COURSE CODE	COURSE TITLE	L	T	P	C
1152CS148	**MODERN NUMBER THEORY**	**3**	**0**	**0**	**3**

Course Category: Program Elective

A. Preamble :

This course introduces to the concepts of number theory, computation theory computational number theory; and emphasizes their significance in modern cryptography.

B. Prerequisite Courses:

Sl. No	Course Code	Course Name
1	1150MA202	Engineering Mathematics-I
2	1150CS201	Problem Solving using C

C. Related Courses:

Sl. No	Course Code	Course Name
1	1152CS155	Principles of Cyber Physical Systems
2	1152CS156	Modern Cryptography Theory
3	1152CS157	Ethical Hacking
4	1152CS158	Cyber Security
5	1156CS601	Minor Project
6	1156CS701	Major Project

D. Course Outcomes :

Upon successful completion of the course, students will be able to:

CO Nos.	Course Outcomes	Knowledge Level (Based on revised Bloom's Taxonomy)
CO1	Discuss how number theory is related to and used in modern cryptography.	K2
CO2	Manipulate the properties implied by the definitions of groups, fields and rings	K3
CO3	Apply the multiplicative inverse function to solve linear congruences	K3
CO4	Apply the concepts of primality testing to prove the Prime Number Theorem with an error term.	K3
CO5	Analyse and solve problems involving integer factorization	K3
CO6	Apply the properties of discrete logarithms to solve exponential and Index Calculus problems.	K3

E. Correlation of COs with POs :

Cos	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	M	M	L	L				L				L	L	M	M
CO2	H	M	L	L	L				L	L	L	M	M		
CO3	M	M	L	L	L								M	L	M
CO4	H	H	M	L	L							M			
CO5	M	M	M	L	L							L	M		
CO6	H	M	L	L	L			L	L	L	L	M	L	L	L

H- High; M-Medium; L-Low

F. Course Content :

UNIT I INTRODUCTION TO CRYPTOGRAPHY L – 9

Introduction - Number Theory, Computation Theory, Computational Number Theory and Modern Cryptography.

Secret-Key Cryptography - Cryptography and Cryptanalysis, Classic Secret-Key and Modern Secret-Key Cryptography.

UNIT II FUNDAMENTALS OF NUMBER THEORY L – 9

Fundamental(L/M) - Basic Algebraic Structures, Divisibility Theory and Arithmetic Functions.

UNIT III CONGRUENCE THEORM L – 9

Fundamental(M/M) - Congruence Theory , Primitive Roots and Elliptic Curves

UNIT IV PRIMALITY TESTING AND INTEGER FACTORIZATION L – 9

Primality Testing – Basic Tests, Miller-Rabin Test, Elliptic Curve Test and AKS Test

Integer Factorization(L/M) - Basic Concepts, Trial Division Factoring, ρ *and* $\rho - 1$ Methods and Elliptic Curve Method

UNIT V DISCRETE LOGARITHMS L – 9

Integer Factorization(M/M) - Continued Fraction Method, Quadratic Sieve and Number Field Sieve

Discrete Logarithms – Basic Concepts, Baby-Step Giant-Step Method, Pohlig-Hellman Method, Index Calculus and Elliptic Curve Discrete Logarithms

Total: 45 Periods

G. Learning Resources

i. Text Books:

1. Song Y. Yan, “Computational Number Theory and Modern Cryptography”, John Wiley (ISBN 978-L-LL8-L8858-H), M0LH.

ii. Reference:

1. David M. Burton, “Elementary Number Theory”, Seventh Indian Edition (Indian , McGraw Hill Education), M0LM.
2. K.Rosan, “Elementary Number Theory and its Application”, Fifth Edition, Addison-Wesley,M005.
3. Marlow Anderson, Todd Feil, "A First Course in Abstract Algebra Rings, Groups, and Fields”, Third edition, CRC Press, M0L5.

iii. Online resources

1. http://people.reed.edu/~jerry/H6L/lectures/mats.html
2. http://citeseerx.ist.psu.edu/viewdoc/download?doi=L0.L.L.705.8H87&rep=repL&type=pdf
3. http://nptel.ac.in/courses/LLLL0H0M0/
4. https://ocw.mit.edu/courses/mathematics/L8-785-number-theory-i-fall-M0L6/syllabus/
5. http://archives.math.utk.edu/topics/numberTheory.html