ABSTRACT

Cryptology is the study of secret codes. While speaking of cryptology, we discuss two main branches. One is Cryptography, concerned with the writing of messages in secret code while the other is Cryptanalysis is concerned with reading encrypted messages by breaking secret codes. The most basic of the modules in modern Cryptography is that of a primitive, which may be regarded as a Cryptographic building block which performs one or more desired functions, and may be combined with others to form a Cryptographic protocol. In general, primitives are designed to satisfy particular security objectives, which may be built from the four basic objectives-Confidentiality, data integrity, authentication and non-repudiation.

In view of hiding the information from unauthorized sources i.e., the confidentiality, protecting from the intruders i.e., integrity and making unavailable to unauthorized sources is very much essential in the network security. The existing symmetric key Crypto systems meeting the requirements to the satisfactory level i.e., ATM transactions, online banking transactions providing enough security unless until the negligence of the user. The recent developments proved that the double encryption schemes strengthen the Data Encryption Standards.

In the present thesis several Cryptographic schemes were developed basing on 1. Fibonacci matrices obtained from Fibonacci relation, likewise Bernoulli numbers, Lucas numbers, Pell numbers.2. Affine and Vigenere ciphers. In addition to double encryptions the thesis
concluded by introducing triple encryption schemes using two independent keys using Fibonacci numbers, Fibonacci matrices, Affine and Vigenere ciphers and Fibonacci-Lucas matrices.