Exam.Code:0934
Sub. Code: 6222

1048

B.E. (Information Technology)
Sixth Semester
IT-634: Network Security and Cryptography (OLD)

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) Avalanche Effect

b) Determine $35^{16} \bmod 16$

c) Man-in-the Middle Attack

d) How source and destination non-repudiation is achieved using public key cryptosystem?

e) Difference between Hash Function and Message Authentication Code (MAC). (5x2)

UNIT – I

II. a) How Confusion and Diffusion are implemented in DES?

b) Discuss the different block ciphers modes of operation that can be used as stream ciphers. (4,6)

III. a) Determine gcd (24140, 16762) using Euclidian algorithm

b) Explain substitution and permutation operations of AES. (3,7)

IV. a) Users A and B use the Diffie Hellan Key exchange technique with a common prime q=71 and a primitive root α=7.

i) If user A has private key $X_A = 5$. What is A's public key Y_A?

ii) If user B has private key $X_B=12$. What is B's public key Y_B?

iii) What is the shared secret key?

b) What is the role of Digital Certificates in network security? (5,5)

UNIT – II

V. a) Explain the working of RSA algorithm with the following parameters: p=7, q=ll, e=13, M=7

b) How to overcome the disadvantage of Arbitrated Digital Signature? (5,5)

P.T.O.

VI. Discuss in detail IPSec transport mode and tunnel mode. (10)

VII. a) Explain the operations of SSL Record Protocol.

b) How Merchant and Acquirer verify Dual Signatures in e-transaction? (5,5)

x-x-x