[ECS 706]
M.Tech. Degree Examination

Computer Science & Technology
II SEMESTER

CRYPTOGRAPHY & NETWORK SECURITY
(Effective from the admitted batch 2015–16)

Time: 3 Hours  Max.Marks: 60

Instructions:  Each Unit carries 12 marks.
Answer all units choosing one question from each unit.
All parts of the unit must be answered in one place only.
Figures in the right hand margin indicate marks allotted.

MODULE-I

1. a) Define Active Attack. Explain briefly about the four categories
   of Active attacks
   b) With a suitable example explain in detail about the Caesar cipher

   OR

2. a) List and briefly define categories of Security mechanisms
   b) Explain in detail about the Transposition techniques

MODULE-II

3. a) Discuss the Differential Cryptanalysis technique and its
   applicability to DES
   b) What is the purpose of S-boxes in the DES? Explain

   OR

4. With a neat block diagram illustrate the scheme of DES encryption
   algorithm

MODULE-III

5. a) Describe briefly about the two assertions of the Chinese
   Remainder Theorem
   b) Explain Elliptic Curve Cryptography in detail
6. a) Explain in detail about the Euler’s Theorem
   b) Discuss briefly about the principles of public key cryptosystems

**MODULE-IV**

7. Describe the applications of the Cryptographic Hash Functions with simplified examples

**OR**

8. a) What are the different attacks that can be identified in the context of communication across a network? Explain
   b) Explain the Security of MACs

**MODULE-V**

9. a) Explain Remote User-Authentication Principles
   b) Discuss in detail about the applications of IP Security

**OR**

10. a) What are the advantages of PGP? Explain
    b) Explain briefly about the need of Firewalls

[02/I2 S/216]