A New Cryptographic Scheme Involving Finite State Machine and Recurrence Matrix

Ayush Mittal

Abstract: ***The object of this paper is to develop a new cryptographic scheme involving finite state machine and Mersenne's recurrence matrix. The proposed algorithm is more secure cryptographic algorithm that solves many problems which are facing now days. For secure communication the designed encryption scheme involving finite state machine and recurrence matrix maintained the secrecy of the message.***

Keywords: Finite State Machine, Recurrence Matrix, Encryption, Decryption, Binary Number.

I. INTRODUCTION

To ensuing the secrecy and authentication of information, we studied various techniques in cryptography. If authenticity of the public key is ensured then public key encryption schemes are secure. With increasing impact of internet by means of communication and e-commerce, the importance of security of data is ever expanding. The refer protection of information from hackers is very essential. To storing of highly sensitive information, the secret sharing schemes are ideal.

In the process of encryption as well as inverse process or in decryption process, many mathematical models are play's an active role. The 'tracing of the inverse of a function is not easy' is the main idea behind the designing of such type of mathematical function. An art of coding and decoding of information is known as cryptography. It is used in electronic communication as security mechanism. 'Plain Text' is message which we want to send and 'Cipher Text' is the disguised message. 'Encryption' is the process which convert the 'Plain Text' into 'Cipher Text', while decryption is the reveres process that converts the 'Cipher Text' into 'Plain Text' [6].

In the field of cryptography application of automaton theory having a wide range. A deterministic finite automaton (DFA) which is also known as deterministic finite state machine is a branch of theoretical computer science in automata theory. For each input string, this finite state machine produces a unique computation. Deterministic means uniqueness of the computation. With discrete inputs and outputs, the finite automaton is a mathematical model of a system. Finite automata are called non-deterministic finite automata when it allows 0, 1 or more transitions from a state on the same input symbol. The outcome for deterministic automata is a state i.e. element of S, while outcome is the subset of S in case of non-deterministic automata, where S is the finite non-empty set of states. Finite state machine is a behavior model that composed a finite number of states and transition between them. Recently, in cryptography finite state machines are used to encrypt the message as well as maintain secrecy of the message also.

Finite State Machine:

A mathematical model of computation that is used to design both sequential logic circuit and computer program is known as finite state machine [2]. It is an abstract machine and it can be one of the finite states. It can be reside in one state only at a time. The state is called current state in which machine can reside at any given time. When machine is initiated by triggering event or condition, then it can change from one state to another state, which is called transition.

A finite machine M is specified by a 6-tuple (S, I, O, f, g, s_0), where

1. S is a finite set of states (s_0, s_1, s_2, …) whose elements are called state of machine.
2. s_0 is a special element of S referred to as the initial state of the machine.
3. I = {i_1, i_2, …} is a finite set of input letters.
4. O = {o_1, o_2, …} is a finite set of output letters.
5. f is a function from S × I to S called the transition function.
6. g is a function from S to O called the output function.

At any instant, a finite state machine is in one of its states. On receiving an input symbol, the machine will go to another state according to the transition function. Moreover, at each state the machine produces an output according to the output function. At the very beginning, the machine is in the initial state s_0.

Finite state machines are divided into two types:

1. Mealy Machine
2. Moore machine

If in a finite state machine, output depends on the present state as well as the present input, then this type of machine is called Mealy machine, while in the Moore machine the outputs depended on only the present state. Here we will use Mealy machine.

Recurrence Matrix:

A matrix whose elements are taken from a recurrence relation is known as recurrence matrix. Here in this paper we use the Mersenne's recurrence relation which is generated from Mersenne's sequence [1]. The Mersenne's sequence is defined as 0, 1, 3, 7, 15, 31, 63, … Here we define Mersenne's recurrence matrix of order 4 × 4 as follows:

$$R_M = \begin{bmatrix} 1 & C_{n+2} & C_{n+1} & C_n \\ C_{n+2} & 1 & C_{n+4} & C_{n+3} \\ C_{n+1} & C_{n+4} & 1 & C_{n+5} \\ C_n & C_{n+3} & C_{n+5} & 1 \end{bmatrix}$$

Revised Manuscript Received on January 5, 2020

Mr.Ayush Mittal, Phd, Computer Science and Engineering from Sarvepalli Radhakrishnan University, Bhopal, MP.

$$= \begin{bmatrix} 1 & 7 & 3 & 1 \\ 7 & 1 & 31 & 15 \\ 3 & 31 & 1 & 63 \\ 1 & 15 & 63 & 1 \end{bmatrix}$$

where $n \geq 0$ and C_n's are taken from Mersenne's sequence. Here we use recurrence matrix as secrete key.

