MODIFYING PLAYFAIR CIPHER WITH PADDING

Yash Patel[1]

[1]*Computer Engineering, Pimpri Chinchwad College of Engineering*

---***---

Abstract - There are billions and trillions of pieces of data being produced at any given time because to the internet. The majority of it is connected to the financial industry, the intelligence sector, or perhaps personal information about people and the country. Therefore, it is essential to safeguard and protect it. Data is encrypted using cryptography, which also secures its transmission over the internet. Different methods have developed over time to cypher the original text. The most used cryptographic algorithm is the Playfair algorithm. However, it is exploited by brute force. By altering the matrix and tricking the attackers into thinking it is a different cipher, the suggested approach enhances the performance of the conventional Playfair cypher.

Key Words: Security; Cryptography; Playfair; Base64; Cipher

1.INTRODUCTION

The process of transforming plain text into unintelligible text is known as cryptography. Since plain text may be read by anyone, it must be transformed into ciphertext using cryptography in order to be transmitted securely via a communication channel. The text that is difficult to understand is known as ciphertext. The words "Crypt" and "Graphy" stand for "writing style" and "hiding" respectively. Secure information communication methods formed from mathematical ideas and a set of guidelines known as algorithms are referred to as cryptography. The message is changed from being legible and understandable to being unreadable and difficult to grasp.

The two types of cryptography algorithms are symmetric and asymmetric. The Playfair cipher is a symmetric encryption technique that encrypts and decrypts data using the same key. Charles Wheatstone created it as the first useful digraph substitution cipher in 1854. Later, it was given the name Lord Playfair since he advocated the algorithm. This was the first method for encrypting and decrypting a pair of letters known as a "digraph."

The Playfair cipher encrypts and decrypts data using a matrix sometimes referred to as "key-Square." The standard key square measurement is 5*5. The plain text is broken up into digraphs, and each digraph is subsequently encrypted using predetermined criteria.

Rules for Encryption:

1. If both the characters in the digraph are in the same row: Replace each character with the letter to its immediate right.
2. If both the characters in the digraph are in the same column: Replace each character with the letter to its immediate below.
3. If both the characters in the digraph are in a different row and column: Form a rectangle with those two letters and consider horizontally opposite letters.

For the process of decryption, it uses the above conditions in exactly the opposite manner. The Playfair cipher is relatively difficult to decrypt however owing to the small size of the key square it can be decoded using brute force attack.

The proposed research work aims to improve the performance of the traditional Playfair cipher algorithm by constructing a key square of size 7*9 in contrast to the standard size of 5*5 and adding padding (“=”) at the end of the ciphertext to confuse attackers into thinking that it is a Base64 cipher.

Base64 is a group of related binary-to-text encoding techniques that output binary data as an ASCII string and convert it to a radix-64 representation. A specific MIME content transfer codec is known by the moniker Base64. Base64 algorithms are frequently utilized when binary data needs to be decoded before being saved or sent via ASCII-compatible media. By doing this, it will be ensured that the data is delivered in its original form.

The paper is structured as follows – Section 1 gave a brief introduction to the Cryptography and security algorithms used in the proposed research work. Section 2 summarizes the related survey work carried out. The proposed methodology is elaborated in Section 3 while the conclusion and future work is stated in Section 4 and Section 5 respectively.

2. LITERATURE REVIEW

Authors of [1] have proposed a method to improve the performance of the traditional Playfair cipher algorithm by constructing a key square of size 4*19 in contrast to the standard size of 5*5 and using the RSA algorithm along with the novel technique - RMPS keyless transposition to further enhance the security and confidentiality of the message.

The authors of [2] created a modified Playfair cipher technique by building a matrix of size 6*6 that contains 26 English alphabets and digits 0 through 9. The author takes into account four reserved keywords, using them to encrypt plain text four times and then decode it using the same reserved keywords.

The authors have suggested utilizing a 16x16 matrix, the Exclusive OR method, the two's complement, and the bit-swapping method to increase the key security of the Playfair encryption. Features of the suggested strategy have Strong avalanche effects [3] and increased security from brute-force assaults [4].

[5] uses CUDA programming to implement the traditional Playfair cipher in parallel. The authors have significantly sped up and reduced time complexity compared to the sequential version of the traditional Playfair cipher algorithm by using parallelization.

The combination of the Playfair cipher with the RSA approach has been utilized by the authors of [6] to exchange keys between sender and recipient in a very secure manner. The present Playfair cipher matrix has been modified in an effort to increase its size to 16*16. The proposed approach is made more secure by using the RSA algorithm to encrypt the key used in the Playfair cipher scheme. Future applications of this technique include reducing the RSA algorithm's decryption time.

