Punjab University Journal of Mathematics (2023),55(3),89-98
https://doi.org/10.52280/pujm.2023.550301

IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS USING MOORE MACHINE AND RECURRENCE MATRIX

Rachna Navalakhe
Department of Applied Mathematics and Computational Science,
S.G.S.I.T.S Indore, M.P., India
E-mail: sgsits.rachna@gmail.com

Harsha Atre
Department of Applied Science, SAGE University Indore, M.P.,INDIA
E-mail: atre.harsha.p22@gmail.com

Received: 28 November,2022 / Accepted: 24 February, 2023 / Published online: 25 March, 2023

Abstract. Today in this modern and digital world, people need privacy and security during digital communication of their secret information. Cryptographic techniques provide methods for secure digital communication. In this paper, we have proposed a secret message sharing algorithm using finite state machine and recurrence relation to enhance the security level of the messages which is being sent between sender and receiver. The proposed new cryptographic encryption and decryption algorithm has been implemented using Moore machine which is a type of finite state automaton and two recurrence matrices namely Fibonacci numbers and Mersenne numbers. The importance of these algorithms is that, we can send information securely through the communication channel using them. The efficiency of the proposed algorithm has been analyzed and the analysis shows high level cryptographic protection during digital communication. In these algorithms we have used multiple set of keys to encipher the original message and its inverse to decipher it again and the authenticity of algorithms is assured because these algorithms have different levels of security which enhance the chances to keep our data or information confidential and secure for long time. There are many states in Moore machine to calculate the appropriate output. In every state it takes a new recurrence relation which depends upon the input. To compute the output, we apply mathematical operation which is our cipher text. At each level we have number of cipher text which increases the data security.

Key Words: Cryptography, Cipher and plain text, Finite state machine, Recurrence relation.

1. Introduction and preliminaries

Cryptography is an art of writing codes and protecting data in a particular form so that only those for whom it is defined can read and access it. The cryptography consists of two techniques one is encryption and another one is decryption. Both the techniques are mainly used to secure the information. Encryption is a method of conversion of plain text into cipher text. Decryption is the reverse process of encryption i.e., conversion of cipher text into plain text. One who practices the encryption and decryption algorithms is known as cryptographers. The information is determined by the user who has some secret message. The secret message can decipher the information back into its original form. The secret message can be called as a key. Now a days, the importance of security of data has been increased due to the arrival of digital communication in business and in our daily life. Therefore, it become necessary to protect our confidential data and information from hackers. According to [2] cryptographic methods are currently the most dependable means of safeguarding information. [16] studied, many different types of attacks on cryptographic primitives and protocols. In order to protect the data from threat of attack, many secret sharing cryptographic schemes and techniques can be applied during transmission process of the message. Cryptography in its more contemporary form was fathered by Claude Shannon in 1949. Claude Shannon was known widely for his work in electronic communications and in digital computing. The basic mathematical theory of cryptography has been established by Shannon. In [8] modern cryptography depends mainly on mathematics and the use of digital systems. In the modern world, people need privacy and security during communication and cryptography provides methods and techniques for a secure communication. Based on the key type, the cryptosystems can be classified into symmetric key (private key) and asymmetric key (public key) cryptosystem. In a symmetric cryptosystem, a system depends on using the same key for encryption and decryption. In public key cryptography, a user generates a pair of keys consisting of a private key that is kept secret and a public key which is shared with others. Depending on the application, either the giver's private key or the receiver's public key can be utilized to encrypt the original message by [21].

The basic idea of cryptosystem based on finite automata is quite simple: the encryption key consists of an automaton and its inverse is the decryption key. Therefore, in many cases it is difficult to find the automaton that inverts the function of a given automata. Moreover, these systems have been designed in order to overcome the biggest drawbacks of the cryptosystem based on grammar and word problem, i.e. insecurity, ciphertext expansion and lack of digital signature. Most of finite automata-based cryptosystem use transducer machines (Mealy and Moore machines), cellular automata, and automata without output (acceptors).

2. Literature review

The theory of finite automata, models of computing devices with a finite non-extensible memory, was initiated in 1940s and 1950s mainly by McCulloch, Pitts and Kleene.

[13] were the first to employ finite automata in cryptography. In the early 1980s, Professor Tao and Professor Chen Shihua conducted research on the theory of the invertibility of finite automata.

