MCA sem III (CCBGS) Network Security 29/11/2016

QP CODE : 515000

(3 Hours) [total 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.

1. A] What is Key Distribution Center? How does the key distribution work with multiple KDC domains? 10
   B] What do you mean by Hash function? How will you define SHA1 and Explain message digest algorithm of MD5. 10

2. A] Define Network Security. What are the services and mechanisms provided by Network Security? 08
   B] What is man in the middle attack? Alice and Bob establish a secret key using Diffie – Hellman key exchange using g = 7, n = 13. Alice takes x as 3 & Bob takes y as 9. Tom an intruder selects x as 8 and y as 6. Show the working of the man-in-middle attack. 07

3. A] What do you mean by IDEA algorithm and also explain the detailed working principle of IDEA. 08
   B] What are the algorithm modes uses for secret key cryptography? 07

4. A] What is password based authentication? How the authentication mechanism works? Explain various problems associated with password based authentication. Suggest some solutions. 08
   B] Explain how SET ensures a secure e – commerce transaction. 07

5. A] Define Firewall. What are the types of Firewall? Explain in brief. 08
   B] Explain RSA algorithm with a suitable example. 07

6. 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

7. Write short notes on: (any three) 15
   a) IPSec
   b) Integrity check
   c) PEM in E-mail Security
   d) Honey Pots