Roll No. ..... Total Pages : 02

BT-7/D-18 37007

SECURITY AND CRYPTOGRAPHY

CSE-473

Time : Three Hours] [Maximum Marks : 75

Note : Attempt *Five* questions in all, selecting at least *one* question from each Unit.

Unit I

1. (a) What do you mean by differential and linear crypto analysis ? 7
   (b) Is IDEA algorithm asymmetric or symmetric ? Explain its working, key structure and decrpyion mechanism. 8

2. (a) Explain cipher block chaining. 8
   (b) Describe, how knapsack problem is applied to public key cryptography. 7

Unit II

3. (a) Explain briefly the working of Needham-Schroeder symmetric encryption algorithm. 10
   (b) What are public key and screte key signature ? Explain their working. 5

4. (a) How does AES encryption work ? Draw suitable diagrams for different steps. 8
   (b) Discuss methods and issues in key distribution and handling. 7

Unit III

5. (a) Describe the working of antivirus code. 6
   (b) Explain various password attacks. What considerations must be made to make passwords secur from attacks ? 9

6. (a) In what ways a database may be compromised ? Describe methods to make tables and records of a database secure. 8
   (b) Describe life-cycle of a virus and its various types. 7

Unit IV

7. (a) Discuss in detail different security attacks that may happen on a computer system. 8
   (b) How to secure network components ? 7

8. (a) Explain the techniques to secure enterprise networks. 9
   (b) What is a Firewall ? What is access control list ? Discuss with example. 6