Improved Cryptography by Applying Transposition on Modified Playfair Algorithm Followed by Steganography

Dr. Rachana Patil
Department of Computer Engineering
Pimpri Chinchwad College of Engineering,
Pune, Maharashtra, India

Piyush R. Chaudhari, Mayuresh R. Dindorkar,
Shalakha V. Bang, Rohit B. Bangar
Department of Computer Engineering
Pimpri Chinchwad College of Engineering,
Pune, Maharashtra, India

Abstract:- The current internet era is marked with the generation of billions and trillions of data. Most of it is concomitant with the financial sector, intelligence sector or may be the personal data pertaining to individuals and to the nation. Hence, it is crucial to protect and secure it. Cryptography is a technique that encrypts the data and makes it secure to be transmitted over the internet. Over the time various techniques have been evolved to cipher the original text. Playfair algorithm is the most widely used cryptographic algorithm. But is however subjected to brute force attacks. The proposed method improves the performance of traditional playfair cipher and introduces novel technique of keyless transposition i.e. RMPS (Rohit Mayuresh Piyush Shalakha) transposition to further enhance the security capability of proposed methodology. Further, in order to secure the communication between sender and receiver, steganography is used to provide an additional layer of security.

Keywords:- *Security; Cryptography; Playfair; RSA; Keyless Transposition; Steganography; Key Encryption; RMPS.*

I. INTRODUCTION

Cryptography is the process of converting the plain text into unintelligible text. Plain text is nothing but text which is easily read by a normal human being and hence to securely transfer it over a communication channel, it is converted by the process of cryptography into ciphertext. The ciphertext is the text which is not easily readable. In the word "Cryptography", "Crypt" stands for "hiding" or "vault" and "graphy" stands for "way of writing". Cryptography refers to secure information communication techniques derived from mathematical concepts and a set of rules called algorithms. It converts the original readable and understandable message to an unreadable and not easily understandable message.

The cryptographic algorithms are categorized as Symmetric and Asymmetric algorithms. The Playfair cipher is a symmetric cryptographic algorithm that uses the same key to cipher and decipher. It was invented in 1854 by Charles Wheatstone as the first practical digraph substitution cipher. It was later named after Lord Playfair who promoted this algorithm. This was the first technique that encrypts and decrypts the ‘digraph’ - a pair of letters.

Playfair cipher uses a matrix often called "key-Square" to perform encryption and decryption. The standard size of the key square is 5*5. The plain text is splitted into digraphs and then each digraph is encrypted by following certain rules.

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.

RSA is an asymmetric cryptography algorithm that uses two different keys for encryption and decryption namely public key and private key. RSA stands for Rivest, Shamir, Adleman because these people invented this algorithm in 1978. It is a public-key encryption algorithm.

Different type of steganography illustrated in Fig. 1:

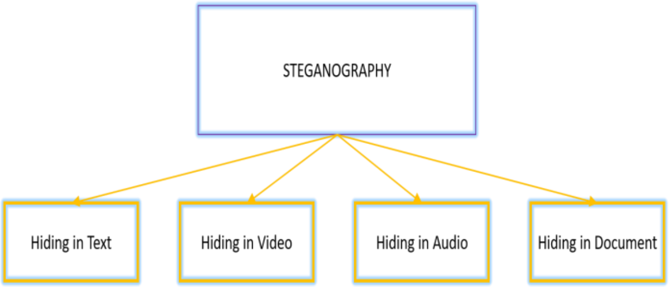


Fig. 1. Types of Steganography

Steganography is a technique of pounding the secret data within a file, message, audio, or image to avoid the identification of the secret message. In this technique, it does not alter the original characters of the message, instead it aims to hide it and make it invisible.

The proposed research work aims to improve the performance of traditional Playfair cipher algorithm by constructing a key square of size 4*19 in contrast to standard size of 5*5 and use the RSA algorithm along with the proposed novel technique - RMPS keyless transposition to further enhance the security and confidentiality of the message.

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

II. LITERATURE SURVEY

Authors in [1] have implemented a modified Playfair cipher algorithm by constructing matrix of size 6*6 that includes 26 alphabets in English and 0-9 digits. The author considers four reserved keywords on which the plain text is encrypted 4 times and then the same reserved keywords are used during the process of decryption.

