Application Of Mealy Machine And Recurrence Relations In Cryptography

P. A. Jyotirmie[1], A. Chandra Sekhar[2], S. Uma Devi[3]

[1]Department of Engineering Mathematics, Andhra University, Visakhapatnam, INDIA
[2]Department of Mathematics, GIT, GITAM University, Visakhapatnam, INDIA
[3]Department of Engineering Mathematics, Andhra University, Visakhapatnam, INDIA

1. ABSTRACT

Cryptography is the study of techniques for ensuring the secrecy and authentication of the information. Public key encryption schemes are secure only if the authenticity of the public key is ensured. The importance of security of data is ever expanding with increasing impact of internet as means of communication and e-commerce. It is essential to protect the information from hackers and eavesdroppers. Secret sharing schemes are ideal for storing information that is highly sensitive. The motivation for secret sharing is secure key management.In this paper, with the help of finite state machine (Mealy machine) and recurrence matrices a secret sharing scheme is developed for secure communication which is designed for encryption and also maintains secrecy of the message.

Key words: Mealy Machine, Recurrence matrix, Fermat's and Mersenne's sequence.

1. INTRODUCTION

There is a scope for a wide range of application of automaton theory in the field of cryptology. In automata theory, a branch of theoretical computer science, a deterministic finite automaton (DFA)—also known as deterministic finite state machine—is a finite state machine that accepts/rejects finite strings of symbols and only produces a unique computation (or run) of the automaton for each input string.'Deterministic' refers to the uniqueness of the computation. 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 [2][9][4]. 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.

In this paper, new secret sharing scheme is proposed using finite state machines. Secret sharing schemes were discovered independently by Blakley and Shamir. The motivation for secret sharing is to have secure key management. In some situations, there is usually one secret key that provides access to many important files, if such a key is lost then all the important files become inaccessible. The basic idea in secret sharing is to divide the secret key into pieces and distribute the pieces to different persons so that certain subsets of the persons can get together to recover the key.[7][1]

In Mealy Machine every finite state machine has a fixed output. Mathematically Mealy machine is a six-tuple machine and is defined as :

M= ($Q, \sum, \Delta, \delta, \lambda', q_0$)

Q : A nonempty finite set of state in Mealy machine

$\sum$: A nonempty finite set of inputs.

Δ : A nonempty finite set of outputs.

δ : It is a transition function which takes two arguments one is input state and another is input symbol. The output of this function is a single state.

λ' : Is a mapping function which maps Q x $\sum$ to Δ, giving the output associated with each transition.

q_0 : Is the initial state in Q

Mealy machine can also be represented by transition table, as well as transition diagram.

Now, we consider a Mealy machine [4][8][9].

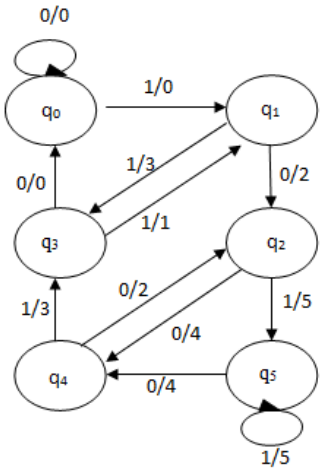

Fig 1 Mealy machine

..In the above diagram 0/1 represent input/output.

Recurrence Matrix

Recurrence matrix is a matrix whose elements are taken from a recurrence relation [1].

The recurrence matrix in this paper is defined as

$$R_n=\begin{bmatrix} 1 & C_{n+1} & C_n \\ C_{n+1} & 1 & C_{n+2} \\ C_n & C_{n+2} & 1 \end{bmatrix}$$

R_n is a symmetric matrix.

where $n \geq 0$ and C_n 's are either taken from Fermat's sequence or Mersenne's sequence.

The sequence 0, 1, 3, 7, 15, 31,... is the Mersenne sequence, and 2, 3, 5, 9, 17, 33, . . . is the Fermat sequence. These are just powers of 2 plus or minus 1

2. Proposed Algorithm

Encryption

Step 1

Represent plain text with 'P'

Step 2

Divide the plain text into n number of texts *i.e* into square matrices.

Step 3

Define a Finite state machine through public channel.

Step 4

Define input.

Step 5

Get output through finite state machine.

Step 6

Define recurrence matrix and choose recurrence relation.

Step 7

Define the value of n of recurrence relation.

Step 8

Define cipher text at each stage for all the plain texts.

Step 9

Send the cipher text to the respective receivers.

Decryption

The message is decrypted using the inverse operation and key to get the original message.

3 Performance analysis

Mathematical analysis

Algorithm proposed, is a simple application of addition of two matrices. But the recurrence matrix and elements of recurrence matrix are different at each stage depending on the input and output. It is very difficult to break the cipher text without proper key, defined operation and the chosen finite state machine. The key is defined as the sum of all the elements of this plain text.

4. Security analysis

Extracting, the original information from the Cipher text is difficult due to the selection of the recurrence matrix, secret key and chosen finite state machines. Brute force attack on key is also difficult because of the key size.

Table 1 Security analysis

S. No	Name of the attack	Possibility of the attack	Remarks
1	Cipher text attack	It is difficult to crack the cipher text.	Because of the chosen finite state machine and the key.
2	Known plain text attack	Difficult	Because of the chosen finite state machines and key.
3	Chosen plain text attack	Difficult	Because of the chosen finite state machine and key.
4	Adaptive chosen plain text attack	Difficult	Because of the chosen finite state machines and different individual keys.
5	Chosen cipher text attack	Difficult to crack Cipher text	Because of the chosen finite state machine, key and the recurrence matrix.
6	Adaptive chosen cipher text attack	Difficult to crack Cipher text	Because of the chosen finite state machine, key and chosen recurrence matrix at each stage.

