2005-ANDHRA UNIVERSITY

IV B.TECH II SEMESTER DEGREE EXAMINATION

CRYPTOGRAPHY AND NETWORK SECURITY

(INFORMATION TECHNOLOGY)

TIME-3HOUR
MARKS-70

SECTION A IS COMPULSORY.ATTEMPT ANY FOUR QUESTIONS FROM SECTION B.

SECTION A [5*2=10 MARKS]

1. a) What is Non-repudiation?

b) What is denial service attack?

c) Distinguish between stream and block ciphers

d) Find the value of 89 mod 17

e) What is electronic money?

SECTION B [4*15=60 MARKS]

2. a) Describe the Diffie - Hellman key exchange 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. a) Describe the steps in the creation of a digital certificate.

b) Discuss XML security concepts.

6. a)Describe the time stamping protocol. What is its significance?

b) Describe pretty good privacy.

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

b) Describe the KERBEROS protocol.

8. a) What are the characteristics of a good firewall implementation?

b) What is a VPN? Explain briefly about the VPN architecture.