RESEARCH ARTICLE OPEN ACCESS

A Comprehensive Study of Substitution and Transposition Techniques in Cryptographic Systems

Binita Thakkar
Information Technology, VIVA College of Arts, Commerce and Science, Virar (W)

ABSTRACT
This paper explores classical encryption techniques used for secure communication, focusing on substitution and transposition methods. The study covers Caesar cipher, Modified Caesar cipher, Monoalphabetic cipher, Vigenere cipher, Rail Fence cipher, Simple columnar transposition, Multi-columnar transposition, and Vernam cipher. The paper highlights their working mechanisms, strengths, weaknesses, and relevance in modern cryptography. Additionally, a comparative analysis of these techniques is presented to assess their cryptographic security and practicality. A Java-based implementation was done for each encryption technique, followed by a performance analysis in terms of time complexity and memory usage. The findings highlight the efficiency and security implications of these classical techniques in modern cryptographic systems.

Keywords — substitution techniques, transposition techniques, efficiency

I. INTRODUCTION

In the digital age, the significance of information security has grown exponentially as individuals, organizations, and governments strive to protect sensitive data and maintain privacy. Information security encompasses the practices, technologies, and strategies designed to safeguard information from unauthorized access, misuse, disclosure, disruption, or destruction. It ensures confidentiality, integrity, and availability of information, often referred to as the CIA triad. As data becomes the cornerstone of global operations, robust security measures are indispensable to prevent cyber threats, data breaches, and malicious attacks.

Cryptography, a cornerstone of information security, plays a pivotal role in protecting data. It involves the art and science of converting plain, readable information into an encrypted format, ensuring that only authorized parties can access the original data. The field of cryptography traces back to ancient civilizations, where methods such as substitution ciphers were employed for secure communication. Today, it has evolved into an advanced discipline relying on complex mathematical algorithms and computational techniques.

The process of securing information through encryption is called cryptography [1]. The role of encryption in information security is protecting confidentiality and integrity of data. To do so, various classical cryptography techniques are still used. Two of the classical cryptography techniques are: substitution ciphers and transposition ciphers [2]. Substitution cipher replace characters in plaintext to another character. Transposition ciphers rearrange plaintext characters without changing them.

The research objective of this paper to review the classical cryptographic techniques and implement the same in Java. This implementation strategy will identify the total time required for encryption/decryption process and total memory utilized in every technique. Further, a comparative analysis for the same will be done to provide detail of the work done.

II. LITERATURE REVIEW

B. Thakkar and B. Thankachan [3] made a study of various cryptographic algorithms and comparative analysis of the study concluded that Blowfish is the best suitable algorithm.

V. Veerasingam and N. Harun [4] made a study of Caesar cipher columnar transposition cipher and row transposition cipher in tamil language. Their study identified that Caesar cipher was less secure.

D . Kang and J. Lee [5] made a study of frequency analysis on monoalphabetic ciphers. They proposed a new index selection algorithm using dictionary-based technique to overcome decryption process using frequency analysis.

B. Thakkar and B. Thankachan [6] made a study of various substitution and transposition ciphers and developed a multitransposition technique using rail fence followed by simple columnar technique.

A. Verma and A. Gakhar [7] made a systematic study of various ciphers like Shift cipher , Hill cipher, Polyalphabetic cipher, and various algorithms like DES, AES and RSA. They made the detailed study through the pseudocode and various analysis tools.

B. Kumar et.al [8] proposed a three layer encryption technique using substitution cipher and involution function for securing e-commerce sites. Combing two approaches they made an hybrid outcome.

B. Thakkar and B. Thankachan [9] made a study of various cryptographic algorithms and proposed a new algorithm where plain text data was first passed to multitransposition technique, followed by DES then Blowfish. They made the study on various file size, and identified the encryption time, decryption time and memory usage of the same.

B. Thakkar and B. Thankachan [10] made a study of various deduplication techniques. They proposed an algorithm using message digest 5 to check deduplication of files on cloud. If the file with same hash value was already present on cloud, file uploading was rejected. If the hash value of file was not present on cloud, file uploading was allowed.

J. Mohammad et al. [11] conducted a study analysing cryptographic algorithms with respect to key size, performance, and output size. The study concluded that symmetric algorithms are both faster and more efficient. Among these, AES emerged as the most efficient algorithm, followed by DES, 3DES, RC4, and Blowfish.

T. Ramaporkalai [12] examined the effectiveness of different security algorithms in the context of cloud computing, such as DES, AES, 3DES, Blowfish, IDEA, Homomorphic encryption, RSA, and D-H. The study emphasized the need for a more efficient cryptographic algorithm to enhance data security in the cloud environment.

