

Roll No.

Total No. of Pages : 02

Total No. of Questions : 09

B.Tech.(CSE) (Sem.-6)

INFORMATION SECURITY

Subject Code : BTCS-904

M.Code : 71113

Date of Examination : 14-07-22

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

1. Answer briefly :

- a. Information security policy
- b. Symmetric *versus* Asymmetric Encryption
- c. Diffie-Hellman key exchange
- d. Secure Socket Layer
- e. Authentication Header
- f. Cryptanalysis
- g. IPv4 vs. IPv6
- h. Firewall Policies
- i. Authentication Header
- j. Confidentiality.

SECTION-B

2. Describe various security mechanisms defined in X.509.
3. What are the important features of Message digest algorithms?
4. Illustrate advantages of using symmetric ciphers for network security.
5. What are the various standards of Digital Signature?
6. What is need of encapsulation in security? How it is achieved in Networks?

SECTION-C

7. What are the problems associated with digital signatures? What are the different authentication protocols to secure the transmission of information?
8. Explain strengths and weaknesses of DES. Differentiate between differential and linear cryptanalysis. What are advantages of using Triple DES?
9. How firewall filter network traffic? Explain its working with a diagram.

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.