SUBJECT NO-CS60094, SUBJECT NAME- Computational Number Theory

LTP- 3-0-0,CRD- 3

SYLLABUS :-

Algorithms for integer arithmetic: Divisibility, gcd, modular arithmetic, modular exponentiation, Montgomery arithmetic, congruence, Chinese remainder theorem, Hensel lifting, orders and primitive roots, quadratic residues, integer and modular square roots, prime number theorem, continued fractions and rational approximations. Representation of finite fields: Prime and extension fields, representation of extension fields, polynomial basis, primitive elements, normal basis, optimal normal basis, irreducible polynomials. Algorithms for polynomials: Root-finding and factorization, Lenstra-Lenstra-Lovasz algorithm, polynomials over finite fields. Elliptic curves: The elliptic curve group, elliptic curves over finite fields, Schoof s point counting algorithm. Primality testing algorithms: Fermat test, Miller-Rabin test, Solovay-Strassen test, AKS test. Integer factoring algorithms: Trial division, Pollard rho method, p-1 method, CFRAC method, quadratic sieve method, elliptic curve method. Computing discrete logarithms over finite fields: Baby-step-giant-step method, Pollard rho method, Pohlig-Hellman method, index calculus methods, linear sieve method, Coppersmith s algorithm. Applications: Algebraic coding theory, cryptography. References 1.Victor Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press. 2.Maurice Mignotte, Mathematics for Computer Algebra, Springer-Verlag. 3.Ivan Niven, Herbert S. Zuckerman and H. L. Montgomery, An Introduction to the Theory of Numbers, John Wiley. 4.Joachim von zur Gathen and Juergen Gerhard, Modern Computer Algebra, Cambridge University Press. 5.Rudolf Lidl and Harald Niederreiter, Introduction to Finite Fields and their Applications, Cambridge University Press. 6.Alfred J. Menezes, editor, Applications of Finite Fields, Kluwer Academic Publishers. 7.Joseph H. Silverman and John Tate, Rational Points on Elliptic Curves, Springer International Edition. 8.D. R. Hankerson, A. J. Menezes and S. A. Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag. 9.A. Das and C. E. Veni Madhavan, Public-key Cryptography: Theory and practice, Pearson Education Asia. 10.Henri Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag.