Roll No. ………………….

23541

M. Tech 1st Sem. (Cyber Forensics and Information Security)

Examination – December, 2014

Mathematical Foundations of Information Security

Paper : MTCF-101

Time : Three Hours] *[Maximum Marks :100*

Before answering the questions, candidates should ensure that they have been supplied the correct and complete question paper. No complaint in this regard, will be entertained after examination.

Note : Question No. **1** is *compulsory* and attempts *four* more questions selecting *one* question from each Section. All questions carry equal marks.

1. Write the short notes on the followings :

(a) Quadratic residues

(b) Use of block ciphers

(c) Secure cryptosystem

(d) Elliptic curve factorization

(e) Applications of factoring

P. T. O.

SECTION - A

2. State and prove quadratic reciprocity law.

3. Find the least positive common solution of the following linear congruence

$$x \cong 1 (\mathrm{mod}\ 3),\ x \cong 2 (\mathrm{mod}\ 4),\ x \cong 3 (\mathrm{mod}\ 5)$$

SECTION - B

4. Discuss symmetric and asymmetric cryptosystem in detail.

5. Explain vigenere cipher, stream cipher and block cipher with their different applications.

SECTION - C

6. (a) Explain RSA cryptosystem and bit security of RSA.

(b) Discuss an oblivious transfer protocol and its application for the exchange of secrets.

7. Explain Zero - Knowledge protocol and the main attacks used to try to break ZK protocols.

SECTION - D

8. Explain elliptic curves and elliptic cryptosystem in detail with examples.

9. Write the short notes on the followings :

(a) Elliptic curve cryptosystems

(b) Elliptic curve primality

(c) continued fraction method

(d) Pseudo primes