International Journal of Mathematical Archive-4(5), 2013, 219-222
Available online through www.ijma.info ISSN 2229 – 5046

FINITE STATE MACHINES AND RECURRENCE MATRICES OF CRYPTOLOGY

T. surendra[1*], P. A. Jyotirmie[2], A. Chandra Sekhar[3] and S. Uma Devi[4]

[1]Department of Mathematics, GIT, GITAM University, Visakhapatnam, India

[2]Department of Engineering Mathematics, Andhra University, Visakhapatnam, India

[3]Department of Mathematics, GIT, GITAM University, Visakhapatnam, India

[4]Department of Engineering Mathematics, Andhra University, Visakhapatnam, India

(Received on: 23-03-13; Revised & Accepted on: 17-04-13)

ABSTRACT

Cryptology is the process of Cryptography (Encryption) and Cryptanalysis (Decryption). The application of Mathematical models playing a vital role in the security goals and consequently the security attacks for secure communication. The cracking of the code is also a major challenge in recent times. In this process the role of mathematics is, defining a function for encryption in such a way that tracing the inverse of the function must be a difficult process. The fundamental mathematical model in cryptology is the concept of Matrices and in particular nonsingular matrices. In this paper we proposed an innovative technique for cryptology using Finite State Machines (FSM) and matrices obtained from recurrence relations.

Key words: *Finite state machine – Recurrence matrix – Fibonacci sequence.*

1. INTRODUCTION

The finite automaton is a mathematical model of a system with discrete inputs and outputs. The system can be one of a finite number of internal configurations or states. The finite automaton is a mathematical model or a system, with discrete inputs and outputs. When the finite automata is modified to allow zero, one, or more transitions from a state on the same input symbol then it is called a nondeterministic finite automata. For deterministic automata the outcome is a state, i.e., an element of Q, for nondeterministic automata the outcome is a subset of Q, where Q is a finite nonempty set of states. Automata theory is the study of abstract computing devices or machines. It is a behavior model composed of a finite number of states, transition between those states and actions in which one can inspect the way logic runs when certain conditions are met. Recently finite state machines are used in cryptography, not only to encrypt the message, but also to maintain secrecy of the message.

A finite state machine or finite-state automaton is a mathematical model of computation used to design both computer programs and sequential logic circuits [2], [9]. It is conceived as an abstract machine that can be in one of the finite states. The machine is only in one state at a time, the state it is in at any given time is called the current state. It can change from one state to another when initiated by triggering event or condition, this called a transition.

Automata theory is a key to software for verifying systems of all types that have a finite number of distinct states, such as communication protocols or protocol for secure exchange of information. In Mealy Machine every finite state machine has a fixed output [1], [2], [4]. Mathematically a Moore machine is a six-tuple M= $(Q, \sum, \Delta, \delta, \lambda', q_0)$ where Q is nonempty finite set of states, $\sum$ is a nonempty finite set of input symbols, Δ is a nonempty finite set of output symbols, δ is a transition function from Q x $\sum \rightarrow Q$ and finally λ is a output function defined as $\lambda(q_i)$ = i for i = 0,1,2……. Let us consider the Moore machine for residue modulo 5 [9], [4].

Corresponding author: *T. surendra[1*]*
[1]Department of Mathematics, GIT, GITAM University, Visakhapatnam, India

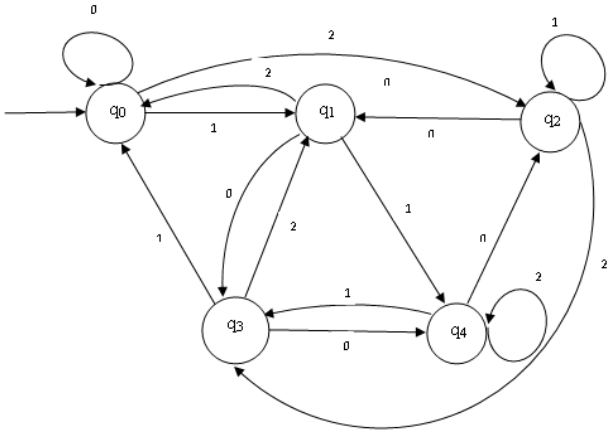

Fig 1 Moore machine which calculates residue mod 5

Let us choose the number 18, the ternary conversion is 200. Clearly when 18 divided by 5 the remainder is 3. We have $\delta(q_0, 2) = q_2$, $\delta(q_2, 0) = q_1$, $\delta(q_1, 0) = q_3$. Therefore $\lambda(q_3) = 3$.

Recurrence Matrix
In the recurrence matrix the elements are from recurrence relation.

For example $Q_n = \begin{bmatrix} 1 & 0 & 0 \\ 0 & f_{n+1} & f_n \\ 0 & f_n & f_{n+1} \end{bmatrix}$; $n \geq 0$.

