

COMPUTATIONAL NUMBER THEORY

Course code: 15CS2202

L	P	C
3	0	3

Pre requisites: Number theory basics, Security issues.

Course Outcomes:

A student who successfully completes this course should, at a minimum, be able to

- CO1:** Develop the mathematical skills to solve number theory problems and to develop the mathematical skills of divisions, congruence's, and number functions.
- CO2:** Learn the history of number theory and its solved and unsolved problems.
- CO3:** Investigate applications of number theory and the use of computers in a Number theory.
- CO4:** Estimate the time and space complexities of various Secure Algorithms.
- CO5:** Learn various factorization and logarithmic methods.

UNIT-I: (10-Lectures)

TOPICS IN ELEMENTARY NUMBER THEORY: O and Ω notations – time estimates for doing arithmetic – divisibility and the Euclidean algorithm – Congruence's: Definitions and properties – linear congruence's , residue classes, Euler's phi function

UNIT II: (10-Lectures)

FERMAT'S LITTLE THEOREM – Chinese Remainder Theorem – Applications to factoring – finite fields – quadratic residues and reciprocity: Quadratic residues – Legendre symbol – Jacobi symbol. Enciphering Matrices – Encryption Schemes – Symmetric and Asymmetric Cryptosystems – Cryptanalysis – Block ciphers –Use of Block Ciphers.

UNIT-III: (10-Lectures)

MULTIPLE ENCRYPTION – Stream Ciphers –Affine cipher – Vigenere, Hill, and Permutation Cipher – Secure Cryptosystem. Public Key Cryptosystems: The idea of public key cryptography – The Diffie–Hellman Key Agreement Protocol - RSA Cryptosystem – Bit security of RSA – ElGamal Encryption

UNIT-IV: (10-Lectures)

DISCRETE LOGARITHM – Knapsack problem – Zero-Knowledge Protocols – From Cryptography to Communication Security - Oblivious Transfer. Primality and Factoring: Pseudo primes – the rho (γ) method – Format factorization and factor bases.

UNIT-V: (10-Lectures)

THE CONTINUED FRACTION METHOD – the quadratic sieve method. Number Theory and Algebraic Geometry: Elliptic curves – basic facts – elliptic curve cryptosystems – elliptic curve primality test – elliptic curve factorization.

TEXT BOOKS:

1. Neal Koblitz: “A Course in Number Theory and Cryptography”, 2nd Edition, Springer, 2002.
2. Johannes A. Buchman: “Introduction to Cryptography”, 2nd Edition, Springer, 2004.

REFERENCES:

1. Serge Vaudenay, “Classical Introduction to Cryptography Applications for Communication Security”, Springer, 2006.
2. Victor Shoup: “A Computational Introduction to Number Theory and Algebra”, Cambridge University Press, 2005.
3. A. Manazes, P. Van Oorschot and S. Vanstone: “Hand Book of Applied Cryptography”, CRC Press, 1996.