

BT-7/M-21**47151****CRYPTOGRAPHY AND INFORMATION SECURITY****Paper–CSE-419N**

Time Allowed : 3 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) What are Security attacks ? Discuss concept of Attacks and Threats.
(b) Explain Classical Cryptography.
2. (a) Explain Shannon's theorem.
(b) What is the concept of Cipher ? Write the types of Cipher.

UNIT-II

3. (a) What is the concept of Discretionary and Mandatory Access Control ?
(b) Discuss 3-DES.
4. (a) Explain RSA modes of Operation.
(b) Define Tiger and Gear Hashing.

UNIT-III

5. Explain key exchange using Diffie-Hellman algorithm.
6. (a) Explain Key Exchange protocols.
(b) Explain Public Key Crypto system with reference to Kerberos, SSL and IPSEC.

UNIT-IV

7. (a) What is Digital Signature ? Discuss the concept of SHA1 and Rabin Finger Print.
(b) Explain Firewall and Intrusion Detection system.
8. Write notes on the following :
(a) MD-5 algorithm.
(b) Secure Military Computation.