The authors have proposed an enhanced key security of Playfair cipher using matrix of size 16x16, Exclusive OR method, two’s complement, and swapping of bit method. The proposed method in [2] has strong avalanche effect and greater security from brute-force attacks [3].

In [4], the parallel implementation of conventional Playfair cipher is done by using CUDA programming. By applying parallelization, the authors have achieved significant speed up and reduction in time complexity over the sequential version of conventional Playfair cipher algorithm.

Authors in [5] have used the combination of Playfair cipher and RSA technique to exchange the keys between sender and receiver in a much secured manner. An attempt has been made to modify the existing Playfair cipher matrix and making it to the size of 16*16. The RSA algorithm is used to encrypt the key which is used in the Playfair cipher algorithm, thereby enhancing the security of the proposed method. The future scope of this method aims to decrease the decryption time of the RSA algorithm.

An attempt to enhance the performance of existing Playfair cipher algorithm by proposing the modified Playfair cipher with the matrix size of 5*19 was made by the authors in [6]. Though the method uses 95 printable characters, the disadvantage of performing cryptanalysis by the method of counting frequency of occurrence still persists.

There are several ways through which the traditional Playfair cipher algorithm can be enhanced. One such method is to create the 3D Playfair cipher by increasing the confusion rates and making 4 matrices of 4*4 each. This 3D Playfair cipher accepts a combination of three characters rather than a pair of two. The authors in [7] have modified this 3D Playfair cipher extensively by using 4 matrices of size 128*128. With such a high number of i.e. 65536 characters, the proposed method in this case has become more immune to Frequency analysis and the brute force cryptanalysis techniques.

The proposed research work in [8] uses the Radix conversion method that uses 65 characters to encode and decode the message at sender and receiver side. The original Playfair cipher algorithm of 5*5 matrix is enhanced and a matrix of size 8*8 is used which is initially filled with the predetermined keyword.

III. PROPOSED METHOD

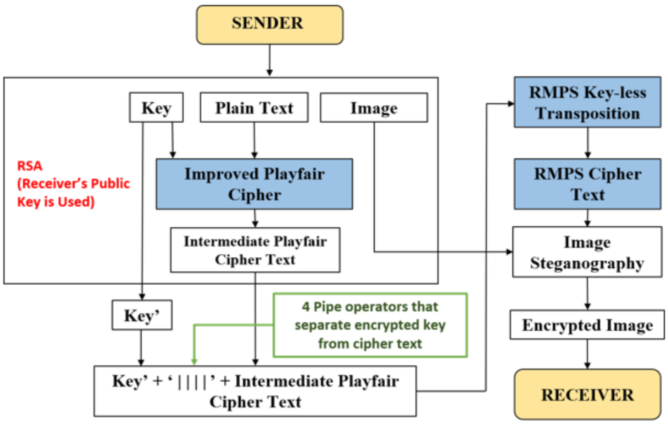
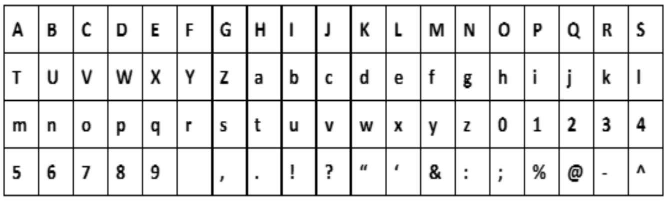


Fig. 2. Block Diagram of Proposed Method

The proposed methodology depicted in Fig. 2 follows the following process to encrypt the plain text message which is intended to be sent from sender to receiver.

A. *Improved Playfair Cipher Algorithm*

The traditional Playfair cipher algorithm consisting of matrix of size 5*5 is improved by constructing the matrix of size 4*19 consisting of all 76 characters - 26 small letter English alphabets (a-z), 26 capital letter English alphabets (A-Z), 10 digits (0-9) and 14 symbols (<space>, <,>, <.>, <!>, <?>, <">, <'>, <&>, <:>, <;>, <%>, <@>, <->, <^>) refer Fig. 3. Sender utilizes the ‘key’ to encrypt the plain text using the Improved Playfair cipher algorithm to generate the cipher text.



