EasyChair Preprint

№ 7661

A Review Paper on Cryptography Using Automata Theory

Aadesh Kabra, Ketan Gangwal, Atharv Kinage and Kirti Agarwal

March 29, 2022

A Review paper on Cryptography using Automata Theory

Aadesh Kabra
Artificial Intelligence and Data Science
Vishwakarma Institute of Technology
Pune,411037, Maharashtra.
aadesh.kabra20@vit.edu

Ketan Gangwal
Artificial Intelligence and Data Science
Vishwakarma Institute of Technology
Pune,411037, Maharashtra.
ketan.gangwal20@vit.edu

Atharv Kinage
Artificial Intelligence and Data Science
Vishwakarma Institute of Technology
Pune,411037, Maharashtra.
atharv.kinage20@vit.edu

Kirti Agarwal
Artificial Intelligence and Data Science
Vishwakarma Institute of Technology
Pune,411037, Maharashtra.
kirti.agarwal20@vit.edu

***Abstract*— Cryptography's two most important aspects are encryption and decryption. The primary goal of both systems is to protect data. To convert ordinary text to ciphertext, we used encryption. In the opposite direction of encryption, decryption is the process of transforming encrypted text into plain text. The devised encryption solution assures data secrecy for secure communication by utilizing a finite state machine and the LU decomposition approach. We also use lower and upper triangular matrices, which are created by decomposing a square matrix, in our proposed method. The key will be a lower triangular matrix modulated by a prime number in the encryption process, and an upper triangular matrix modulated by a prime number in the decryption process. The strategy is advantageous.In industries where sensitive data must be supplied, such as banking and military services, this strategy is advantageous.**

Keywords— Encryption, Decryption, Finite Automata, Turing Machine and LU decomposition.

INTRODUCTION

Cryptography relies heavily on encryption and decryption. Both tactics are primarily used to protect data. To convert plain text to encrypted text, we use an encryption technique. In the opposite direction of encryption, decryption is the process of transforming encrypted text into plain text.[3] Someone who works with encryption and decoding is referred to as a "cryptographer." When a user possesses a certain piece of concealed knowledge, information is identified. A key is the hidden information that is transferred to the receiver. In cryptography, the encryption process is the process of safely converting data from one form to another. As a result, ciphertext is the value of encryption because it cannot be read by unauthorized individuals. Encryption protects data stored on a computer system or transmitted over the internet. The most critical part of any encryption is the encryption key. The two types of keys are public and private keys. In the encryption and decryption operations, both keys are used. Public keys are available to everyone, but private keys must be kept private.[23] The key size is proportional to the encryption strength. As a result, breaking encrypted data gets increasingly harder as the key size increases. Decryption is the process of transforming encrypted text into text that we or our computer can read and comprehend. Decryption is the manual process of decrypting data using the necessary codes or keys. Without the secret key, decoding data is exceedingly difficult. We'll get the original text after decoding. Automata theory has several applications in the field of cryptography. Deterministic finite automaton (DFA)is a field of Theory of Computation which is based on Automata. For every given string character input, a finite state machine creates a unique encoded string. The words "deterministic" and "uniqueness of computation" are synonymous.Non-deterministic finite automata allow for zero, one, or more transitions from one state to another on the similar input symbol.If S is a non-empty collection of

kjlstates, then the outcome is element of S for deterministic automata and a subset of S for non-deterministic automata. As a result, a finite state machine is a behavior algorithm with a limited count of states and transitions. Nowadays, this technique is widely used in cryptography to encode data and ensure data privacy.

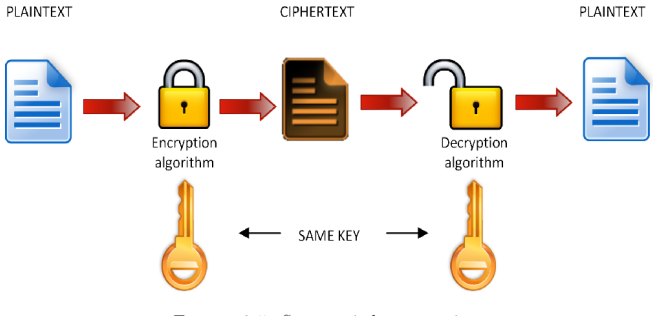
1. Vernam Cipher and secret key cryptography

Vernam Cipher is a cryptographic encryption algorithm. It is one of the Transposition methods used to convert plain strings to an encrypted string. In this strategy, we allot a number to each character in the normal-Text.