The authors of [7] proposed a modified Playfair cipher with a matrix size of 5*19 in an effort to improve the performance of the present Playfair cipher method. Despite the method's use of 95 readable characters, counting the frequency of occurrence is still used in cryptanalysis, which has a number of drawbacks.

The traditional Playfair cypher algorithm can be improved in a number of different ways. One such technique is to make four matrices with a size of 4*4 each while raising the confusion rates to produce the 3D Playfair cypher. Instead of two pairs of two characters, this 3D Playfair cypher accepts a combination of three characters. By employing 4 matrices with a 128*128 size, the authors in [8] significantly altered the 3D Playfair cypher. The proposed solution in this situation has grown more resistant to Frequency analysis and brute force cryptanalysis techniques with such a large number of characters, i.e. 65536.

The suggested research study in [9] uses the Radix conversion mechanism, which encrypts and decrypts messages at the sender and recipient sides using 65 characters. A matrix of size 8*8 is utilized, which is initially filled with the specified keyword, and the original Playfair cypher procedure of a 5*5 matrix is upgraded.

3. PROPOSED METHOD

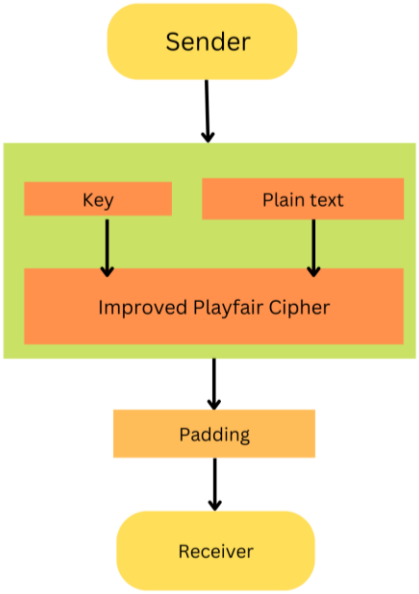

Fig. -1: Block Diagram of Proposed Method

The proposed methodology depicted in Fig. 1 follows the following process to encrypt the plain text message which is intended to be sent from sender to receiver.

Improved Playfair Cipher Algorithm The traditional Playfair cipher algorithm consisting of a matrix of size 5*5 is improved by constructing the matrix of size 7*9 consisting of all 63 characters- 26 small letters of English alphabets (a-z), 26 capital letters of English alphabets (A-Z), 10 digits (0-9) and 1 symbol (<^>) refer Fig. 2. Sender utilizes the ‘key’ to encrypt the plain text using the Improved Playfair cipher algorithm to generate the cipher text.

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	a	b
c	d	e	f	g	h	i
j	k	l	m	n	o	p
q	r	s	t	u	v	w
x	y	z	0	1	2	3
4	5	6	7	8	9	<space>

Table -1: 7*9 Key Matrix

Example:
Key: SECRET
Plain Text: Plan Ready

Encryption Steps:

[1] Generate Key Square

A	B	C	D	E	F	G
H	I	J	K	L	M	N
O	P	Q	R	S	T	U
V	W	X	Y	Z	a	b
c	d	e	f	g	h	i
j	k	l	m	n	o	p
q	r	s	t	u	v	w
x	y	z	0	1	2	3
4	5	6	7	8	9	<space>

2. In case of repetition of letters, separate them by x.
3. If the entire message length is odd then append <space> at the end to make the length even.
Here, Plan Ready→ length = 9 (Odd)
Plan Ready<space> = 10 (Even)
4. Generate digraphs.
Pl, an, Re, ad, y<space>
5. Substitute the letters in the digraph by following standard rules of replacement.

Digraph	Substituted Digraph
Pl	Qk
an	Zo
Re	Qf
ad	Wh
y<space>	35

6. After encryption:
QkZoQfWh35
7. Add padding as "=="
8. Final Cipher text:
QkZoQfWh35==

Decryption Steps:
1. Accept the cipher text.
QkZoQfWh35==
2. Ignore the padding:
QkZoQfWh35
3. Create the key square.
3. Generate digraphs Qk, Zo, Qf, Wh, 35
4. Digraph substitution

Digraph	Substituted Digraph
Qk	Pl
Zo	an
Qf	Re
Wh	ad
35	y<space>

5. Retrieve the original text
Pl,an,Re,ad,y<space>
Plan Ready

4. CRYPTANALYSIS

The effectiveness of established cryptographic security solutions against various forms of cyberattacks is represented by cryptanalysis [10]. The attacks listed below are those that we took into account when evaluating the performance of the suggested modified Playfair algorithm.

