Exam.Code:0920 2
Sub. Code: 6819

1059

B.E. (Computer Science and Engineering)
Eighth Semester
Elective – V
CS-803D: Cryptography and Network Security

Time allowed: 3 Hours Max. Marks: 50

***NOTE:** Attempt five questions in all, including Question No. I (Section-A) which is compulsory and selecting two questions each from Section B-C.*

x-x-x

Section -A

(10)

Q 1(a) What are active attacks?

(b) What are mono-alphabetic ciphers?

(c) What is Vigenere?

(d) What are shift registers?

(e) How bucket brigade attack is executed?

(f) List the different ways to key exchange.

(g) Why true random number generation is difficult?

(h) List the different digital signature standards.

(i) List the different types of Firewall.

(j) What is the use of VPN?

Section -B

Q2 (a) How the different challenges in information security can be addressed in security policy? Describe the various possible threats to mitigate in security policy. (6)

(b) Describe the various types of ciphers used? (4)

Q3 (a) Describe the Diffie-Hellman Key exchange algorithm by considering common prime q=29 and primitive root α=4. A's private key Xa=7 and B's private key Xb=11. Determine public key of A and B and shared secret Key. (5)

(b) What is block cipher? What are different ways to use it? (5)

Q 4 (a) Explain the encryption and decryption process in RSA using p=3; q=11; e=2; 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) How the size of message digest generated by secure hash algorithm-1 is calculated? (4)

Q6 (a) What are the main steps involved in the PGP message generation, transmission and reception process? (5)

(b) What is Kerberos? Explain the full process using an example. (5)

Q7 (a) How session level and transport layer level security is provided? What are main issues involved? (5)

(b) What are intrusion detection system? Can we manage the intrusions using firewalls? Which levels of intrusions cannot be managed at firewall level? (5)

x-x-x