II. LITERATURE REVIEW

Sirivaram [5], Jyotirmie [3], Krishna [4] and various researchers are developed an innovative technique for encrypting and hiding the data using finite state machines, Laplace transformation, LU decomposition, Fourier sine and cosine transformation, Fibonacci series, balancing and Lucas-balancing numbers and other tools also, which is designed for encryption and also maintains secrecy of the message.

III. METHODOLOGY

Following Sirivaram [5], Jyotirmie [3], Krishna [4] and various researchers in this paper we propose to develop a new cryptographic scheme involving finite state machine and Mersenne's recurrence matrix. Proposed algorithm is based on modulo multiplication of Mersenne's recurrence matrix as secret key and chosen finite state machine. Finite state machine, secret key and private key maintained the secrecy. Without proper key and the chosen finite state machine, it is very difficult to break the cipher text. To avoid the cipher attacks the number of element in the sequence must be maximum.

For encryption we use the following formula:

Cipher matrix at q_{i+1}th state
= Cipher matrix at q_ith state ×
(Key matrix) $^{(\text{output at } q_{i+1}\text{th state})}$(mod p)

For decryption we use the following formula:

Cipher matrix at q_ith state
= Cipher matrix at q_{i+1}th state ×
[inverse of {(Key matrix)$^{(\text{output at } q_{i+1}\text{th state})}$}](mod p)

IV. ALGORITHM

The following conversion table for the alphabets/symbols is used for substitution.

Table I

alphabet/ symbol	numerical value	alphabet/ symbol	numerical value
@	0	P	16
A	1	Q	17
B	2	R	18
C	3	S	19
D	4	T	20
E	5	U	21
F	6	V	22
G	7	W	23
H	8	X	24
I	9	Y	25
J	10	Z	26
K	11	[	27
L	12	\	28
M	13	]	29
N	14	space	30
O	15		

Encryption:

1. Consider the plain text. Convert each alphabet of plain text into their corresponding numeric value using Table I (agreed by sender and receiver) and divide the plain text into n number of texts, also arrange them into a square matrix of order n, n > 0, call them plain matrix.
2. Add all the elements of plain text matrix and convert them into binary form, which is the input and secrete key also.
3. Define a Finite state machine, here we use Mealy machine. Obtained the output from Finite state machine under residue mod q (agreed by sender and receiver).
4. Consider the key matrix which is generated from recurrence matrix.
5. For all plain text matrix, calculate the cipher text matrix at each stage using the following formula:
   Cipher matrix at q_{i+1}th state
   = Cipher matrix at q_ith state ×
   (Key matrix) $^{(\text{output at } q_{i+1}\text{th state})}$(mod p)
6. Convert numeric value of each element of last cipher text matrix into corresponding alphabet and send the cipher text to receiver.

Decryption:

1. Receiver received the secret key, cipher text, finite state machine and recurrence matrix.
2. Convert each alphabets/symbols of the cipher text into corresponding numeric value using Table I and apply the multiplicative inverse of the recurrence matrix and the secret key. To do this using the following formula:
   Cipher matrix at q_ith state
   = Cipher matrix at q_{i+1}th state ×
   [inverse of {(Key matrix)$^{(\text{output at } q_{i+1}\text{th state})}$}]
   (mod p)
3. Finally obtain the original message.

