23541

M.Tech. 1st Semester

Examination, December–2018

CYBER FORENSICS AND INFORMATION SECURITY

Paper– MTCF–101

Mathematical Foundations of Information Security

Time allowed : 3 hours] *[Maximum marks : 100*

Note: *Attempt **five** questions in total, selecting **one** question from each Section and **Question No. 1 , which is Compulsory.** All questions carry equal marks.*

1. (a) Find g.c.d. of 1547 and 560 using Euclidean algorithm. 5×4=20

   (b) Write a note on Elliptic Curves.

   (c) Write a note on Secure Cryptosystem.

   (d) Write a note on Zero- Knowledge Protocol.

Section–A

2. List and Explain the basic properties of congruencies. Also define the Legendre symbol. Determine whether

5. Write a note on following: 20

(a) Vigenere Cipher

(b) Affine Cipher

Section–C

6. Describe and Explain Diffie- Hellman Key Exchange protocol by taking suitable example. Also write a note on security of RSA. 20

7. Explain Secure Socket Layer (SSL) protocol for communication security in detail. 20

Section–D

8. Explain Quadratic Sieve method for factoring large integers in detail by giving suitable example. 20

9. Explain Elliptic curve primality test in detail using suitable example. 20