Method for obtaining a key:
In the Vernam cypher algorithm, we use a key to encrypt the strings, and the key's length should be the same as the string's length.

Algorithm for Encryption:

1. Assign a numerical value to each count in the string.
2. Add the two numbers together.
3. If the extra integer is larger than 26, deduct the integer from 26; else you are good to go.



2. Finite Automaton Public Key Cryptosystems:

Finite automata are the foundations of language-theoretic cryptosystems. The majority of cryptosystems built on language and word problems are either unsafe or do not meet digital signature prosperity requirements. Automata-based cryptosystems are divided into three categories: transducers, cellular automata, and acceptors. In this study, we explore the benefits and drawbacks of popular finite automata-based cryptosystems such as FAPKC, Gysin, Wolfram, Kari, Dmsi's cryptosystems[20].

Any cryptosystem must adhere to two fundamental principles: secrecy and authenticity. These two concepts provide a dilemma for the symmetric cryptosystem. The difficulty with confidentiality in symmetric cryptography is that, as we all know, a secret key is used to both convert and decode the communication. As a result, this key must be interchanged by both communication parties in some way, or they must depend on a third organization, such as a key allocation center, to allocate the key.[15]

However, depending on a third organization jeopardizes the secret key's confidentiality. In public key cryptography, each user must produce a pair of keys, one of which is kept hidden and is known as a private key, while the other is made public and is known as a public key. Now, whether the giver's private key or the receiver's public key is used to encipher the original message is entirely up to the application[20].

3. Cellular automata and cryptography

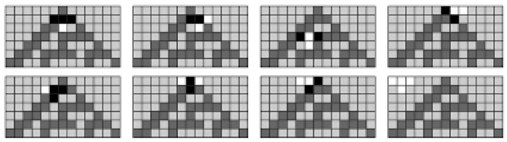
Cellular automata are dynamic with distinct attributes. This algorithm consists of a sequence of cells, and which are updated in sequential manner with random time. Cellular Automata is a distinct computing paradigm that gives an easy, extensible, and effective platform for revitalizing large systems and executing sophisticated computations based on evidence from the surroundings[12]. CA is made up of two parts. 1) a collection of cells and 2) a set of regulations. Control signals are used on a CA structure in PCA.

The primary goal of LCASE's (Lightweight Cellular Automata) design is to significantly improve both parties' necessities. The model, on the other hand, has several flaws to deal with traditional security concerns and different difficulties taken into account when developing the suggested algorithm are:

a. Fast performance with a low code density.

b. Impervious to attacks like traditional cryptanalysis as well as assault timing

c. Code-effective and simple implementation.



LITERATURE REVIEW

Sr No	Title	Authors	Year	Method	Advantages
1	Encryption and Decryption scheme involving Finite State Machine and LU Decomposition [1]	Ayush Mittal, Dr. Ravindra Kumar Gupta	2020	The paper suggests an approach on research to develop a novel cryptographic technique based on a the LU decomposition method and finite state machine[1]	Its security is enhanced mainly due to the factor that the matrix is broken into lower and upper triangular matrices. The system maintains four levels of security due to the finite state machine and the secret key.
2	Cryptographic Limitations on Learning Boolean Formulae and Finite Automata[2]	MICHAEL KEARNS, LESLIE VALIANT	1994	This paper shows how a constant depth threshold circuit, DFA, has significant cryptographic and number theory implications.[2]	It can decode RSA keys, factor Blum integers, and determine quadratic residues, among other things.
3	Application of finite automata in cryptography[3]	A.A.Sharipbay, Zh.S.Saukhanova, G.B.Shakhmetova, N.S.Saukhanov	2019	The main principles of asymmetric and symmetric cryptosystems are discussed in this paper. It also explains the technologies used in the finite automaton model system mainly in information encryption.[3]	The essay goes through several key symmetric and asymmetric concepts. In asymmetric cryptosystems, the technologies for implementing the finite automaton model in the field of information encryption are investigated.
4	On Linear Finite Automata and Cryptography[4]	Ivone Amorim, Ant´onio Machiavelo, Rog´erio Reis	2011	This paper studies Tao's formalisation and derives fundamental conclusions on the issue. It also proposes a different criterion for a specific type of automaton.[4]	The paper presents the advantages of Tao's formalisation with important conclusions on this issue. It also offers an innovative standard for a specific type of automaton consisting of weakly invertible delay.

