cusatxpress.com | campus blog of cusat

B.Tech Degree VIII Semester (Supplementary) Examination September 2011

CS 801 SECURITY IN COMPUTING

(2006 Scheme)

Time : 3 Hours Maximum Marks : 100

PART A

(Answer *All* questions) (8 x 5 = 40)

I. (a) What is secure computing? Explain the goals of security.
(b) Briefly explain the Caesar cipher.
(c) Write a note on strength and weakness of DES algorithm.
(d) Explain the different modes of operation of block cipher.
(e) Explain Miller-Rabin Algorithm.
(f) Give any three applications of Public Key Cryptosystem.
(g) Explain the various goals of IDS.
(h) Briefly explain secure e-mail.

PART B

(4 x 15 = 60)

II. Explain substitution cipher system and transposition cipher system with suitable examples. (15)

OR

III. (a) Differentiate between stream cipher and block cipher. (8)
(b) Describe the properties of modular arithmetic. (7)

IV. What do you mean by symmetric key encryption? Explain with an example of any one symmetric key encryption. (15)

OR

V. (a) Compare DES with AES (8)
(b) Write a note on security of AES (7)

VI. Describe public key encryption. Explain with an example of RSA algorithm. (15)

OR

VII. (a) Write a note on Diffie – Hellman Crypto system. (8)
(b) How public key encryption can be used to create digital signature? (7)

VIII. (a) Write the applications and benefits of IP security. (7)
(b) What are viruses? Explain the different types of viruses (8)

OR

IX. What is a firewall? Explain the different types of firewalls and their characteristics in detail. (15)

***