2. ALGORITHM

Encryption:
1) Arrange the plain text in the form of a square matrix 'T'.

2) A Moore machine for residue modulo is chosen and sent through public channel.

3) Choose a recurrence matrix from a Fibinacci or Lucas sequence and consequently the corresponding matrix is extracted, say Q_n.

4) Perform $T*Q_n$.

5) Choose the sum of the elements of any row or column, and convert the number to Ternary base.

6) The cipher text at j_{k+1}^{th} state is j_k^{th} state+ Q_n if the input is 0, otherwise it is j_k^{th} $*Q_n$. At each stage, the value of 'n' is the output multiplied by 3.

Decryption: As the matrix obtained from recurrence matrix is nonsingular, the inverse Q_n is I_n. The matrix in the j_{k+1}^{th} state is multiplied by I_n to get j_k^{th} state cipher text. Repeat the process to get the required plain text.

Implementation:
Allocate 0 to letter a, 1 to letter b, 2 to letter c and so on and 25 to letter z. Let the plain text be 'COMMITTEE'. The corresponding matrix of the plain text T is

$$T = \begin{bmatrix} C & O & M \\ M & I & T \\ T & E & E \end{bmatrix} = \begin{bmatrix} 2 & 14 & 12 \\ 12 & 8 & 19 \\ 19 & 4 & 4 \end{bmatrix}$$

Let the recurrence matrix be

$$Q_n = \begin{bmatrix} 1 & 0 & 0 \\ 0 & f_{n+1} & f_n \\ 0 & f_n & f_{n+1} \end{bmatrix}$$

where 'f_n' is Fibonacci sequence. Secret key = Sum of the elements of the last column =35 = $(1022)_3$.

The cipher text at each stage is

S. No.	Input	Previous state	Present state	Output	Key values	Cipher text
1	1	q^0	q^1	1	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 2 & 3 \end{bmatrix}$	$\begin{bmatrix} 2 & 66 & 64 \\ 12 & 62 & 73 \\ 19 & 20 & 20 \end{bmatrix}$
2	0	q^1	q^3	3	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 55 & 34 \\ 0 & 34 & 55 \end{bmatrix}$	$\begin{bmatrix} 2 & 5806 & 5764 \\ 12 & 5892 & 6123 \\ 19 & 1780 & 1780 \end{bmatrix}$
3	2	q^3	q^1	1	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 2 \\ 0 & 2 & 3 \end{bmatrix}$	$\begin{bmatrix} 2 & 28946 & 28904 \\ 12 & 29922 & 30153 \\ 19 & 8900 & 8900 \end{bmatrix}$
4	2	q^1	q^0	0	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 2 & 28946 & 28904 \\ 12 & 29923 & 30153 \\ 19 & 8900 & 8901 \end{bmatrix}$

Table: 1

Therefore the cipher text matrix is $\begin{bmatrix} 2 & 28946 & 28904 \\ 12 & 29923 & 30153 \\ 19 & 8900 & 8901 \end{bmatrix}$.. Reducing each entry in the matrix to mod 26, the resultant message is 38181223191989, which is equivalent to dismxttij. [8]

CONCLUSIONS

In the proposed method a new concept of finite state machines is introduced, a choice of selecting the recurrence matrix is presented. The security levels are

1) Secret key
2) Recurrence matrix
3) Moore machine for residue modulo 'n'

In view of the above security levels the cracking of the code is very difficult by known attacks.

REFERENCES

1. B. Krishna Gandhi, A. Chandra Sekhar, S.Srilakshmi "Cryptographic scheme for digital signals using finite state machine" International journal of computer applications (September 2011).
2. Adesh K. Pandey. Reprint 2009 - "An introduction to automata theory and formal languages 'S. K. Kararia & sons. New Delhi.
3. A. Menezed, P.Van Oorschot Hand book of Applied and S. Vanstone Cryptography e-Book.
4. John E. Hopcroft, Rajeev Motwain, Jeffrey D. Ulman– "Introduction to automata theory, language, and computation" Vanstone3rd impression, 2007 CRC Press., Dorling Kindersley (India) Pvt. Ltd.
5. http://www.certicom.com/index.php/eccctutorial
6. EL Gamal. A public key Cryptosystem and a signature scheme based on discrete logarithms. In Advances in Cryptology (CRYPTO 1984), Springer.

7. W. Diffi and M. E. Helman "New directions in Cryptography." IEEE Transactions on Information theory, 22, 644-654, 1976.
8. A Course in Number Theory and Cryptography by Neal Koblitz.
9. Theory of Computations by Mishra and Chandrashekharan.

Source of support: Nil, Conflict of interest: None Declared

