**Abstract**

|  |  |
| --- | --- |
|  | This thesis is a detailed study of primality testing and factorization algorithms. In the first part, we study about famous algorithms such as Fermat’s factorization scheme, Robin-Miller Test, Solovay-Strassen Test, Continued Fraction Factoring Algo rithm, Pollard-rho and p − 1 test etc., then we study deterministic polynomial time AKS Algorithm. In, second part we study about Quadratic sieve algorithm and polynomial time lattice reduction algorithm, The LLL-Algorithm. Then we study in detail about poly nomial factorization in finite field Z/pZ and in field of rationals, Q. In the last part, we study polynomial factorization using the LLL-Algorithm. |