Exam.Code:0920
Sub. Code: 33400

2055

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 Section.***

x-x-x

Q 1(a) Illustrate the difference between active and passive attacks?

(b) Compare the purpose of S and P-box in DES.

(c) How bucket brigade attack is executed?

(d) What is Kerberos used for?

(e) What do you mean by Transportation layer security?

(5x2)

Section - A

Q2 (a) What are the main elements of a security policy? Describe the various possible threats to mitigate in security policy. (5)

(b) Highlight the main ingredients of a symmetric cipher? Differentiate between a block cipher and stream cipher. (5)

Q3 (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 (5)

(b) What is block cipher? What are different operations? (5)

Q 4 (a) Explain the encryption and decryption process in RSA using p=3; q=11; e=7; M=5. (5)

(b) How random numbers are generated? Describe the steps to generate random number based on given probability distribution. (5)

Section -B

Q5 (a) What are the main risks using the MD5 algorithm? Compare the performance of MD5 for different cases with SHA-1. (6)

(b) Describe the secure hash algorithm in detail. (4)

Q6 (a) Explain in detail the PGP message generation, transmission and reception process. (5)

(b) What are the main steps involved in the SSL record protocol transmissions? Differentiate between SSL connection and SSL session. (5)

Q7 (a) What are virtual private networks? How risk associated with them can be avoided? (5)

(b) Explain the use of Firewall? Discuss its architecture and usage in detail (5)

x-x-x