writing mobile number or making passing request on any page of Answer sheet will lead to UMC case against the Student.