Enhanced 6x6 Playfair Cipher using Double Myszkowski Transposition

Anirban Bhowmick
Student – B.Tech
Dept of CSE- MIT, Manipal

Anand Vardhan Lal
Student – B.Tech
Dept of CSE- MIT, Manipal

Nitish Ranjan
Student – B.Tech
Dept of CSE- NIE, Mysore

***Abstract*-With the growing importance of transmitting data over the network, data encryption is becoming critical. Encryption helps safeguarding the data transmitted over the network from an unwanted entity. The two methods to encrypt data are-Substitution and Transposition.**

Transposition refers to changing the position of characters in a given text. On the other hand, substitution is the process of replacing each character of the plaintext with some other character.

Playfair cipher is an illustration of substitution cipher. The classical playfair cipher has a 5x5 matrix. To increase the resistance of playfair cipher, this paper proposes to introduce double Myszkowski transposition on a modified 6x6 playfair matrix. The 6x6 matrix includes the all the alphabets along with the single digit numbers. A comparison with the classical 5x5 playfair cipher proves the enhanced security of the proposed algorithm.

Keywords: Cryptography, Modified Playfair Cipher, Double Myszkowski Transposition.

I. INTRODUCTION

Information being transmitted from sender to receiver should be kept safe from intruders. With loads of information being sent over the networks, encryption of information at the transmitter's end is crucial to safeguard the information against security attacks [1] and provide the much needed data confidentiality [2]. This ciphered information, once received, can be decrypted. Encryption and decryption uses a secret key. When this key is known only to the transmitter and the reciever, it is called symmetric encryption [3]. On the other hand, asymmetric encryption uses a public key [4] [5].

The playfair cipher is a substitution cipher [6]. The traditional playfair cipher uses a 5x5 playfair matrix containing a keyword or phrase. To generate the key matrix, one would first fill the cells of the matrix with the letters in the keyword row by row overlooking the repeating characters and then fill the remaining letters alphabetically, usually omitting 'Q' to reduce the alphabets to fit in the matrix otherwise treat 'I' and 'J' as a single alphabet.

To encrypt a message, one would divide the message into digraphs (groups of 2 letters) and map them on the key table. If required, append a 'Z' to complete the last digraph [7]. Then apply the 4 rules [13], in order, to every pair of letters in the plaintext:

- If both alphabets are identical, add an 'X' after the first alphabet. Encrypt the new pair and carry on. 'X' is not mandatory. Any rare monograph will do.
- If the alphabets are on the same row of the table, substitute them with the alphabets to their immediate right respectively.
- If the alphabets are on the same column of the table, substitute them with the alphabets immediately below respectively.
- If the alphabets don't appear on the same row or column, substitute them with the alphabets on the same row respectively but at the other pair of corners of the rectangle demarcated by the original pair. The order is important – the first letter of the encrypted pair is the one that lies on the same row as the first alphabet of the plaintext pair.

The traditional playfair cipher had one key flaw. A digraph and its reverse (e.g. AB and BA) will decrypt to the same alphabet pattern in the plaintext (e.g. RE and ER). There are several words which cover these reversed digraphs such as REceivER and DEpartED. Identifying adjacent reversed digraphs in the cipher text and matching the pattern to a list of known plaintext words containing the pattern is a way to create possible plaintext strings with which the key can be constructed. In this paper, the authors introduce the concept of double Myszkowski transposition on playfair cipher making it difficult to cryptanalyze.

Further, Myszkowski transposition is a transposition cipher [6]. It is a technique in which the plain text is written in a matrix in row-wise manner. The cipher text is obtained by reading this matrix column-wise. The order in which the columns are read is again decided by a key which is a string of numbers. Plaintext columns with unique numbers are transcribed downward but those with recurring numbers are transcribed left to right.

The rest of the paper is divided into the following sections. Section 2 highlights some of the existing work done in the field of enhancing the playfair cipher. In section 3, the authors describe the proposed algorithm in detail. Section 4 contains brief examples of the proposed algorithm. The authors compare the proposed algorithm with classical playfair cipher in section 5. Finally, in section 6 the authors present the conclusion.

II. RELATED WORKS

The Playfair is significantly harder to break since the frequency analysis [8] used for simple substitution ciphers does not work with it. The frequency analysis of digraphs is possible, but significantly more difficult. Over the years, a number of improvements have been suggested to improve the resistance of playfair cipher.

In [9], authors have suggested a 6x6 matrix. This matrix includes the alphabets followed by the single digit numbers. The matrix cells are filled with the keyword first followed by the remaining alphabets as in traditional playfair cipher. Also, numbers between 0 and 9 are placed in the cells providing the additional benefit of encrypting numbers.

