15104

15104

M. Tech. I - Sem. (Main) Exam., Dec. - 2018

Computer Science & Engineering

1MCS4.2 Information System Security

Time: 3 Hours **Maximum Marks: 100**

Min. Passing Marks: 33

Instructions to Candidates:

*Attempt any **five questions,** Marks of questions are indicated against each question. Draw neat and comprehensive sketches wherever necessary to clearly illustrate your answer. Assume missing data suitable if any and specify the same. Use of following supporting material is permitted during examination. (Mentioned in form No. 205)*

1. NIL 2. NIL

Q.1 (a) Explain principle behind One Time Pads. Why they are highly secure? [10]

(b) What is Play Fair Cipher? Explain in detail. [10]

Q.2 (a) Explain various types and modes of symmetric key algorithms. [10]

(b) Explain principal of DES algorithm with the help of diagram. [10]

Q.3 (a) Explain steps for Digital Certificate Creation. [10]

(b) What is the role of certificate revocation list in X.509 authentication server? Explain in detail. [10]

Q.4 (a) How RSA can be used for performing digital signature? Explain Knapsack Algorithms. [10]

(b) Explain various mechanism for protecting Private keys. [10]

Q.5 (a) Describe the Diffie-Hellman key exchange algorithm in detail. [10]

(b) Explain, how PGP provide confidentiality and authentication service for E-mail applications. [10]

Q.6 (a) How does certificate based authentication works? Explain with the help of diagram. [10]

(b) Discuss Java cryptography architecture in detail. [10]

Q.7 (a) What is firewall? Explain working of packet filters. [10]

(b) Explain the concept of dual signature in context of Secure Electronics Transaction (SET). Briefly describe the sequence of events that are required for a SET transaction. [10]

Q.8 Write short notes on (ANY TWO) [2×10=20]

(a) International Data Encryption Algorithm (IDEA)

(b) Hashes and Message Digest

(c) Virtual Private Network (VPN)

(d) Secure Hyper Text Transfer Protocol (SHTTP)
