

B. Tech Degree VIII Semester Examination, April 2010

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 are the major vulnerabilities in a Computer System?
b. Write a short note on Symmetric Cipher Model.
c. Write a note on Strength of DES algorithm.
d. What are the AES parameters and write its significance also?
e. Write the differences between Conventional Encryption and Public Key Encryption.
f. Give any three applications of Public Key Cryptosystems.
g. Write a note on Digital Signature.
h. Write the applications and Benefits of IP Security.

PART B

(4 x 15 = 60)

- II. Describe any three Substitution Techniques. (15)
OR
III. a. Write a note on Transposition Techniques. (7)
b. Describe the properties of Modular Arithmetic and Modulo Operator. (8)
- IV. Describe the DES Encryption and Decryption Algorithm in detail. (15)
OR
V. Describe the AES Encryption and Decryption Algorithm in detail. (15)
- VI. With the help of an example, explain the RSA algorithm. (15)
OR
VII. a. Describe the Miller-Rabin Algorithm. (7)
b. Write a note on Diffe-Hellman Crypto systems. (8)
- VIII. a. Explain various approaches for the Digital Signature Function. (7)
b. Describe various approaches to Intrusion Detection. (8)
OR
IX. Describe various types of Firewalls and their characteristics in detail. (15)