5	Theory and Applications of Cellular Automata in Cryptography[5]	S. Nandi , B.K. Kar and P.Pal Chaudhari	1994	This thesis and use of Cellular Automata for a kind of block and stream ciphers are discussed in this study. Analytically, they demonstrated that cellular automata using XNOR rules may create an alternating group.[5]	The thesis and use of automata to a kind of block with steam ciphers are examined in this paper. They show that using XNOR principles, cellular automata may create an alternating group.
6	Encryption and Decryption Using Automata Theory[6]	Zubair Saqib, Murtza Ahmad Shahid and Muhammad Umair Ashraf	2015	Encryption and decryption are performed in this article utilizing computer theory methods. Encryption is performed using an encryptor created by a Turing machine, while decryption is performed using a decryptor.[6]	In this article, computer theory approaches are used to conduct encryption and decryption. Encryption is done with a Turing machine-created encryptor, while decryption is done with a decryptor.
7	Encryption and Decryption algorithm using two dimensional cellular automata rules in Cryptography[7]	Sambhu Prasad ,Umesh Prasad ,Madhusmita Sahu	2011	This study offers a novel block cipher encryption and decryption procedure based on the principles of nonlinear and linear cellular automata.[7]	Based on nonlinear and linear (periodic boundary-PB) cellular automata rules, this paper proposes a novel block cipher encryption and decryption technique.
8	Cryptography Using Cellular Automata[8]	Harsh Bhasin, Ramesh Kumar, Neha Kathuria	2013	This study describes an encryption technique used on Cellular Automata. This method is tested, with preliminary findings showing that it can compete with AES.[8]	The created application can create cellular automata patterns with a variety of rules and store them in text format. The method looks to be sound enough to compete with other approaches.

9	A Symmetric Cryptography based on Extended cellular automata[9]	Zhao Xuelong , Li Qianmu , Xu Manwu and Liu Fengyu	2003	They created a producer to produce numbers arbitrarily using a unidimensional type of extended automata.[9]	To produce good arbitrarily numbers, a unidimensional that extends irregular CA is utilized. The extended CA producer presented in this paper surpasses typical producers according to the results. Producers include the following: Producer, Congruential Producer, and Lagged Fibonacci Producer. This producer can fulfill protection criteria for cryptography while also offering unique techniques to create arbitrary integers.
10	Graphic Cryptography with Pseudorandom Bit Generators and Cellular Automata[10]	Gonzalo Alvarez Maran ´on, Luis Hern ´andez Encinas, Ascenso ´on Hern ´andez Encinas,	2003	We provide a novel graphic symmetrical encryption strategy for encrypting a coloured image given by pixels. This system is made on an amendable bidimensional automaton and includes a pseudo random producer.[10]	We describe a novel visual symmetrical encryption approach for encrypting a coloured image with any number of colors given by pixels in this work.
11	An Analytical Study of Cellular Automata and its Applications in Cryptography [11]	G. Kumaresan, N.P. Gopalan	2017	Using numerous examples, this paper examines the fundamental ideas of several functions of automata which discusses their uses in this field.[11]	This paper addresses the main principles of various types used in cellular automata and illustrates their uses in the field of cryptography through several use cases.
12	Evolving Behavior of Cellular Automata for Cryptography [12]	Miroslaw Szaban , Franciszek Seredynski and Pascal Bouvry.	2006	In this research they have researched about one dimensional cellular automata and used a genetic model to see protocols of cellular automata cells resulting in sequences matching for symmetric key cryptography.[12]	The researchers investigated one-dimensional cellular automata and used a GA to identify subsets-based rules that govern cellular automata cells, yielding high-quality output for cryptography.

CONCLUSION

In this survey paper, we have reviewed twelve different research papers on the topic 'Cryptography using Automata Theory'. After reviewing these research papers we got to know that most of the research papers used cellular automata for cryptography but by using finite automata the results were significant. For image encryption cellular automata give the best results. Currently there is no system which gives both image and text encryption and decryption.In some of the papers, the authors had developed encryption techniques which could compete with AES. Thus, to conclude, we have thoroughly studied and reviewed different research papers.

