Exam.Code:0924
Sub. Code: 6852

1058

B.E. (Information Technology) Sixth Semester
ITE-643: Network Security and Cryptography

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. Define the following:-

a) Information Security

b) Fabrication

c) IP Spoofing

d) Digital Signature

e) Avalanche Effect

f) M an-in-the Middle Attack

g) Block Cipher

h) Cryptanalysis

i) Trojan Horse

j) Access Matrix

UNIT – I

II. Differentiate between threat and attack. Discuss Active and Passive attacks in detail along with the measures to control these attacks. (10)

III. a) With a neat and clean diagram, elaborate the functioning of round function in DES.

b) How CFB and OFB modes of block cipher operations work like Stream cipher? Explain. (5,5)

IV. a) Why Public Key Certificate? is the best technique to exchange public key among parties?

b) Alice and Bob want to establish a secret key using Diffie-Helman Key exchange protocol using two prime numbers q=11, α =5, A's private key, X_A=5 and B's private key X_B=7. And Eve is an Intruder with private key X_e = 4. Compute the Secret Key between .Alice -Eve and Bob -Eve. (5,5)

P.T.O.

UNIT – II

V. a) Differentiate MAC and HASH. Discuss MD5 compression function in details.

b) Encrypt the following data using RSA

p=7, q=11, e=13, M=5

(6,4)

VI. Discuss IPSec ESP header for transport and tunnel mode. (10)

VII. Write a short note on the following:-

a) Dual Signatures

b) Packet filtering firewall

(5,5)

x-x-x