1. Brute force Attack:

In a brute force attack, the intruder attempts to generate a key with a structured format. Here, the key domain is 62! (62 Factorial), which values around 3.14 * 10^85. Unfortunately, such a large number of generations for a key is impossible. Thus, a brute force attack is challenging to carry out.

2. Frequency Analysis Attack:

Calculated and subsequently mapped with the known ranked occurrences of alphabets in the English language is the frequency of characters found in the ciphertext. The order of alphabets in English literature, in non-increasing order of frequency, is ETAOIN SHRDL UCMFG YPWBV KXJQZ [11–12].

In the standard Playfair algorithm, the minimal probability of a particular alphabet occurring is 1 / 26 ~ 0.0385, whereas, in the modified Playfair algorithm, it corresponds to 1/62 ~ 0.0161. Unequal probabilities indicate that the number of alphabets in both ciphers is not the same. This will result in unequal replacement, which ultimately results in unequal ciphertext that has been deciphered (Plain text). Therefore, using a Frequency Analysis attack to compromise the modified Playfair algorithm is challenging.

3. Replay attack:

The encrypted message is vulnerable to replay attacks because it lacks a timestamp. However, the replay attack will be thwarted by the key freshness characteristic, which creates a new Playfair key for each message transfer.

5. CONCLUSIONS

The modified Playfair algorithm, with its larger alphabet size and reduced letter frequency correlations, demonstrates increased resistance to frequency analysis attacks compared to the standard version. This enhancement makes it a more secure option for cryptographic applications where traditional frequency analysis techniques are a potential threat.

However, it's crucial to acknowledge that while the modified algorithm is more resilient, it's not entirely immune to other cryptanalytic methods. Factors such as known-plaintext or chosen-plaintext attacks, combined with advances in computing power and cryptanalysis techniques, could potentially compromise its security. Therefore, a comprehensive security assessment should consider multiple attack vectors and cryptographic techniques to ensure the overall robustness of a system employing the modified Playfair algorithm.

REFERENCES

[1] Improved Cryptography by Applying Transposition on Modified Playfair Algorithm Followed by Steganography R Patil, SV Bang, RB Bangar- Int. J. Innov. Sci. Res. Technol, 2021

[2] Chand, N., & Bhattacharyya, S. (2014). A novel approach for encryption of text messages using playfair cipher 6 by 6 matrix with four iteration steps. International Journal of Engineering Science and Innovative Technology (IJESIT) Volume, 3, 478-484

[3] Marzan, R. M., & Sison, A. M. (2019, February). An enhanced key security of playfair cipher algorithm. In Proceedings of the 2019 8th International Conference on Software and Computer Applications (pp. 457- 461)

[4] Bhole, D., Mote, A. and Patil, R., 2016. A new security protocol using hybrid cryptography algorithms. International Journal of Computer Sciences and Engineering, 4(2), pp.18-22

[5] Goyal, S., Pacholi, B. S., Rao, B. A., Rai, S., & Kini, N. G. (2021). Parallel Message Encryption Through Playfair Cipher Using CUDA. In Evolution in Computational Intelligence (pp. 519-526). Springer, Singapore

[6] Mathur, S. K., & Srivastava, S. (2018). Extended 16x16 Play-Fair Algorithm for Secure Key Exchange Using RSA Algorithm. International Journal on Future Revolution in Computer Science & Communication Engineering, 4(2), 496-502.

[7] Anshari, M., & Mujahidah, A. (2019, October). Expending Technique Cryptography for Plaintext Messages by Modifying Playfair Cipher Algorithm with Matrix 5 x 19. In 2019 International Conference on Electrical Engineering and Computer Science (ICECOS) (pp. 10-13). IEEE.

[8] Ahmed, A. M., Ahmed, S. H., & Ahmed, O. H. (2017, April). Enhancing 3D-playfair algorithm to support all the existing characters and increase the resistance to brute force and frequency analysis attacks. In 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT) (pp. 81-85). IEEE.

[9] Kalaichelvi, V., Manimozhi, K., Meenakshi, P., Rajakumar, B., & Vimala Devi, P. (2017). An Adaptive Play fair Cipher Algorithm for Secure Communication Using Radix 64 Conversion. International Journal of Pure and Applied Mathematics, 117(20), 325-330

[10] Patil, R.Y. and Ragha, L., 2011, December. A rate limiting mechanism for defending against flooding based distributed denial of service attack. In 2011 World Congress on Information and Communication Technologies (pp. 182-186). IEEE.

[11] "Letter Frequency across English Literature" https://en.wikipedia.org/wiki/Letter_frequency Patil, N. and Patil, R., 2018, January. Achieving Flatness: with Video Captcha, Location Tracking, Selecting the Honeywords. In 2018 International Conference on Smart City and Emerging Technology (ICSCET) (pp. 1-6). IEEE