The work by Professor Tao develops a theory and contains strong results concerning invertible finite automata: the input sequence can be recovered from the output sequence. This is a desirable feature both in cryptography and error correcting codes.
This theory served as the foundation for a novel streaming cryptosystem featuring a public key. In 1985, the finite automation public key cryptosystem (FAPKC) was unveiled to the academic community by [6]. While all versions of FAPKC share a common cryptosystem algorithm, they differ in their generation of various types of finite automata employed for encrypting/decrypting data, as detailed more extensively in [15].
[14] introduced the first cryptosystem based on cellular automata (CA), which utilized a simple one-dimensional CA consisting of a circular register with cells, each assigned a value of either 0 or 1. However, due to a lack of key, this system was successfully attacked by known plaintext. The vulnerabilities of this cryptosystem were highlighted by [11]. To address these shortcomings and enhance security and performance [14] proposed the use of reversible cellular automata (RCA) as efficient encryption and decryption devices. In 1985 [19, 20] developed a public key cryptosystem called finite automata public key cryptosystem (FAPKC), which is based on the Mealy machine and relies on the difficulty of inverting finite automata composition. These systems offer several advantages, including rapid implementation in software and hardware and the ability to serve as means for confidentiality and digital signature. The public key in these systems is a combination of two finite automata, while the private key is comprised of the inverse of these automata. In 2008 [3] introduced a novel stream cipher founded on the Rabin-Scott model of finite automata, which serves as a key for encrypting plaintext and decrypting ciphertext.
[12] and [9] introduced new cryptographic algorithms in 2012 that rely on Mealy/Moore automata and recursive functions.
A novel approach to encrypting and concealing data using finite state machines, Laplace transformation, LU decomposition, Fourier sine and cosine transformation, Fibonacci series, balancing and Lucas-balancing numbers and other tools has been developed by [17], [4], [7] and several other researchers. This technique is specifically designed for encrypting messages while preserving their confidentiality. In Russia, they also deal with the use of finite automata in cryptography. The example given by [1] of using finite automata as cryptographic algorithms and their components describes cellular automaton generators of pseudorandom sequences, cellular automaton hash functions, finite automaton symmetric and asymmetric ciphers which demonstrates functional equivalence of flow and automaton cryptosystems.

3. FINITE STATE AUTOMATA

The finite state machine is a mathematical model of a system with discrete inputs and outputs. Finite state automata [10] are an abstract machine that can be in exactly one of a finite number of states at any given time. Finite state machine has finite internal memory where an input feature reads symbols one at a time and an output feature produces output which can be understood by user once the model is created. The state at which finite state machine takes the input is known as initial state which goes through transitions from one state to another state. When all the symbols have been read by finite state machine then it is marked as successful flow of operation called as an accepting state. Finite automata may

have outputs corresponding to each transition. There are two types of finite state machines that generate output −

(i) **Moore Machine:** Moore machine is FSM whose outputs depend on only the present state.
(ii) **Mealy Machine:** A Mealy Machine is FSM whose output depends on the present state as well as the present input.

4. Recurrence relation

A recurrence relation is an equation that defines a sequence based on a rule that gives the next term as a function of the previous term for some function f. The recurrence relation is of the form $A_0x_n + A_1x_{n-1} + A_2x_{n-2} + ... + A_kx_{n-k} = Y_n$
Matrix which is derived from the recurrence relation is known as recurrence matrix and the values may be taken from this relation.

(i) **Fibonacci Numbers:** Fibonacci Numbers [2, 18] is the sum of two preceding terms or number which lies in that series. Fibonacci numbers can be given by recurrence relation $F_n = F_{n-1} + F_{n-2}$ with initial conditions $F_1 = 1, F_2 = 1$ or $F_0 = 0, F_1 = 1$.
Now introduce a 2*2 square matrix as shown below $M = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ According to the above matrix values are $M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ where $n = 0, 1, 2, ..., F_{n-k}$ are the Fibonacci numbers.
(ii) **Fermat Numbers:** In the field of Mathematics, the Fermat number [5] is first studied by Pierre de Fermat who discovered it. Fermat number are $2, 3, 5, 9, 17, 33, ...$ and it is of the form $F_n = 2^n + 1$.
(iii) **Mersenne Numbers:** Mersenne numbers [5] are named after the French mathematician Marin Mersenne. These numbers are of the form
$M_n = 2^n - 1$, where n is a natural number and Mersenne numbers are $0, 1, 3, 7, 15, 31, ...$
Recurrence Matrix for Fermat number and Mersenne number

$$P_n = \begin{bmatrix} 1 & Q_{n+1} & Q_n \\ Q_{n+1} & 1 & Q_{n+2} \\ Q_n & Q_{n+2} & 1 \end{bmatrix}$$

where $n \geq 0$ and Q_n's are taken from Fermat sequence when the input is 0 and Mersenne sequence when the input is 1.