5 Implementation

We assign 1 to letter a, 2 to letter b and so on and 26 to the letter z. We assign 27 to full stop and 0 to space.

Let us encrypt the 'Birds are singing.'

This sentence has eighteen characters which include space and full stop.

Step 1

P= BIRDS ARE SINGING

Step 2

As per the algorithm, we construct two plain texts

$$A=\begin{bmatrix} B & I & R \\ D & S & - \\ A & R & E \end{bmatrix}=\begin{bmatrix} 2 & 9 & 18 \\ 4 & 19 & 0 \\ 1 & 18 & 5 \end{bmatrix}$$

$$\text{And } B=\begin{bmatrix} - & S & I \\ N & G & I \\ N & G & . \end{bmatrix}=\begin{bmatrix} 0 & 19 & 9 \\ 14 & 7 & 9 \\ 14 & 7 & 27 \end{bmatrix}$$

Now, we apply the remaining algorithm to plain texts A and B.

Step 3

Mealy machine is publicized through public channel.

Step 4

All the elements of both the plain texts are added and converted into binary form. This is the input.

The sum of all the elements of plain text A is equal to $76 = (1001100)_2$

And B is equal to $106 = (1101010)_2$

Step 5

The output of the above key is found with the help of Mealy machine.

Step 6

The recurrence matrix is defined as

$$R_n=\begin{bmatrix} 1 & C_{n+1} & C_n \\ C_{n+1} & 1 & C_{n+2} \\ C_n & C_{n+2} & 1 \end{bmatrix}$$

The elements of recurrence matrix are taken from

Sl. No	Input	Output / Transition	N	Key values	Cipher text
1	1	1	1	$\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}$	$\begin{bmatrix}1&22&10\\17&8&16\\15&14&28\end{bmatrix}$
2	1	3	3	$\begin{bmatrix}1&15&7\\15&1&31\\7&31&1\end{bmatrix}$	$\begin{bmatrix}2&37&17\\32&9&47\\22&45&29\end{bmatrix}$
3	0	0	0	$\begin{bmatrix}1&3&2\\3&1&5\\2&5&1\end{bmatrix}$	$\begin{bmatrix}3&40&19\\35&10&52\\24&50&30\end{bmatrix}$
4	1	1	1	$\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}$	$\begin{bmatrix}4&43&20\\38&11&59\\25&57&31\end{bmatrix}$
5	0	2	2	$\begin{bmatrix}1&9&5\\9&1&17\\5&17&1\end{bmatrix}$	$\begin{bmatrix}5&52&25\\47&12&76\\30&74&32\end{bmatrix}$
6	0	5	25	$\begin{bmatrix}1&63&31\\63&1&127\\5&17&1\end{bmatrix}$	$\begin{bmatrix}6&115&56\\110&10&203\\35&97&33\end{bmatrix}$
7	0	4	4	$\begin{bmatrix}1&33&17\\33&1&65\\17&65&1\end{bmatrix}$	$\begin{bmatrix}7&148&73\\143&14&268\\52&156&34\end{bmatrix}$

a recurrence relation.

Step 7

Let 'C_{i+1}' be the cipher text at C_i+i^{th} state and is defined as

$C_{i+1} = C_i + R_n$

Where R_n depends on the input.

$$R_n = \begin{cases} \text{Fermat's sequence when input=0} \\ \text{Mersenne's sequence when input = 1} \end{cases}$$

Step 8

Calculate cipher text at each state.

Then the cipher text at each state is as follows:

Receiver 1

Sl. No	Input	Output / Transition	N	Key values	Cipher text
1	1	1	1	$\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}$	$\begin{bmatrix}3&12&19\\7&20&7\\2&25&6\end{bmatrix}$
2	0	2	2	$\begin{bmatrix}1&9&5\\9&1&7\\5&17&1\end{bmatrix}$	$\begin{bmatrix}4&21&24\\16&21&24\\7&42&7\end{bmatrix}$
3	0	4	4	$\begin{bmatrix}1&33&17\\33&1&65\\17&65&1\end{bmatrix}$	$\begin{bmatrix}5&54&41\\49&22&89\\24&117&8\end{bmatrix}$
4	1	3	3	$\begin{bmatrix}1&15&7\\15&1&31\\7&31&1\end{bmatrix}$	$\begin{bmatrix}6&69&48\\64&23&1240\\31&138&9\end{bmatrix}$
5	1	1	1	$\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}$	$\begin{bmatrix}7&72&49\\67&24&127\\32&145&1\end{bmatrix}$
6	0	2	2	$\begin{bmatrix}1&9&5\\9&1&17\\5&17&1\end{bmatrix}$	$\begin{bmatrix}8&81&54\\76&25&144\\37&162&11\end{bmatrix}$
7	0	4	4	$\begin{bmatrix}1&33&17\\33&1&65\\17&65&1\end{bmatrix}$	$\begin{bmatrix}9&114&71\\109&26&209\\54&227&12\end{bmatrix}$

Receiver 2

Send cipher text $\begin{bmatrix}9&114&71\\109&26&209\\54&227&12\end{bmatrix}$ to receiver 1

And cipher text $\begin{bmatrix}7&148&73\\143&14&268\\52&156&34\end{bmatrix}$ to receiver 2.

Concluding Remarks

Algorithm proposed, is based on finite state machine and operations on matrices. Secrecy is maintained at four levels

1. The secret key.

2. The chosen finite state machine

3. The different operations

4. The recurrence matrix.

The obtained cipher text becomes quite difficult to break or to extract the original information even when the algorithm is known.

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] ELGamal. 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.