Illustration:

Encryption Steps:

1. Consider the message ENCRYPT DECRYPT as Plaintext.

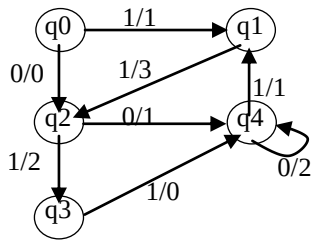
2. Convert the chosen plain text into corresponding numerical values using above given Table 1 and arrange them in a matrix of order 4, we get

$$P = \begin{bmatrix} 5 & 14 & 3 & 18 \\ 25 & 16 & 20 & 30 \\ 4 & 5 & 3 & 18 \\ 25 & 16 & 20 & 30 \end{bmatrix}$$

3. Sum of the all elements of plain text P is equal to 252 = $(11111100)_2$. Suppose 11111100 is the secret key.

4. The Mealy machine for input key 11111100 with output under residue mod 5 (say) is define as follows:

SN	Input	Previo-us State	Prese-nt State	Out put	Cipher matrix
1	1	q_0	q_1	1	$\begin{bmatrix}6&9&5&19\\10&21&1&5\\4&24&2&7\\10&21&1&5\end{bmatrix}$
2	1	q_1	q_2	3	$\begin{bmatrix}20&22&30&26\\9&25&6&27\\7&12&22&18\\9&25&6&27\end{bmatrix}$
3	1	q_2	q_3	2	$\begin{bmatrix}10&23&28&9\\30&12&17&10\\19&1&7&3\\30&12&17&10\end{bmatrix}$
4	1	q_3	q_4	0	$\begin{bmatrix}10&23&28&9\\30&12&17&10\\19&1&7&3\\30&12&17&10\end{bmatrix}$
5	1	q_4	q_1	1	$\begin{bmatrix}16&11&5&20\\20&0&24&20\\19&24&5&13\\20&0&24&20\end{bmatrix}$
6	1	q_1	q_2	3	$\begin{bmatrix}28&25&8&29\\30&5&15&2\\2&20&30&0\\30&5&15&2\end{bmatrix}$
7	0	q_2	q_4	1	$\begin{bmatrix}8&5&28&6\\19&28&14&29\\15&3&5&22\\19&28&14&29\end{bmatrix}$
8	0	q_4	q_4	2	$\begin{bmatrix}24&16&16&0\\1&1&14&12\\1&22&6&13\\1&1&14&12\end{bmatrix}$



where i/o indicate input/output.

5. Consider the key matrix is

$$K = R_M(mod31) = \begin{bmatrix}1&7&3&1\\7&1&31&15\\3&31&1&63\\1&15&63&1\end{bmatrix}(mod31)$$

$$\Rightarrow K = \begin{bmatrix}1&7&3&1\\7&1&0&15\\3&0&1&1\\1&15&1&1\end{bmatrix}$$

6. Calculate cipher matrix on each state by the following formula:

Cipher text matrix at q_{i+1}th state
= Cipher text matrix at q_ith state ×
(Key matrix) $^{(\text{output at } q_{i+1}\text{th state})}$(mod p),

where we take p = 31. Therefore

(i) $C_1 = P\times(K)^{(\text{output at } q_{i+1}\text{th state})}$ (mod 31)

$$= \begin{bmatrix}5&14&3&18\\25&16&20&30\\4&5&3&18\\25&16&20&30\end{bmatrix}\begin{bmatrix}1&7&3&1\\7&1&0&15\\3&0&1&1\\1&15&1&1\end{bmatrix}(\text{mod } 31)$$

$$= \begin{bmatrix}6&9&5&19\\10&21&1&5\\4&24&2&7\\10&21&1&5\end{bmatrix}$$

(ii) $C_2 = C_1\times(K)^{(\text{output at } q_{i+1}\text{th state})}$ (mod 31)

$$= \begin{bmatrix}6&9&5&19\\10&21&1&5\\4&24&2&7\\10&21&1&5\end{bmatrix}\begin{bmatrix}394&2099&297&612\\2099&1033&160&4227\\297&160&37&563\\612&4227&563&898\end{bmatrix}(\text{mod } 31)$$

$$= \begin{bmatrix}20&22&30&26\\9&25&6&27\\7&12&22&18\\9&25&6&27\end{bmatrix}$$

(iii) $C_3 = C_2\times(K)^{(\text{output at } q_{i+1}\text{th state})}$ (mod 31)

$$= \begin{bmatrix}20&22&30&26\\9&25&6&27\\7&12&22&18\\9&25&6&27\end{bmatrix}\begin{bmatrix}60&29&7&110\\29&275&36&37\\7&36&11&5\\110&37&5&228\end{bmatrix}(\text{mod } 31)$$