In [13] various kinds of classical ciphers studies were made such as Affine cipher and one-time pads.

III. SUBSTITUTION TECHNIQUES

Substitution techniques is a way in which a character of a plain text message is replaced by any other character, number or symbol [14]. There are various substitution techniques as shown below:

A. Caesar Cipher

This is the simplest form of substitution cipher. In this technique, every plain text alphabet is replaced with another alphabet that is three places down the line. That is, for encryption process, A is replaced with D, B is replaced with E, C is replaced with F so on X will be replaced with A, Y will be replaced with B and Z will be replaced with C. The decryption process will just be the reverse. Fig 1, shows example of plaintext replaced with character three places down the line.

Plain text	S	T	U	D	E	N	T
Cipher text	V	W	X	G	H	Q	W

Fig 1. Caesar cipher example

B. Modified Caesar Cipher

In this technique, every plain text alphabet is replaced with another alphabet that is any places down the line. That is, for encryption process, A can be replaced with B or G or X or any other character. This replacement scheme once decided will be constant for other alphabets in the plaintext. Fig 2, shows example of plaintext replaced with the character 7 places down the line.

Plain text	C	O	M	P	U	T	E	R
Cipher text	J	V	T	W	B	A	L	Y

Fig 2. Modified Caesar cipher example

C. Monoalphabetic Cipher

In this technique, given a plaintext message, each A can be replaced with any alphabet from B through Z, B is replaced with A or any alphabet from C through Z and so on. There is no such fixed replacement scheme. Fig 3, shows example of plaintext replaced with character any places down the line.

Plain text	H	A	R	D	W	A	R	E
Cipher text	Z	F	Y	M	G	F	Y	Q

Fig 3. Monoalphabetic cipher example

D. Vigenere Cipher

In this cipher, multiple one-character key is used. Each key encrypts one plaintext character at a time. This key is called as a period. It can be of any size. Fig 4, shows an example of Vigenere cipher where key used was 'CIPHER' and applied on plain text 'SOFTWARE' to produce the corresponding ciphertext.

Plain text	S	O	F	T	W	A	R	E
Cipher text	U	W	U	A	A	R	T	M

Fig 4. Vigenere cipher example

IV. TRANSPOSITION TECHNIQUES

Transposition techniques is a way in which characters of plain text message are not only replaced with another characters but also some kind of permutation and combination is applied [14]. There are various transposition techniques as shown below:

A. Rail Fence Cipher

This technique uses a simple algorithm [15] where plaintext message is written in zig-zag manner and read later row wise to generate cipher text. Consider the example, comehometomorrow and write in zig-zag manner as shown in Fig 5. Read row-wise to generate the cipher text cmhmtmrooeoeoorw.

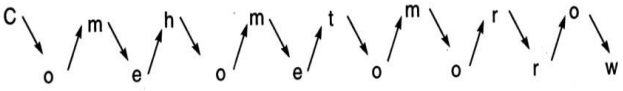

Fig 5. Rail Fence Cipher example

B. Simple Columnar Cipher

In this technique, a grid of predefined size is taken and every plain text alphabet is filled in the grid. Later, it is read column wise randomly to generate cipher text. Fig 6, shows a grid of 4x3 and plain text as 'AATACKATDAWN' filled in the grid row-wise. To generate the cipher text, read the data column-wise randomly. Here we choose the order 2,4,3,1. So the cipher text obtained will be 'TKAATNTAWACD'.

A	T	T	A
C	K	A	T
D	A	W	N

Fig 6. Simple Columnar Cipher example

C. Multi Columnar Cipher

This technique is same as the simple columnar technique. The only difference is that the process can be done twice or more than that. For this, we take the example of simple columnar technique. The cipher text generated in above example 'TKAATNTAWACD' is used as plaintext and filled in the grid row-wise for round 2 as shown in Fig 7.

T	K	A	A
T	N	T	A
W	A	C	D

Fig 7. Multi Columnar Cipher example

To generate the cipher text, read the data column-wise randomly. Here we choose the order again as 2,4,3,1. So the cipher text obtained will be 'KNAAADATCTTW'. This can be continued for any more number of rounds.

D. Vernam Cipher

This method involves using a one-time pad with the plain text, ensuring that the pad's letters are unique and not repeated. The plain text message and the one-time pad must be of equal length. In this approach, each letter in the plain text and the one-time pad is converted into a numerical value based on its position in the alphabet (A = 0, B = 1, .. , Z = 25). The corresponding numbers from the plain text and the pad are then added together. If the resulting sum exceeds 25, subtract 26 from it. Finally, the resulting numbers are converted back into letters to form the cipher text.