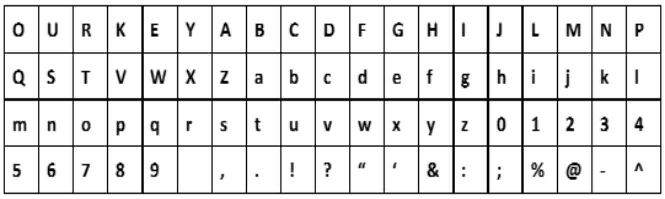
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	U	V	W	X	Y	Z	a	b	c	d	e	f	g	h	i	j	k	l
m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4
5	6	7	8	9		,	.	!	?	“	‘	&	:	;	%	@	-	^

Fig. 3. 4*19 Key matrix used for modified playfair algorithm

Example:
Key: OURKEY
Plain Text: Hello World

Encryption Steps:

1. Generate Key Square.



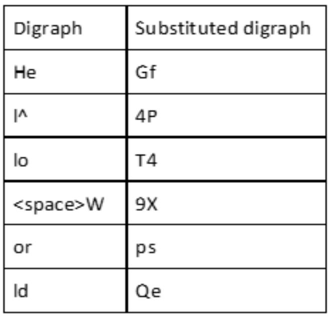
O	U	R	K	E	Y	A	B	C	D	F	G	H	I	J	L	M	N	P
Q	S	T	V	W	X	Z	a	b	c	d	e	f	g	h	i	j	k	l
m	n	o	p	q	r	s	t	u	v	w	x	y	z	0	1	2	3	4
5	6	7	8	9		,	.	!	?	“	‘	&	:	;	%	@	-	^

2. In case of repetition of letters, separate them by < ^ >.
   Hello World → Hel^lo World

3. If the entire message length is odd then append < ^ > at the end to make the length even.
Here, Hel^lo World → length = 12 (Even).

4. Generate digraphs.
He, l^, lo, <space>W, or, ld

5. Substitute the letters in digraph by following standard rules of replacement.



Digraph	Substituted digraph
He	Gf
l^	4P
lo	T4
<space>W	9X
or	ps
ld	Qe

6. Form the Final cipher Text
Gf4PT49XpsQe

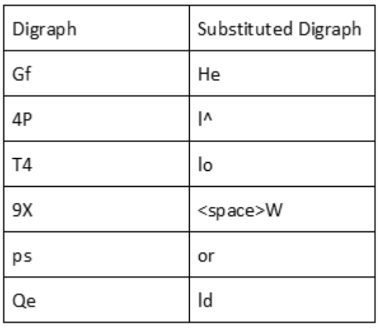
Decryption Steps:

1. Accept the cipher text.
Gf4PT49XpsQe

2. Create the key square.

3. Generate digraphs
Gf, 4P, T4, 9X, ps, Qe

4. Digraph substitution



Digraph	Substituted Digraph
Gf	He
4P	l^
T4	lo
9X	<space>W
ps	or
Qe	ld

5. Retrieve the original text
He, l^, lo, <space>W, or, ld
Hello World (After removing all ^ characters)

B. *Encrypting Key using RSA*

The ‘key’ which is used for encryption in the playfair cipher algorithm is encrypted by the sender using the receiver's public key in accordance with the RSA algorithm. This encrypted key (key’) is concatenated with the cipher text obtained in previous step i.e. “intermediate playfair cipher” text using 4 pipe (||||) operators.

C. *The Proposed RMPS Keyless Transposition*

Proposed RMPS transposition is elucidated in Fig. 4. The string formed in previous step (Key’+ |||| + "intermediate playfair cipher") is broken down into two separate lists - list 1 (containing even positioned characters) and list 2 (containing odd positioned characters). Finally concatenate the list 2 with list 1 and reverse the concatenated list to obtain the “RMPS cipher text”.