$$= \begin{bmatrix}10&23&28&9\\30&12&17&10\\19&1&7&3\\30&12&17&10\end{bmatrix}$$

(iv) $C_4 = C_3\times(K)^{(\text{output at } q_{i+1}\text{th state})}$ (mod 31)

$$= \begin{bmatrix}10&23&28&9\\30&12&17&10\\19&1&7&3\\30&12&17&10\end{bmatrix}$$

(v) $C_5 = C_4\times(K)^{(\text{output at } q_{i+1}\text{th state})}$ (mod 31)

$$= \begin{bmatrix}10&23&28&9\\30&12&17&10\\19&1&7&3\\30&12&17&10\end{bmatrix}\begin{bmatrix}1&7&3&1\\7&1&0&15\\3&0&1&1\\1&15&1&1\end{bmatrix}(\text{mod } 31)$$

$$= \begin{bmatrix}16&11&5&20\\20&0&24&20\\19&24&5&13\\20&0&24&20\end{bmatrix}$$

(vi) $C_6 = C_5\times(K)^{(\text{output at } q_{i+1}\text{th state})}$ (mod 31)

$$= \begin{bmatrix}16&11&5&20\\20&0&24&20\\19&24&5&13\\20&0&24&20\end{bmatrix}\begin{bmatrix}394&2099&297&612\\2099&1033&160&4227\\297&160&37&563\\612&4227&563&898\end{bmatrix}(\text{mod } 31)$$

$$= \begin{bmatrix}28&25&8&29\\30&5&15&2\\2&20&30&0\\30&5&15&2\end{bmatrix}$$

(vii) $C_7 = C_6\times(K)^{(\text{output at } q_{i+1}\text{th state})}$ (mod 31)

$$= \begin{bmatrix}28&25&8&29\\30&5&15&2\\2&20&30&0\\30&5&15&2\end{bmatrix}\begin{bmatrix}1&7&3&1\\7&1&0&15\\3&0&1&1\\1&15&1&1\end{bmatrix}(\text{mod } 31)$$

$$= \begin{bmatrix}8&5&28&6\\19&28&14&29\\15&3&5&22\\19&28&14&29\end{bmatrix}$$

(viii) $C_8 = C_7\times(K)^{(\text{output at } q_{i+1}\text{th state})}$ (mod 31)

$$= \begin{bmatrix}8&5&28&6\\19&28&14&29\\15&3&5&22\\19&28&14&29\end{bmatrix}\begin{bmatrix}60&29&7&110\\29&275&36&37\\7&36&11&5\\110&37&5&228\end{bmatrix}(\text{mod } 31)$$

$$= \begin{bmatrix} 24 & 16 & 16 & 0 \\ 1 & 1 & 14 & 12 \\ 1 & 22 & 6 & 13 \\ 1 & 1 & 14 & 12 \end{bmatrix}$$

Hence Cipher text is XPP@AANLAVFMAANL.

Decryption Steps:

1. Consider the cipher text
   XPP@AANLAVFMAANL
3. Convert each character of cipher text into corresponding numerical values using Table I and arrange them in a matrix of order 4, we get
4. $$\begin{bmatrix} 24 & 16 & 16 & 0 \\ 1 & 1 & 14 & 12 \\ 1 & 22 & 6 & 13 \\ 1 & 1 & 14 & 12 \end{bmatrix} = C_8 \text{ (say)}$$

3. Calculate all cipher text matrix at each state in reverse order by using the following formula:

Cipher matrix at q_ith state = Cipher matrix at q_{i+1}th state × [inverse of {(Key matrix)$^{(\text{output at } q_{i+1}\text{th state})}$}](mod p), where we take p = 31. Therefore

(i) $C_7 = C_8 \times (\text{invers of } K^2) \pmod{31}$

$$= \begin{bmatrix} 24 & 16 & 16 & 0 \\ 1 & 1 & 14 & 12 \\ 1 & 22 & 6 & 13 \\ 1 & 1 & 14 & 12 \end{bmatrix} \begin{bmatrix} 1 & 16 & 14 & 20 \\ 16 & 19 & 29 & 25 \\ 14 & 29 & 6 & 19 \\ 20 & 25 & 19 & 23 \end{bmatrix} \pmod{31}$$

$$= \begin{bmatrix} 8 & 5 & 28 & 6 \\ 19 & 28 & 14 & 29 \\ 15 & 3 & 5 & 22 \\ 19 & 28 & 14 & 29 \end{bmatrix}$$