Plain text	A	L	L	T	H	E	B	E	S	T
	0	11	11	19	7	4	1	4	18	19
ADD										
One-time pad	13	2	1	19	25	16	0	17	23	15
	N	C	B	T	Z	Q	A	R	X	P
Initial total	13	13	12	38	32	20	1	21	41	34
Subtract 26, if >25	13	13	12	12	6	20	1	21	15	8
Cipher text	N	N	M	M	G	U	B	V	P	I

Fig 8. Vernam Cipher example

V. IMPLEMENTATION

All the above techniques are implemented in Java to observe the execution. During implementation of the techniques, total encryption/decryption time i.e. execution time was calculated in milliseconds. Also, memory utilized during execution was calculated in bytes. Table I shows the overall execution time in msec and memory used in bytes of various substitution and transposition techniques.

TABLE I
EXECUTION TIME AND MEMORY UTILIZATION OF VARIOUS CIPHERS

Techniques	Execution Time (msec)	Memory Used (bytes)
Substitution Ciphers		
Caesar Cipher	1348	317592
Modified Caesar Cipher	2176	317656
Monoalphabetic Cipher	1188	320936
Vigenere Cipher	2	291128
Transposition Ciphers		
Rail Fence Cipher	2779	317384
Simple Columnar Cipher	1566	436784
Multi Columnar Cipher	3132	436168
Vernam Cipher	3652	436328

VI. COMPARATIVE AND PERFORMANCE ANALYSIS

Table II shows the comparative analysis of various classical ciphers in terms of memory usage, strength and weakness.

TABLE III
COMPARATIVE ANALYSIS OF VARIOUS CIPHERS

Techniques	Memory Usage	Strength	Weakness
Substitution Ciphers			
Caesar Cipher	Low	Simple	Easily broken
Modified Caesar Cipher	Low	Hard to crack	Cracked in minimum possibilities
Monoalphabetic Cipher	High	Strong	Susceptible to frequency analysis
Vigenere Cipher	Medium	Stronger than mono-alphabetic	Kasiski test attack
Transposition Ciphers			
Rail Fence Cipher	Low	Simple	Pattern recognition attack
Simple Columnar Cipher	Moderate	Harder than rail fence	Key management

Multi Columnar Cipher	High	Strong	High processing time
Vernam Cipher	Very high	Strongest	Used only for small communi-cations

Based upon the implementation of various classical cipher, analysis of total execution time is shown in Fig 9 and memory utilization is shown in Fig. 10.

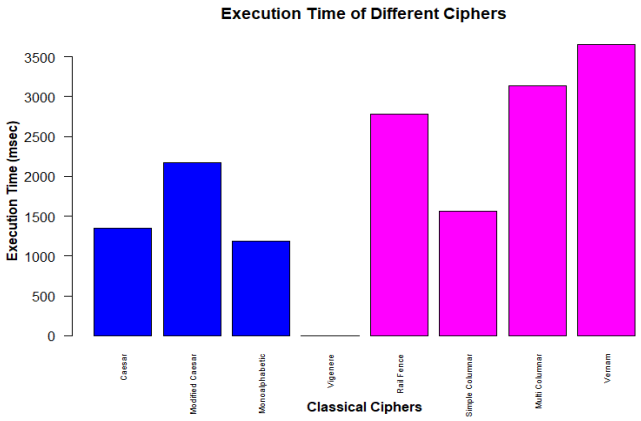

Fig 9. Execution time of classical ciphers

Fig 9 easily shows that, the execution time required for transposition cipher is much more than that of the substitution ciphers.

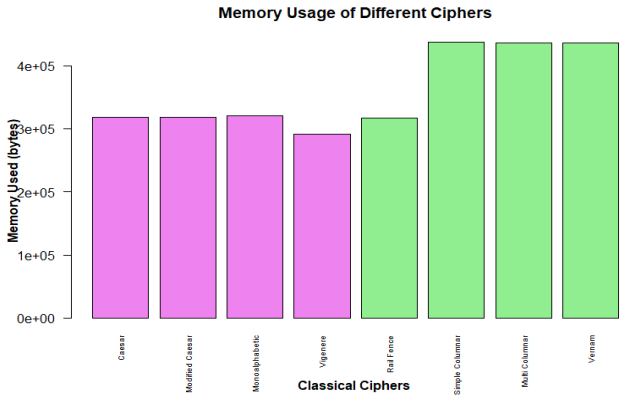

Fig 10. Memory utilization of classical ciphers

Fig 10 easily shows that, the memory usage required for transposition cipher is much more than that of the substitution ciphers.

