PVP 12

Code: CS7T5B

IV B.Tech - I Semester – Regular / Supplementary Examinations
November 2016

INFORMATION SECURITY

(COMPUTER SCIENCE AND ENGINEERING)

Duration: 3 hours Max. Marks: 70

Answer any FIVE questions. All questions carry equal marks

1. a) Explain various security attacks and services with neat diagrams. 7 M

   b) Explain about Internet Standards and RFCs. 7 M

2. a) What are the strengths of DES? Explain briefly. 7 M

   b) Discuss the four stages of AES algorithm and explain the importance of each stage diagrammatically by taking one round of AES. 7 M

3. a) How Diffi-Hellman key exchange technique can be applied to share a secret key securely between two parties? 7 M

   b) Consider a Diffie-Hellman scheme with a common prime, q = 11, and a primitive root, $\alpha = 2$, then 7 M

      If A has a Public key, $Y_a = 9$, what is the A’s Private Key X_a?

      If B has a Public key, $Y_b = 3$, what is the shared secret key K?

4. a) Describe S/MIME certificate processing. 7 M

b) Discuss PGP message generation and reception. 7 M

5. Discuss the IPSec architecture to provide IP security. 14 M

6. a) Explain about Secure electronic Transaction (SET) properties. 7 M

b) List and Explain the SET parameters with neat diagram. 7 M

7. a) Give few examples for worms and explain the virus counter measures. 7 M

b) Explain about SNMPV3 with neat diagram. 7 M

8. a) List the characteristics of Firewall. 7 M

b) Explain the various types of firewalls. 7 M