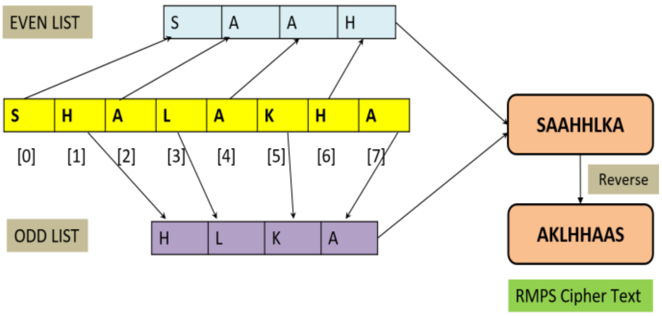


Fig. 4. Proposed Keyless RMPS Transposition algorithm

D. *Image Steganography*

The “RMPS cipher text” is hidden in the image with a technique called Least Significant Bit Steganography (LSBS) to make it more secure and send it to the receiver. LSBS is a technique in which the least significant bit of pixels of the image is replaced with data bits.

E. *Decryption process*

Once the encrypted image is collected by the receiver then the “RMPS cipher text” hidden inside the image is retrieved by steganography. This message is then passed to the RMPS keyless transposition algorithm that applies the exact reverse process of what applied during encryption.

Once the receiver gets access to the “final cipher text”, the "intermediate playfair cipher" and key’ is obtained by splitting it on ‘||||’ (4 pipe operators). Receiver decrypts the key’ by using his/her private key to obtain ‘key’ (used in improved playfair algorithm). Now, the “intermediate playfair cipher” is decrypted using the key, by applying the improved playfair cipher in reverse manner to obtain the original plain text.

IV. CRYPTANALYSIS

Cryptanalysis represents the robustness of implemented cryptographic security systems against different types of cyberattacks [9]. Following are the attacks we have considered for performance evaluation of the proposed 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 73! (73 Factorial), which values around 4 * 10^105. Unfortunately, such a large number of generations for a key is impossible. Thus, brute force attack is challenging to carry out.

2. Frequency Analysis Attack:

The frequency of characters present in the ciphertext is calculated and further mapped with the known ranked occurrences of alphabets in the English language. The ranking of alphabets in non-increasing order of frequency in English literature is ETAOIN SHRDL UCMFG YPWBV KXJQZ [10-11].

In the standard Playfair algorithm, the minimal probability of a particular alphabet to occur is 1 / 26 ~ 0.0385, whereas, in the modified Playfair algorithm, it corresponds to 1/73 ~ 0.0137. Unequal probabilities signify that both ciphers do not contain the same number of alphabets. This will lead to unequal replacement, which eventually leads to unequal decrypted ciphertext (Plain text). Thus, it is difficult to breach the modified Playfair algorithm using the Frequency Analysis attack.

3. Replay attack:

Due to absence of timestamp in the encrypted message it is susceptible to replay attack. But, the key freshness property that generates a new playfair key for every message transfer will help to tackle the replay attack.

4. Man-in-the-middle-attack:

Consider a scenario where S is a sender, R is the receiver, and M is the middle man (Intruder). In this attack, M pretends to be R for S and S for R. While sending message S unknowingly encrypts the message with M's public key thinking that it is R's public key. Now, M decrypts the message with its private key and gets access to the message. Thus, in the proposed method standard RSA is prone to Man-in-the-middle-attack.

V. CONCLUSIONS

The proposed cryptographic technique has the capability to tackle modern day sophisticated cyber-attacks by increasing security of existing models. The use of RSA, Steganography and RMPS keyless transposition to assist the modified playfair cipher in the entire encryption and decryption process further intensifies the task of hackers to intrude in the system.

VI. FUTURE WORK

Having achieved considerable performance enhancement by modified playfair cipher algorithm, we further aim to explore more about the size of ‘key square’ that can be used to achieve greater efficiency and security.

We have used the RSA algorithm to encrypt the key and thus add an extra security level to the model. Further we can replace the RSA algorithm with other more robust algorithms as it can be tempered by middlemen posing threat to the security of public key.

REFERENCES

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

[2]. 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).

[3]. 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.

[4]. 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.

[5]. 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.

[6]. 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.

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

[8]. 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.

[9]. 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.

[10]. "Letter Frequency across English Literature" https://en.wikipedia.org/wiki/Letter_frequency

[11]. 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.