Roll No. .... Total Pages : 02

BT-7/D-19 37151

CRYPTOGRAPHY AND INFORMATION SECURITY

CSE-419N

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. (a) Define Security and differentiate attack and threat.
   (b) What are active and passive attacks ? Explain.

2. Transform the message HAPPYONAM using Verman Cipher. Differentiate between a Stream cipher and Block cipher.

Unit II

3. (a) Explain idea leading to RSA Cryptography. Take an example and explain.
   (b) Define Hashing. Discuss Tiger hash and Gear Hash with example.

4. (a) Explain Access Control Mechanism.

(b) Discuss two cascade approaches for DES algorithm. Also explain why does DES function need expansion permutation ?

Unit III

5. (a) Explain Diffie Hellman Key exchange algorithm.
   (b) Discuss Man-in-middle Attack and Paillier public key crypto system.

6. Explain key exchange protocols with emphasis on Kerberos and VPN.

Unit IV

7. Write intrusion detection system and methods to counter it.

8. (a) Explain MD-5 algorithm.
   (b) Discuss Secure Multiparty computation system.