BT-4/M-22   **44226**

CRYPTOGRAPHIC FUNDAMENTALS
Paper–PC-CS-CYS-212A

Time : Three Hours]   [Maximum Marks : 75

Note : Attempt *five* questions in all, selecting at least *one* question from each unit. Each question carry equal marks.

UNIT–I

1. Describe classical encryption techniques with suitable examples.   (15)

2. (a) Explain Shannon's theory of confusion and diffusion.
                                                    (8)

    (b) Write a short note on Data Encryption Standard. (7)

UNIT–II

3. (a) Explain the principles of public key crypto systems.
                                                    (7)

    (b) Describe Diffie-Hellman key Exchange algorithm. (8)

4. (a) Explain MD5 message digest algorithm.   (8)

    (b) Write a short note on Digital Signatures.   (7)

UNIT–III

5. Describe Computer based Symmetric and Asymmetric Key Cryptographic Algorithms. (15)

6. Explain the following terms :
   (a) Information Management Technologies.
   (b) Multi-level relational data models. (15)

UNIT–IV

7. Define Intrusion detection. Explain security concepts of intrusion detection system. (15)

8. Explain the following terms in context to Intrusion Detection:
   (a) Vulnerability Analysis.
   (b) technical Issues. (15)

———————