5. Algorithm for encryption and decryption

5.1. Encryption Algorithm.

(1) Suppose we have a plain text P in the form of sentence.
(2) Divide the plain text into n numbers of texts and construct a square matrix.
(3) Define a Moore machine through public channel.
(4) Define input.
(5) Get output through Moore machine.
(6) Now define recurrence matrix and choose recurrence relation.

(7) Define the value of n in a recurrence matrix.
(8) Get the cipher text at each stage for all the plain text.
(9) Send the cipher text to the receiver.

5.2. **Decryption Algorithm.** On getting the finite state machine, cipher text and recurrence matrix decode the plaintext either by using multiplicative or additive inverse else we can use inverse operation of the recurrence relation or matrix, to get the plain text or unique information. For a finite state machine with n states, we require n multiplicative or additive inverse.

6. Implementation of an algorithm

Let the plain text be P = FROGS ARE DANCING.

6.1. **Encryption Process.** Now let us encrypt this plain text **P = FROGS ARE DANCING.**

(1) P = FROGS ARE DANCING.
(2) According to algorithm we construct the matrix of size $3 * 3$ and assign the values according to letter.

$$M = \begin{bmatrix} F & R & O \\ G & S & \\ A & R & E \end{bmatrix} = \begin{bmatrix} 6 & 18 & 15 \\ 7 & 19 & 0 \\ 1 & 18 & 5 \end{bmatrix}$$

$$N = \begin{bmatrix} - & D & A \\ N & C & I \\ N & G & . \end{bmatrix} = \begin{bmatrix} 0 & 4 & 1 \\ 14 & 3 & 9 \\ 14 & 7 & 27 \end{bmatrix}$$

(3) Moore machine is generalized through public channel.
(4) Now we add all the element of both the matrix and convert it into an appropriate binary form. This binary form is taken as input in Moore machine. The sum of elements of Matrix

$$M = 6 + 18 + 15 + 7 + 19 + 1 + 0 + 18 + 5 = 89$$

$$N = 0 + 4 + 1 + 14 + 3 + 9 + 14 + 7 + 27 = 79$$

Binary form of Matrix

$$M = 89 = (1011001)_2$$

$$N = 79 = (1001111)_2$$

(5) The output of the above key is found by Moore machine shown in Fig 1 and Fig 2:
(6) The Recurrence matrix for computing cipher text is defined by recurrence relation

$$P_n = \begin{bmatrix} 1 & Q_{n+1} & Q_n \\ Q_{n+1} & 1 & Q_{n+2} \\ Q_n & Q_{n+2} & 1 \end{bmatrix}$$

We use recurrence relation with the power of 2 plus or minus 1 to increase the secrecy level or make the cipher text complicated so it is hard to break the key.

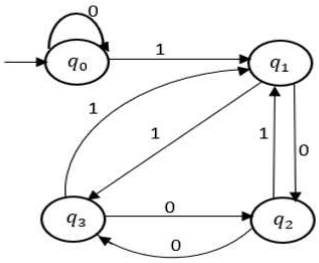

Fig 1: Moore Machine to calculate output for M

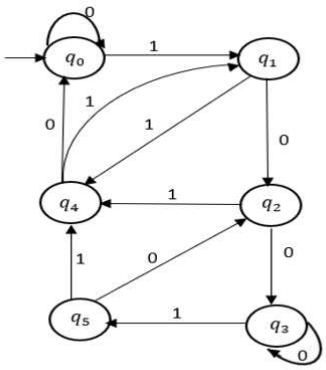

Fig 2: Moore Machine to calculate output for N

(7) Suppose Q_{i+1} is the cipher text at $(i+1)$ level and given as

$$Q_{i+1} = Q_i + P_n$$

Here we do matrix addition and P_n is totally dependent on the input.

