PVP 17

Code: 17CSCS2T6A

I M.Tech - II Semester - Regular Examinations – AUGUST 2018

CRYPTOGRAPHY & NETWORK SECURITY
(COMPUTER SCIENCE & ENGINEERING)

Duration: 3 hours   Max. Marks: 60

Answer the following questions:

1. a) Explain Network security model with neat diagram.   8 M

   b) Define threat and attack. What is the difference between both? List some examples of attacks which have arisen in real world cases.   7 M

(OR)

2. a) Explain symmetric cipher model with neat block diagram.   8 M

   b) Explain the characteristics of block and stream ciphers.   7 M

3. Explain cipher block modes of operations in detail.   15 M

(OR)

4. Explain Data Encryption Standard (DES) in detail.   15 M

5. a) Explain RSA algorithm. 7 M

b) Demonstrate encryption and decryption for the RSA algorithm parameters: p=3, q=11, e=7, d=?, M=5. 8 M

(OR)

6. a) Briefly Explain Deffie-Hellman Key Exchange. 7 M

b) Users A and B use the Deffie-Hellman Key Exchange technique with a common prime q=71 and a primitive root α =7 . If user A has private key X_A=5, what is A's public key Y_A ? 8 M

7. a) What do you mean by Security Association? What are the parameters? Briefly explain the basic Combinations of security associations. 8 M

b) What is an audit record? What is the use of audit record in intrusion detection? 7 M

(OR)

8. Explain the following:

a) Firewall Configurations 5 M

b) Viruses 5 M

c) Trusted Systems. 5 M