Exam.Code:1006
Sub. Code: 35101

2055

M.E. (Information Technology)
Second Semester
MEIT-2201: Information Security

Time allowed: 3 Hours Max. Marks: 50

NOTE: *Attempt five questions in all, including Question No. I which is compulsory and selecting two questions from each Unit.*

x-x-x

1. Distinguish between the following:-

a) Authentication Vs Access Control

b) Substitution vs Transposition Ciphers

c) Certificate Authority (CA) Vs Key Distribution Centre (KDC)

d) Threat Vs Attack

e) Hash Vs MAC (5x2)

UNIT - I

2. a) Enlist advantages and disadvantages of Symmetric and Asymmetric Cryptography. How best of both the worlds help in achieving confidentiality over the Internet in efficient manner. Explain with suitable diagrams. 2+4

b) Design mutual authentication protocol that can thwart replay and Man-in Middle attacks. You can also use asymmetric cryptography for the purpose. 4

3. a) What are Public Key Certificates? What are their typical contents? 5

b) What is Man-in-the-Middle attack? How Public Key Certificates help in defending against Man-in-the-Middle attack? 5

4. What are limitations of DES? Explain working of AES in detail and demonstrate how AES removes the limitations of DES. 2+8

P.T.O.

Sub. Code: 35101

UNIT - II

5. a) Design a secure communication system between sender and receiver having confidentiality, mutual authentication and message integrity. 3+5

b) What do you mean by primitive root? Explain with an example. 2

6. a) What are limitations of SSL Protocols? 2

b) What are the contents of the purchase request raised by the Customer in SET protocol? Explain the process of verifying the purchase request by merchant and Issuer. 4+2+2

7. What is single sign on? Explain architecture of Kerberos in detail. 2+8

x-x-x