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

(8) Now we compute cipher text at each level.
Then the cipher text for matrix M is as follows in Table 1:

S. N.	In put	Out put	Key	Cipher text
1	1	1	$\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}$	$\begin{bmatrix}6&18&15\\7&19&0\\1&18&5\end{bmatrix}+\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}=\begin{bmatrix}7&21&16\\10&20&7\\2&25&6\end{bmatrix}$
2	0	2	$\begin{bmatrix}1&9&5\\9&1&17\\5&17&1\end{bmatrix}$	$\begin{bmatrix}7&21&16\\10&20&7\\2&25&6\end{bmatrix}+\begin{bmatrix}1&9&5\\9&1&17\\5&17&1\end{bmatrix}=\begin{bmatrix}8&30&21\\19&21&24\\7&42&7\end{bmatrix}$
3	1	1	$\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}$	$\begin{bmatrix}8&30&21\\19&21&24\\7&42&7\end{bmatrix}+\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}=\begin{bmatrix}9&33&22\\22&22&31\\8&49&8\end{bmatrix}$
4	1	3	$\begin{bmatrix}1&15&7\\15&1&31\\7&31&1\end{bmatrix}$	$\begin{bmatrix}9&33&22\\22&22&31\\8&49&8\end{bmatrix}+\begin{bmatrix}1&15&7\\15&1&31\\7&31&1\end{bmatrix}=\begin{bmatrix}10&48&29\\37&23&62\\15&80&9\end{bmatrix}$
5	0	2	$\begin{bmatrix}1&9&5\\9&1&17\\5&17&1\end{bmatrix}$	$\begin{bmatrix}10&48&29\\37&23&62\\15&80&9\end{bmatrix}+\begin{bmatrix}1&9&5\\9&1&17\\5&17&1\end{bmatrix}=\begin{bmatrix}11&57&34\\46&24&79\\20&97&10\end{bmatrix}$
6	0	3	$\begin{bmatrix}1&17&9\\17&1&33\\9&33&1\end{bmatrix}$	$\begin{bmatrix}11&57&34\\46&24&79\\20&97&10\end{bmatrix}+\begin{bmatrix}1&17&9\\17&1&33\\9&33&1\end{bmatrix}=\begin{bmatrix}12&74&43\\63&25&112\\29&130&11\end{bmatrix}$
7	1	1	$\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}$	$\begin{bmatrix}12&74&43\\63&25&112\\29&130&11\end{bmatrix}+\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}=\begin{bmatrix}13&77&44\\66&26&119\\30&137&12\end{bmatrix}$

TABLE 1. **Cipher text for Matrix M**

The cipher text for matrix N is as follows in Table 2:

(9) Send cipher text $\begin{bmatrix}13&77&44\\66&26&119\\30&137&12\end{bmatrix}$ to receiver A.

And cipher text $\begin{bmatrix}7&161&78\\171&10&326\\91&324&36\end{bmatrix}$ to receiver B.

6.2. **Decryption Process: Decryption process for matrix M and N**

For decryption process we need to add the cipher text with the inverse of the recurrence matrix used. So, on getting the finite state machine and recurrence matrix (which is our secret key) we can decode the cipher text. For a finite state machine with n states, we require an additive inverse matrix. So,

Decryption at $q_i{}^{th}$ **state = Cipher text** $+{P_n}^{-1}$.

7. PERFORMANCE ANALYSIS

(i) **Mathematical work :** In proposed algorithm, we have used multiplication and addition of two matrices. Here, at each stage based on input and output the recurrence

