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

BT-7/M-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. All questions carry equal marks.

Unit I

1. What are the different modes of operations in DES ? Explain about triple DES algorithm with example. What is meant by Avalanche effect in DES algorithm ? 15

2. (a) What is RSA Algorithm ? Discuss the attacks on RSA algorithm.
   (b) Distinguish between differential and linear cryptanalysis. 8+7=15

Unit II

3. (a) Explain digital signature standard. Differentiate between Secret key and public key signatures.
   (b) Briefly explain Diffle-Hellman key exchange algorithms. 8+7=15

4. (a) Elaborately explain Kerberos authentication mechanism with suitable diagram.
   (b) Describe MD5 algorithm in detail. Compare its performance with SHA-1 algorithm. 8+7=15

Unit III

5. What are the principles of database security ? How password technology and administration ensures database security ? 15

6. (a) Discuss the life-cycle of a virus. How can system be prevented from virus ?
   (b) What do you mean by Trojan horse and bombs ? Discuss any *two* advanced antivirus techniuqes in detail. 8+7=15

Unit IV

7. What do you understand by network security ? How can you secure Local area network ? Discuss its security plan and policy. 15

8. Write notes on the following :
   (a) Network setting priorities
   (b) Securing network components. 8+7=15