Exam.Code:0920
Sub. Code: 6819

1019

B.E. (Computer Science and Engineering)
Eighth Semester
CS-803D: Cryptography and Network 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. Attempt the following:-

a) How active attacks are different from the passive attacks?

b) What is the purpose of the P-box?

c) What is the meaning of term Diffusion?

d) What is bucket brigade attack?

e) Why RSA is difficult to break?

f) List the basic services provided by PGP

g) What is Kerberos used for?

h) What is man-in-middle attack?

i) How many header fields are used in MIME?

j) List any two IDS techniques. (10x1)

UNIT – I

II. a) What is the security policy of a network? Describe the various issues it needs to address.

b) What is Stream Cipher? Differentiate it from XOR Cipher, Poly alphabetic Cipher, Rotation Cipher. (5,5)

III. a) In the man-in-the-middle attack on the Diffie-Hellman key exchange protocol the adversary generates two public-private key pairs for the attack. Could the same attack be accomplished with one pair? Explain.

b) Explain the different modes of operations employed by Block Cipher. (5,5)

IV. a) Explain the encryption and decryption process in RSA using p=5; q=17; e=3; M=9.

b) What are the different ways to generate the random numbers? (5,5)

P.T.O.

UNIT – II

V. a) Describe MD5 algorithm in detail. Compare its performance with SHA-1.

b) Explain the classification of authentication function in detail. (5,5)

VI. a) Explain the S/MIME specifications in detail.

b) Explain in detail the PGP message generation, transmission and reception process. (5,5)

VII. a) Explain the different mechanism used to provide the security at Transport Layer?

b) What are virtual private networks? How risk associated with them can be avoided? (5,5)

x-x-x