S. N.	In put	Out put	Key	Cipher text
1	1	1	$\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}$	$\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}+\begin{bmatrix}0&4&1\\14&3&9\\14&7&27\end{bmatrix}=\begin{bmatrix}1&7&2\\17&4&16\\15&14&28\end{bmatrix}$
2	0	2	$\begin{bmatrix}1&9&5\\9&1&17\\5&17&1\end{bmatrix}$	$\begin{bmatrix}1&7&2\\17&4&16\\15&14&28\end{bmatrix}+\begin{bmatrix}1&9&5\\9&1&17\\5&17&1\end{bmatrix}=\begin{bmatrix}2&16&7\\26&5&33\\20&31&29\end{bmatrix}$
3	0	3	$\begin{bmatrix}1&17&9\\17&1&33\\9&33&1\end{bmatrix}$	$\begin{bmatrix}2&16&7\\26&5&33\\20&31&29\end{bmatrix}+\begin{bmatrix}1&17&9\\17&1&33\\9&33&1\end{bmatrix}=\begin{bmatrix}3&33&16\\43&6&66\\29&64&30\end{bmatrix}$
4	1	5	$\begin{bmatrix}1&63&31\\63&1&127\\31&127&1\end{bmatrix}$	$\begin{bmatrix}3&33&16\\43&6&66\\29&64&30\end{bmatrix}+\begin{bmatrix}1&63&31\\63&1&127\\31&127&1\end{bmatrix}=\begin{bmatrix}4&96&47\\106&7&193\\60&191&31\end{bmatrix}$
5	1	4	$\begin{bmatrix}1&31&15\\31&1&63\\15&63&1\end{bmatrix}$	$\begin{bmatrix}4&96&47\\106&7&193\\60&191&31\end{bmatrix}+\begin{bmatrix}1&31&15\\31&1&63\\15&63&1\end{bmatrix}=\begin{bmatrix}5&127&62\\137&8&256\\75&254&34\end{bmatrix}$
6	1	1	$\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}$	$\begin{bmatrix}5&127&62\\137&8&256\\75&254&34\end{bmatrix}+\begin{bmatrix}1&3&1\\3&1&7\\1&7&1\end{bmatrix}=\begin{bmatrix}6&130&63\\140&9&263\\76&261&35\end{bmatrix}$
7	1	4	$\begin{bmatrix}1&31&15\\31&1&63\\15&63&1\end{bmatrix}$	$\begin{bmatrix}6&130&63\\140&9&263\\76&261&35\end{bmatrix}+\begin{bmatrix}1&31&15\\31&1&63\\15&63&1\end{bmatrix}=\begin{bmatrix}7&161&78\\171&10&326\\91&324&36\end{bmatrix}$

TABLE 2. **Cipher text for Matrix N**

matrix and their elements are different. Therefore, it is very difficult to decrypt the cipher text without having proper key or recurrence matrix and finite state machine.

(ii) **Key Reliability:** In proposed algorithm, even when the finite state machine is known or given it is not easy to break the key. The strength of the key depends upon its length.

(iii) **Rounds:** In proposed algorithm, number of rounds is totally dependent upon the key and finite state machine.

8. SECURITY ANALYSIS

Getting original text from the cipher text is challenging due to the selection of recurrence relation and chosen finite state machine. The advantage of the algorithm is that it is difficult to decipher the plain text due to increased size of the secret key. Also brute force attack on the key is difficult.

S.N	Name of the attack	Possibility of attack	Remarks
1	Cipher text attack	Very hard	Have least amount of information and different cipher text at different stages
2	Known plain text	Very hard	Due to multiple states in FSM and multiple recurrence matrix at each stage
3	Chosen Plain Text	Very hard	Due to operation perform on Matrix
4	Chosen Cipher Text	Very hard	Unable due to the selected FSM, Suitable key and recurrence matrix

TABLE 3. **Security Analysis over Attacks**

9. CONCLUSION

The Proposed algorithms are secure and efficient method for encrypting and decrypting information using matrices, finite state machines, and recurrence relations. This algorithms are based on different operations on matrices, chosen finite state machine and recurrence matrix. Here we have encrypted the plain text and decrypted the cipher text by using Moore machine and recurrence relations i.e. Fibonacci numbers, Fermat numbers and Mersenne numbers. To maintain the level of security, we have calculated different ciphers at each stage so that nobody can decrypt it without having suitable key if the algorithm is already known. Using the algorithms, 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 even if algorithm is known. If we increase the size of the matrix and number of rounds, more information can be sent securely at a time.
Overall, this algorithms can be a useful tool for ensuring the confidentiality of sensitive information in various fields such as finance, healthcare, and national security.

10. FUTURE WORK

The study of number sequences in cryptography is an active area of research, with ongoing work focused on exploring new techniques and applications. While Fibonacci and Mersenne numbers are among the most well-known integer sequences in cryptography, the Pell equation and Lucas numbers also possess unique properties and have their own interesting applications. As a result, future research will continue to discover the potential of these and other sequences in cryptography.