References

[1] Encryption and Decryption scheme involving Finite State Machine and LU Decomposition by Ayush Mittal, Dr. Ravindra Kumar Gupta

[2] Cryptographic Limitations on Learning Boolean Formulae and Finite Automata by Michael Kearns, Leslie Valiant

[3] Application of finite automata in cryptography by A.A.Sharipbay, Zh.S.Saukhanova, G.B.Shakhmetova,N.S.Saukhanov

[4] On Linear Finite Automata and Cryptography by Ivone Amorim, Ant´onio Machiavelo, Rog´erio Reis

[5] Encryption and Decryption Using Automata Theory by Zubair Saqib, Murtza Ahmad Shahid and Muhammad Umair Ashraf

[6] Encryption and Decryption algorithm using two dimensional by Zubair Saqib, Murtza Ahmad Shahid and Muhammad Umair Ashraf

[7] Cellular automata rules in Cryptography by Sambhu Prasad , Umesh Prasad , Madhusmita Sahu

[8] Cryptography Using Cellular Automata byHarsh Bhasin, Ramesh Kumar, Neha Kathuria

[9] Harsh Bhasin, Ramesh Kumar, Neha Kathuri A Symmetric Cryptography based on Extended cellular automata by Zhao Xuelong, Li Qianmu, Xu Manwu and Liu Fengyu

[10] Graphic Cryptography with Pseudorandom Bit Generators and Cellular Automata Gonzalo Alvarez Mara on, Luis Hern´andez Encinas,Ascensi´on Hern´andez Encinas, Angel Mart´´ ın del Rey, and Gerardo Rodr´ıguez S´anchez

[11] An Analytical Study of Cellular Automata and its applications in Cryptography by G. Kumaresan, N.P. Gopalan

[12] Evolving Collective Behavior of Cellular Automata for Cryptography by Miroslaw Szaban, Franciszek Seredynski and Pascal Bouvry.

[13] Vayadande, Kuldeep, Ritesh Pokarne, Mahalaxmi Phaldesai, Tanushri Bhuruk, Tanmai Patil, and Prachi Kumar. "SIMULATION OF CONWAY'S GAME OF LIFE USING CELLULAR AUTOMATA." International Research Journal of Engineering and Technology (IRJET) 9, no. 01 (2022): 2395-0056.

[14] Vayadande, Kuldeep, Ram Mandhana, Kaustubh Paralkar, Dhananjay Pawal, Siddhant Deshpande, and Vishal Sonkusale. "Pattern Matching in File System." International Journal of Computer Applications 975: 8887.

[15] Vayadande, Kuldeep, Neha Bhavar, Sayee Chauhan, Sushrut Kulkarni, Abhijit Thorat, and Yash Annapure. Spell Checker Model for String Comparison in Automata. No. 7375. EasyChair, 2022.

[16] VAYADANDE, KULDEEP. "Simulating Derivations of Context-Free Grammar." (2022).

[17] Vayadande, Kuldeep, Neha Bhavar, Sayee Chauhan, Sushrut Kulkarni, Abhijit Thorat, and Yash Annapure. Spell Checker Model for String Comparison in Automata. No. 7375. EasyChair, 2022.

[18] Varad Ingale, Kuldeep Vayadande, Vivek Verma, Abhishek Yeole, Sahil Zawar, Zoya Jamadar. Lexical analyzer using DFA, International Journal of Advance Research, Ideas and Innovations in Technology

[19] Kuldeep Vayadande, Harshwardhan More,Omkar More, Shubham Muley,Atahrv Pathak, Vishwam Talanikar, "Pac Man: Game Development using PDA and OOP", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, p-ISSN: 2395-0072, Volume: 09 Issue: 01 | Jan 2022

[20] Kuldeep B. Vayadande, Parth Sheth, Arvind Shelke, Vaishnavi Patil, Srushti Shevate, Chinmayee Sawakare, "Simulation and Testing

of Deterministic Finite Automata Machine," International Journal of Computer Sciences and Engineering, Vol.10, Issue.1, pp.13-17, 2022.

[21] Rohit Gurav, Sakshi Suryawanshi,Parth Narkhede,Sankalp Patil,Sejal Hukare,Kuldeep Vayadande," Universal Turing machine simulator", International Journal of Advance Research, Ideas and Innovations in Technology, ISSN: 2454-132X, (Volume 8, Issue 1 - V8I1-1268

[22] Kuldeep Vayadande, Krisha Patel, Nikita Punde, Shreyash Patil, Srushti Nikam, Sudhanshu Pathrabe, "Non-Deterministic Finite Automata to Deterministic Finite Automata Conversion by Subset Construction Method using Python," International Journal of Computer Sciences and Engineering, Vol.10, Issue.1, pp.1-5, 2022.

[23] Kuldeep Vayadande and Samruddhi Pate and Naman Agarwal and Dnyaneshwari Navale and Akhilesh Nawale and Piyush Parakh," Modulo Calculator Using Tkinter Library", EasyChair Preprint no. 7578, EasyChair, 2022.