2005 ANDHRA UNIVERSITY M.C.A COMPUTER

MCA 3.1.2
NETWORK SECURITY

Time: 3 Hrs.
Max. Marks: 100

First Question is Compulsory

Answer any four from the remaining

Answer all parts of any Question at one place.

1. a) What is a digital signature?

b) What is denial service attack?

c) What is ECB mode?

d) What is the procedure for key generation using RSA?

e) What is the purpose and the use of a KDC?

f) What is non-repudiation?

g) What is session key?

2. a) Describe the Diffie - Hellman key excha nge algorithm and explain it with an example.

b) Alice and Bob want to establish a secret key using the Diffie – Hellman key exchange protocol using n = 11, g = 5, x = 2 and y = 3. Find the values A and B and the secret key.

3. Describe the data encryption algorithm.

4. a) What are the key requirements of message digests?
b) Describe the secure hash algorithm.

5. Discuss the message formats of Kerberos V4 in detail.

6. a) What is password based encryption? What are the problems associated with it?

b) What is AH? Explain.

7. Discuss SSL in detail?

8. Describe Pretty Good Privacy.