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

Total No. of Questions : 18

B.Tech. (CSE/ IT) (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. Define data confidentiality.
2. What is steganography in information security?
3. Define substitution techniques.
4. What is random number generator?
5. Write a short note on RSA.
6. Discuss the importance of digital signatures.
7. Write the purpose of TLS.
8. Give introduction of IPSec.
9. What is meant by Kerberos?
10. What is Malicious software in Information Security?

SECTION-B

11. Explain and draw the network security model.

12. Explain the principle of Diffie Hellman Key Exchange algorithm by taking an example.

13. Discuss the use of Message Authentication Code algorithm to provide message authentication.

14. What is X. 509 authentication service and what is its purpose?

15. How Secure Electronic Transaction (SET) is used for the security of financial transactions on the Internet?

SECTIONC

16. Explain the functioning of DES algorithm using the block diagram. Discuss the strength of DES.

17. Discuss the Web Security issues. Which are the key Web services security requirements?

18. What are Firewalls? Illustrate how they denies the viruses and related threats?

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.