(ii) $C_6 = C_7 \times (\text{invers of } K) \pmod{31}$

$$= \begin{bmatrix} 8 & 5 & 28 & 6 \\ 19 & 28 & 14 & 29 \\ 15 & 3 & 5 & 22 \\ 19 & 28 & 14 & 29 \end{bmatrix} \begin{bmatrix} 20 & 13 & 6 & 27 \\ 13 & 10 & 9 & 14 \\ 6 & 9 & 5 & 9 \\ 27 & 14 & 9 & 3 \end{bmatrix} \pmod{31}$$

$$= \begin{bmatrix} 28 & 25 & 8 & 29 \\ 30 & 5 & 15 & 2 \\ 2 & 20 & 30 & 0 \\ 30 & 5 & 15 & 2 \end{bmatrix}$$

(iii) $C_5 = C_6 \times (\text{invers of } K^3) \pmod{31}$

$$= \begin{bmatrix} 28 & 25 & 8 & 29 \\ 30 & 5 & 15 & 2 \\ 2 & 20 & 30 & 0 \\ 30 & 5 & 15 & 2 \end{bmatrix} \begin{bmatrix} 15 & 21 & 28 & 3 \\ 21 & 17 & 17 & 11 \\ 28 & 17 & 19 & 27 \\ 3 & 11 & 27 & 14 \end{bmatrix} \pmod{31}$$

$$= \begin{bmatrix} 16 & 11 & 5 & 20 \\ 20 & 0 & 24 & 20 \\ 19 & 24 & 5 & 13 \\ 20 & 0 & 24 & 20 \end{bmatrix}$$

(iv) $C_4 = C_5 \times (\text{invers of } K) \pmod{31}$

$$= \begin{bmatrix} 16 & 11 & 5 & 20 \\ 20 & 0 & 24 & 20 \\ 19 & 24 & 5 & 13 \\ 20 & 0 & 24 & 20 \end{bmatrix} \begin{bmatrix} 20 & 13 & 6 & 27 \\ 13 & 10 & 9 & 14 \\ 6 & 9 & 5 & 9 \\ 27 & 14 & 9 & 3 \end{bmatrix} \pmod{31}$$

$$= \begin{bmatrix} 10 & 23 & 28 & 9 \\ 30 & 12 & 17 & 10 \\ 19 & 1 & 7 & 3 \\ 30 & 12 & 17 & 10 \end{bmatrix}$$

(v) $C_3 = C_4 \times (\text{invers of } K^0) \pmod{31}$

$$= \begin{bmatrix} 10 & 23 & 28 & 9 \\ 30 & 12 & 17 & 10 \\ 19 & 1 & 7 & 3 \\ 30 & 12 & 17 & 10 \end{bmatrix} \pmod{31}$$

$$= \begin{bmatrix} 10 & 23 & 28 & 9 \\ 30 & 12 & 17 & 10 \\ 19 & 1 & 7 & 3 \\ 30 & 12 & 17 & 10 \end{bmatrix}$$

(vi) $C_2 = C_3 \times (\text{invers of } K^2) \pmod{31}$

$$= \begin{bmatrix} 10 & 23 & 28 & 9 \\ 30 & 12 & 17 & 10 \\ 19 & 1 & 7 & 3 \\ 30 & 12 & 17 & 10 \end{bmatrix} \begin{bmatrix} 1 & 16 & 14 & 20 \\ 16 & 19 & 29 & 25 \\ 14 & 29 & 6 & 19 \\ 20 & 25 & 19 & 23 \end{bmatrix} \pmod{31}$$

$$= \begin{bmatrix} 20 & 22 & 30 & 26 \\ 9 & 25 & 6 & 27 \\ 7 & 12 & 22 & 18 \\ 9 & 25 & 6 & 27 \end{bmatrix}$$

