Exam.Code:1006
Sub. Code: 7362

2023
M. E. (Information Technology)
Second Semester
MEIT-2101: 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

I. Distinguish between the following:-

a) Plaintext Vs Ciphertext

b) Vulnerability Vs Patch

c) Block Vs Stream Cipher

d) Non-repudiation Vs Access Control

e) Security Parameter Negotiation Vs TCP Connection Establishment (5x2)

UNIT - I

II. a) Distinguish between symmetric and asymmetric cryptography. Why best of both the worlds are required to achieve confidentiality? (4,2)

b) How symmetric key can be exchanged to achieve secure communication? Describe at least two methods for the same. (4)

III. What is ELGamal Crypto scheme? How this scheme works to achieve confidentiality in the system? Give mathematical proof of this scheme. (2+6+2)

IV. Why digital signatures are important ingredient of secure communication? How digital signatures of CA helps to avoid Man/Woman in the middle attacks. Explain with lucid diagrams. (2+4+4)

UNIT - II

V. What is the need of SSL protocol? How key material is created in SSL protocol? Finally which keys and IVs are used in secure communication at both ends. (2+6+2)

P.T.O.

VI. What do you mean by Single Sign in? Write the complete protocol used in Kerberos system. Explain the process with suitable diagram(s). (2+8)

VII. Why separate payment protocol is required for Credit-Card based transactions? Explain SET protocol with suitable illustrations. (2+8)

x-x-x