20MA502T					Mathematical Foundation of Cyber Security					
Teaching Scheme										
L	T	P	C	Hrs. / Week	Theory			Practical		Total Marks
					MS	ES	IA	LW	LE/Viva	
3	1		0	4	25	50	25	--		--

COURSE OBJECTIVES

- To provide fundamental concept of abstract algebra.
- To study basic concepts of set theory and binary operations.
- To study different operations on algebraic structure.
- To study advanced number theory concepts

UNIT 1 GROUP THEORY **10 Hrs.**

Introduction to Set Theory, Binary Operations on Sets, Equivalence Relations, Introduction to Groups, Subgroups, Cyclic Groups, dihedral groups , Permutation Groups, , cosets, Lagrange's theorem, Normal Subgroups, Quotient Groups, Isomorphisms, Homomorphisms

UNIT 2 RINGS AND FIELDS **10 Hrs.**

Definition and basic concepts in rings, examples and basic properties, zero divisors, integral domains, fields, characteristic of a ring, quotient field of an integral domain, subrings, ideals, maximal ideal, prime ideal, quotient rings. Euclidean domains, Polynomials, prime, irreducible elements and their properties. Eisensteins irreducibility criterion and Gauss's lemma.

UNIT 3 ELEMENTARY NUMBER THEORY **12 Hrs.**

The division algorithm, Divisibility and the Euclidean algorithm, The fundamental theorem of arithmetic, Modular arithmetic and basic properties of congruences; Principles of mathematical induction and well ordering principle. Primality Testing algorithms, Chinese Remainder Theorem, Quadratic Congruence

UNIT 4 ADVANCED NUMBER THEORY **08 Hrs.**

Advanced Number Theory – Primality Testing algorithms, Chinese Remainder Theorem, Quadratic Congruence, Discrete Logarithm, Factorization Methods, Side Channel Attacks, Shannon Theory, Perfect Secrecy, Semantic Security.

40 Hrs

COURSE OUTCOMES

On completion of the course, student will be able to

CO1- Define the concepts related to the basics of set theory and binary operations.
CO2- Demonstrate knowledge and understanding of groups, subgroups, and order of an element in finite groups.
CO3- Develop understanding of algebraic structure ring, and field.
CO4- Discover different operations on algebraic structure.
CO5- Choose appropriate algebraic structure for cryptographic operation.
CO6- Develop understanding of use of algebraic structure in number theory algorithms.

TEXT/REFERENCE BOOKS

1. D.S. Dummit and R.M. Foote, "Abstract Algebra", John Wiley
2. Michael Artin, "Algebra", Pearson Education.
3. J.A. Gallian, "Contemporary Abstract Algebra", Narosa Publishing House.
4. I. N. Herstein, "Topics in Algebra", Wiley.
5. N. Jacobson, "Basic Algebra I", Hindustan Publishing Company.
6. William Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education.