MCA. Sem III (CBGS) 24/11/15

Network Security

QP Code : 25274

Time:3hours Marks:80

Note:

a) Question No. 1 is compulsory

b) Attempt any four from the remaining six questions

c) Assumptions should be made whenever required and should be clearly stated

d) Answers to sub questions should be answered together

e) Illustrate answers with diagrams wherever necessary

Q1 a) What are key principles of security? (20)

b) Explain digital signature.

c) Distinguish between symmetric and asymmetric cryptography.

d) Explain what is meant by E_mail security.

Q2 a) What do you understand by Cryptography. Explain its types. (8)

b) What is Hash? Discuss briefly SHA-1 . (7)

Q3 a) What is the importance of message digest? Explain MD2 (8)

(b) Give an overview of DES. Explain DES round. (7)

Q4 a) Differentiate between :- (8)

i) DES and IDEA

ii) ECB and CBC

b) In an RSA system the public key of a given user is c=31,n=3599.What is a private key of the user? Perform encryption and Decryption using RSA for following .P=3 q=11 e=7 m=5. (7)

Q5 a) How does Kerberos version 4 work? How is Kerberos V5 different from Kerberos V4. (8)

b)Discuss inter_realm authentication in Kerberos. (7)

Q6 a) Explain how SET ensures a secure e-commerce transaction. (8)

b)What is a Digital Certificate? Explain the stepwise process of certificate generation. (7)

Q7 Write short notes on any three of the following (15)

i. Honey pots ii. SSL

iii KDC. iv. Intrusion Detection and its types

PA-Con. 6376-15. — X —