BT/8/M-19   **38195**

INFORMATION SECURITY
IT-406N

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. Define Security. What is the model for network security ? Explain mechanisms.

2. Explain substitution and transposition techniques.

Unit II

3. Describe block cipher and stream cipher. Explain RC4.

4. Explain ECC algorithm with its key distribution.

Unit III

5. Write about the following :

   (a) Message Authentication Code

   (b) CMAC

   (c) Kerberos.

6. Describe public-key infrastructure and biometric authentication.

Unit IV

7. Explain transport layer security and secure electronic transaction.

8. Explain the following :

   (a) Password Management

   (b) Virus related threats

   (c) Intrussion detection.