Exam.Code:1000
Sub. Code: 7632

2072

M.E. (Computer Science and Engineering)

Second Semester

Elective – IV

CS-8207: Network Security

Time allowed: 3 Hours

Max. Marks: 50

NOTE: *Attempt five questions in all, including Question No. 1 (Section-A) which is compulsory and selecting two questions each from Section B-C.*

x-x-x

SECTION-A

1 a) Is it possible to provide Source Non-repudiation in Symmetric Cryptography? If yes, then how?

b) Are there any possible attacks on DES?

c) What are the characteristics of a good hash function?

d) Explain the role of Certification Authorities (CAs)?

e) How filtering is performed on the inbound traffic, based on destination port numbers? 10

SECTION -B

2 a) Why is AES more secure than DES? In AES, what is the importance of Forward and Inverse 'Mix Columns' Transformations? 6

b) Consider a Diffie-Hellman scheme with a common prime q=11, and primitive root α=2.

i) Verify that 2 is primitive root of 11.

ii) If User A has a public key Y_A=9, what is A's private key X_A? 4

iii) If User B has a public key Y_B=3, what is B's private key X_B?

iv) What is shared key of A and B?

3. a) *"The strength of a hash function equals the level of effort required to break the strong collision resistance in that function"*. Explain this statement with a suitable example. 3

b) What is the sequence of Use of Message Words in Various Rounds in MD5? 3

c) List the advantages and limitations of Cipher-Feedback (CFB) Mode. 4

4. What is the strength of RSA? How is it used data confidentiality as well as for digitally signing the messages? Perform encryption and decryption for p=11, q=23, e=13 and m= 2. 10

SECTION-C

5. a) What is significance of Public Key Infrastructure (PKI)? Why do we need it for Public Key Cryptography? 5

b) With the help of a suitable diagram, explain the signing and verifying functions of DSA. 5

6. a) What is Security Association in IPSec? How are Replay Packets rejected in IPSec? 5

b) What is the difference between SSL Session and SSL Connection? 5

7. a) What are the characteristics of a Bastion Host? How is security of Bastion Host maintained? 5

b) Explain different approaches for the Rule-Based Intrusion Detection? 5

x-x-x