Exam.Code:1005
Sub. Code: 7696

1129

M. E. (Information Technology)

First Semester

MEIT-105/115: 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. Use of non-programmable calculator is allowed.*

x-x-x

I. Attempt the following:-

a) Define a symmetric key cipher.

b) Briefly explain the idea behind the Knapsack cryptosystem.

c) Explain why modern block ciphers are designed as substitution ciphers instead of transportation ciphers.

d) Differentiate between Cache poisoning and sequence number prediction attacks.

e) Define Kerberos and name its servers. Briefly explain the duties of each server.

(5x2)

UNIT – I

II. Explain the Feistal Cipher structure. Also explain the various parameter and design choices which determine the actual algorithm of Feistal Cipher. (10)

III. Explain the RSA algorithm in detail. Perform encryption and decryption using RSA algorithm for p = 3, q = 11, e = 7 and M = 5. (10)

IV. Differentiate between conventional encryption and public key encryption. List and briefly define types of cryptanalytic attack based on what is known to attacker. (10)

UNIT – II

V. Explain the Needham -Schroeder protocol in detail. Why is there a need for four nonces in it? (10)

VI. Explain with the neat diagram encapsulating security payload format in detail. (10)

VII. What is Digital Signatures? Also explain the digital signature algorithm in detail. (10)

x-x-x