(vii) $C_1 = C_2 \times (\text{invers of } K^3) \pmod{31}$

$$= \begin{bmatrix} 20 & 22 & 30 & 26 \\ 9 & 25 & 6 & 27 \\ 7 & 12 & 22 & 18 \\ 9 & 25 & 6 & 27 \end{bmatrix} \begin{bmatrix} 15 & 21 & 28 & 3 \\ 21 & 17 & 17 & 11 \\ 28 & 17 & 19 & 27 \\ 3 & 11 & 27 & 14 \end{bmatrix} \pmod{31}$$

$$= \begin{bmatrix} 6 & 9 & 5 & 19 \\ 10 & 21 & 1 & 5 \\ 4 & 24 & 2 & 7 \\ 10 & 21 & 1 & 5 \end{bmatrix}$$

(viii) $C = C_1 \times (\text{invers of } K) \pmod{31}$

$$= \begin{bmatrix} 6 & 9 & 5 & 19 \\ 10 & 21 & 1 & 5 \\ 4 & 24 & 2 & 7 \\ 10 & 21 & 1 & 5 \end{bmatrix} \begin{bmatrix} 20 & 13 & 6 & 27 \\ 13 & 10 & 9 & 14 \\ 6 & 9 & 5 & 9 \\ 27 & 14 & 9 & 3 \end{bmatrix} \pmod{31}$$

$$= \begin{bmatrix} 5 & 14 & 3 & 18 \\ 25 & 16 & 20 & 30 \\ 4 & 5 & 3 & 18 \\ 25 & 16 & 20 & 30 \end{bmatrix}$$

4. Convert each character of last matrix into corresponding numerical values using Table I, we get the original plain text as follows:

ENCRYPT DECRYPT

V. RESULT AND DISCUSSION

Due to selection of the recurrence matrix, secret key and chosen finite state machine the extraction of original plain text is difficult. Because of the size of key brute force attack is also not easier.

Due to the chosen finite state machine alongwith secret key which is generated from Mersenne's sequence, it is very difficult to extract the original information. Brute force attack is also difficult because of the size of key. Explanation of result is as follows:

SN	Name of attack	Opportunity of attack	Explanation
1	Cipher text attack	Very Difficult	Due to the chosen finite state machine and secret key
2	Chosen cipher text attack	Very Difficult	Due to the chosen finite state machine and secret key
3	Adaptive chosen cipher text attack	Very Difficult	Due to the chosen finite state machine and secret key
4	Known plain text attack	Difficult	Due to the chosen finite state machine and secret key
5	Chosen plain text attack	Difficult	Due to the chosen finite state machine and secret key
6	Adaptive chosen plain text attack	Difficult	Due to the chosen finite state machine and secret key

VI. CONCLUSION

Proposed algorithm is based on different operations on matrices and chosen finite state machine. The security is maintained at four levels i.e. chosen finite state machine, recurrence matrix, secret key and different operations on matrices. Extraction of original information from cipher text is quite difficult however algorithm is also known.

REFERENCES

1. David Burton: Elementary Number Theory, McGraw Hill, 2011.
2. John Hopcroft, Jeffrey Ullman: Introduction to Automata Theory, Languages, and Computation, Addison-Wesley, 1979.
3. Jyotirmie P. A., Srilakshmi S., Sekhar A. Chandra and Devi S. Uma: Cryptographic Secret Sharing Scheme of Finite State Machines Using LU Decomposition, International Journal of Mathematical Archive-4(3), 2013, pp. 209-214.
4. Krishna Gandhi B., Chandra Sekhar A., Srilakshmi S.: Cryptographic Scheme for Digital Signals using Finite State Machines, International Journal of Computer Applications,)Vol. 29– No.6, September 2011, pp.61-63.
5. Sirivaram Srilakshmi: New Encryption Scheme Using Laplace Transforms and Finite State Machine, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Special Issue 13, July 2017, pp. 119-122.
6. Stallings W.: Cryptography and Network Security: Principles and Practices, Prentice Hall, 1999.

AUTHORS PROFILE

Mr.Ayush Mittal, did his post-graduation in M.Tech(Master of Technology) in Computer Science and Engineering from Indian Institute of Information Technology and Management(IIITM),Gwalior, MP in 2015. He has also received gold medal in post-graduation degree. Currently, he is pursuing his Phd in Computer Science and Engineering from SRK university, Bhopal, MP. His area of interest includes robotics, cryptography and embedded systems. He has published 2 research papers in International Journals.