19/5/17 (20)

Sem-III M.C.A. (CBSGS)

Network Security

QP CODE : 5150O2

3 Hours

[Max Marks: 80]

N. B : (1) Question number 1 is compulsory

(2) Attempt any 4 from question Nos. 2 to 7.

(3) Illustrate answers with sketches wherever necessary.

Q1a) What is network security? Why is it needed? Explain various security services. (10)

b) What is Key Distribution Centre? How does the key distribution work with multiple KDC domains? . (10)

Q2 a) What do you mean by Hash function? Explain message digest algorithm of MD5. (08)

b) What is cryptography? In an RSA system, the public key of a user is e=7, n=527. What is the private key of the user? (07)

Q3 a) Explain mutual authentication and refection attack with the help of a diagram.

(08)

b) Explain how security of a message is achieved using the SSL (07)

Q4a) What do you mean by IDEA algorithm and also explain the detailed working principle of IDEA. (08)

b) Explain DES algorithm with Initial Permutation. (07)

Q5 a) Define Firewall. What are the types of Firewalls? Explain in brief. (08)

b) Explain how SET ensures a secure e – commerce transaction. (07)

Q6 a) What is Kerberos? Explain the working procedure of Kerberos? Define Kerberos V5 (08)

b) What is a digital certificate? Explain the stepwise process of certificate generation? (07)

Q7. Write short notes on: (any three) (15)

a) IPSec

b) Email security

c) ECB

d)Intrusion detection