VII. CONCLUSION

This paper describes the study of various substitution ciphers and transposition ciphers. The study revealed actual working of the ciphers with their strength and weaknesses. The implementation of ciphers showed the actual time required for execution and total memory utilized in the process. This may vary depending upon what input value is passed during execution. The overall performance analysis of the work was done and it was easy to identify that the execution time and memory usage for transposition ciphers is more than the substitution ciphers. Simple techniques are vulnerable, but modifications improve resistance. Though classical ciphers are insecure alone, they influence modern cryptographic algorithms. In future, enhancing classical encryption with computational complexity and hybrid models would make improvised change.

REFERENCES

[1] S. Rajeswari, R. A. Zahra, and R. Kalaiselvi, “A Survey on the Different Cryptographic Techniques used for Data Access Control in Cloud Computing,” Int. J. Curr. Eng. Sci. Res., vol. 5, no. 4, pp. 49–53, 2018.

[2] R. Sharma, R. Sharma, and H. Singh, “Classical Encryption Techniques,” Int. J. Comput. Technol., vol. 3, no. 1, pp. 84–90, 2012, doi: 10.24297/ijct.v3i1b.2745.

[3] B. Thakkar and B. Thankachan, “A Survey for Comparative Analysis of various Cryptographic Algorithms used to Secure Data on Cloud,” Int. J. Eng. Res. Technol., vol. V9, no. 08, pp. 753–756, 2020, doi: 10.17577/ijertv9is080328.

[4] V. K. Veerasingam, N. Ziadah Harun, and F. Sains Komputer dan Teknologi Maklumat, “A Security Level Comparison of Caesar Cipher, Columnar Transposition Cipher and Row Transposition Cipher in Tamil Messages,” Appl. Inf. Technol. Comput. Sci., vol. 4, no. 1, pp. 92–108, 2023, [Online]. Available: https://doi.org/10.30880/aitcs.2023.04.01.006.

[5] D. Kang and J. Lee, “A Robust Decryption Technique Using Letter Frequency Analysis for Short Monoalphabetic Substitution Ciphers,” J. Comput. Sci. Eng., vol. 18, no. 3, pp. 144–151, 2024, doi: 10.5626/JCSE.2024.18.3.144.

[6] B. Thakkar and B. Thankachan, “A Multilevel Approach of Transposition Ciphers for Data Security over Cloud,” GIS Sci. J., vol. 8, no. 5, pp. 1732–1738, 2021.

[7] P. A. Verma and A. Gakhar, “Analysis of Tools and Techniques in cryptography,” FP-International J. Comput. Sci. Res., vol. 2, no. 1, pp. 37–44, 2015.

[8] B. Kumar, S. Roy, A. Sinha, and V. Kumar, “Invo-Substitute: Three Layer Encryption For Enhanced E-Commerce Website Security Using Substitution Cipher And Involution Function,” J. Pharm. Negat. Results, no. January, pp. 1621–1640, 2023, doi: 10.47750/pnr.2023.14.S02.198.

[9] B. Thakkar and B. Thankachan, “An Approach for Enhancing Security of Data over Cloud Using Multilevel Algorithm,” in Congress on Intelligent Systems, Lecture Notes on Data Engineering and

Communications Technologies, 2022, vol. 114, pp. 305–318, doi: https://doi.org/10.1007/978-981-16-9416-5_22.

[10] B. Thakkar and B. Thankachan, "A Data Deduplication Approach for Eliminating Duplicate File Upload over Cloud," Int. J. Enhanc. Res. Sci. Technol. Eng., vol. 11, no. 2, pp. 13–17, 2022.

[11] O. K. J. Mohammad, S. Abbas, E.-S. M. EI-Horbaty, and A.-B. M. Salem, "A Comparative Study between Modern Encryption Algorithms based On Cloud Computing Environment," 8th Int. Conf. Internet Technol. Secur. Trans., pp. 531–535, 2013.

[12] T. Ramaporkalai, "Security Algorithms in Cloud Computing," Int. J. Comput. Sci. Trends Technol., vol. 5, no. 2, pp. 500–503, 2017, doi: 10.5120/ijca2017915827.

[13] S. Rubinstein-Salzedo, "Other Types of Ciphers," in Cryptography, Springer, 2018, pp. 63–73.

[14] A. Kahate, Cryptography And Network Security, 2nd editio. Tata-Mc-Graw Hill, 2008.

[15] A. Putera and U. Siahaan, "Rail Fence Cryptography in Securing Information," Int. J. Sci. Eng. Res., vol. 7, no. 7, pp. 535–538, 2016.