REFERENCES

[1] G. Agibalov, *State machines in cryptography*,Applied Discrete Mathematics, Appendix Mathematical methods of cryptography **2** (2009) 45-73.
[2] A. Brito, S. Soares, S. Villela, *Metaheuristics in the Project of Cellular Automata for Key Generation in Stream Cipher Algorithms*, Proceedings of the IEEE Congress on Evolutionary Computation (CEC), Rio de Janeiro, Brazil, (2018) 1-8.
[3] P. Dmsi, "A Novel Cryptosystem Based on Finite Automata Without Outputs," in M. Ito, Y. Kobayashi, K. Shoji and S. Kunitaka, eds. AFLAS 8, (2010) 23-32.

[4] J. P. A. Jyotirmie, S. Srilakshmi, A. Chandra Sekhar and S. Uma Devi, *Cryptographic Secret Sharing Scheme of Finite State Machines Using LU Decomposition*,International Journal of Mathematical Archive **4**, No. 3 (2013)209-214.
[5] P. A. Jyotirmie, A. Shekhar Chandra, S. Uma Devi, *Application of Mealy Machine and Recurrence Relations in Cryptography*,International Journal of Engineering Research and Technology **2** , No. 5 (2013) 1286-1290,.
[6] G. Khaleel, Sh. Turaev, I. Al-Shaikhli, M. Mohd Tamrin, *An overview of cryptosystems based on finite automata*, Proceedings of the Journal of Advanced Review on Scientific Research **27**, No. 1 (2016) 1-7.
[7] G. K. B. Krishna, A. Shekhar Chandra, S. Srilakshmi, *Cryptography Scheme For Digital Signals Using Finite State Machine*, International Journal of Computer Applications **29**, No. 6 (2011) 61-63.
[8] Kahate : *Cryptography And Network Security*, Tata McGraw Hill, 2003.
[9] S. Lakshmi: *On finite state machines and recursive functions applications to cryptosystems*, Ph.D. dissertation, Jawaharlal Nehru Technological University, India, 2012.
[10] P. Linz : *An Introduction to Formal Languages and Automata*, 4th ed., Narosa Publishing, 2009.
[11] W. Meier and O. Staffelbach, *Analysis of pseudo random sequences generated by cellular automata* , Workshop on the Theory and Application of of Cryptographic Techniques (1991) 186-199.
[12] K. L. P. Mishra and N. Chandrashekhran: *Theory of Computer Science*, 3rd ed., PHI Learning, 2014.
[13] Renji Tao, Shihua Chen, *On Finite automaton public-key cryptosystem*, Theoretical Computer Science **226**,(1999) 143172.
[14] S. Wolfram, *Cryptography with cellular automata*, Conference on the Theory and Application of Cryptographic Techniques, Springer Berlin Heidelberg (1985) 429-432.
[15] A. Sharipbay, Zh. Saukhanova, G. Shakhmetova, M. Saukhanova, *Ontology of finite-automaton cryptography* **31**, (2019) 36-49.
[16] B. Schneier and N. Ferguson: *Practical Cryptography* Wiley Publishing Inc., 2004.
[17] S. Srilakshmi, *New Encryption Scheme Using Laplace Transforms and Finite State Machine*, International Journal of Innovative Research in Science, Engineering and Technology **6**, special issue 13 (2017) 119-122.
[18] K. R. Sudha, A. Shekhar Chandra, and Prasad Reddy, *Cryptography Protection of Digital Signals Using Some Recurrence Relations*, International Journal of Computer Science and Network Security **7**, No. 5 (2007) 203-207.
[19] R. Tao and S. Chen, *A finite automaton public key cryptosystem and digital signatures*, Chinese Journal of Computers **8**, No. 6 (1985) 401- 409.
[20] R. Tao and S. Chen, *Two varieties of finite automaton public key cryptosystem and digital signatures*, Journal of computer science and technology **1**, No 1 (1986) 9-18.
[21] K. B. Vayadande, P. Sheth, A. Shelke, V. Patil, S. Shevate, and C. Sawakare, *Simulation and Testing of Deterministic Finite Automata Machine*, Int. J. Comput. Sci. Eng. **10**, No. 1 (2022) 13-17.