Authors in [10] have suggested a 10x9 matrix including the special symbols, numbers and alphabets. In addition to what authors in [9] have included in the matrix, the matrix also includes special characters allowing encryption of these characters possible and also providing a higher distorted text.

Another attempt was made by the authors in [11] in which the authors proposed a shift matrix using random shift key generation. The characters in the matrix were shifted towards the left and the number of cells each character was shifted depended on the key generated.

In [12], authors used a 16x16 matrix. The matrix is first filled from left to right and top to bottom with the keyword after the repeating characters have been eliminated like the traditional playfair matrix. The remaining matrix is filled with the remaining characters from ASCII values 0 to 255. This provided a wide range of characters to be encrypted and also be present in the encrypted text.

For all the above proposed algorithms, the same substitution approach (4 rules of substitution) was followed which was earlier mentioned in Section 2. One thing common in all the above mentioned works is that the authors have primarily concentrated in modifying the playfair matrix. This paper proposes an enhancement to the above substitution techniques. Previously, the text was only encrypted using substitution. In this paper, the text is subjected to double Myszkowski transposition [14], after the substitution phase, thereby improving the resistance of the text thereby making cryptanalysis [4] [15] difficult.

III. PROPOSED ALGORITHM

Encryption

The proposed algorithm requires two keys. The first key (K_1) will be a keyword. This keyword will be used to fill the initial cells of the 6x6 matrix. The keyword is written out in row-wise manner ignoring the repetitive occurrence of any alphabet. The remaining letters are then written out alphabetically in the same way. After all characters are exhausted, the single digits are written starting from 0 to 9.

The playfair table or playfair square will be used for substitution of each character. Once the playfair matrix is obtained, the plaintext (P) can be divided into digraphs. Each pair can be then encrypted as done in traditional playfair cipher (discussed in Section 2). This will give us the first intermediary cipher text (C_1). In case of traditional playfair cipher, the cipher text obtained after this step would be the final cipher text that would be transmitted over the network.

In the proposed algorithm, we input another key (K_2). The first intermediary cipher text (C_1) is then subjected to Myszkowski transposition. The second key (K_2) will be a string of digits. The number of digits constituting the length of key K_2 is calculated. C_1 is then written out in rows of the same length as the number of digits in K_2. The second intermediary text (C_2) is obtained by reading the text in column by column manner. The order in which the columns are read is decided by the key K_2. Plaintext columns with unique numbers are transcribed downward but those with recurring numbers are transcribed left to right. The cipher text thus obtained (C_2) is subjected to another Myszkowski transposition. The second intermediary text (C_2) is again written out in a row-wise manner and read in column-wise manner and the order in which the column is read is dependent on the same key K_2. The encrypted text thus obtained is the final encrypted text (C).

Decryption

Symmetric cryptographic algorithms share the same set of keys during encryption and decryption. In such cases, decryption is just the reverse process.

During decryption, both the keys (K_1 and K_2) are used again but this time in the reverse order. The first key to be used will be K_2. The cipher text is written in column by column manner. The order of the columns is decided by the key (K2). Then the matrix formed is read in row-wise manner to obtain the first intermediary plain text (P1). The first intermediary plain text is then subjected to another reverse Myszkowski transposition process. P_1 is written out in another matrix using key K2. The characters are written column by column. The characters are then read in row by row manner to obtain the next plain text (P2). P_2 is then decrypted by playfair cipher which uses the keyword (K_1) generating the same original plain text.

IV. EXPERIMENTAL ANALYSIS

Test Case 1

Plain Text (P)	CRYPTOGRAPHYANDNETWORKSECURITY
Keyword (K_1)	PLAYFAIR
Key 2 (K_2)	431542

Encryption

STEP 1: In the first step, we apply playfair substitution cipher to the original text to obtain the first intermediary cipher text (C_1). We follow the 4 rules discussed in Section 2.

The playfair matrix that will be used is shown below

P	L	A	Y	F	I
R	B	C	D	E	G
H	J	K	M	N	O
Q	S	T	U	V	W
X	Z	0	1	2	3
4	5	6	7	8	9

Fig 3: Playfair cipher table for Example 1

The digraphs obtained are
CR YP TO GR AP HY AN DN ET WO RK SE CU RI TY
The first intermediary cipher text we obtain is
C_1 = DBFLWKRBYLMPFKEMCV3WCHVBDTGPUA

STEP 2: In the second step, we subject the first intermediary cipher text (C_1) to Myszkowski transposition using K_2 to obtain the second intermediary cipher text (C_2).

4	3	1	5	4	2
D	B	F	L	W	K
R	B	Y	L	M	P
F	K	E	M	C	V
3	W	C	H	V	B
D	T	G	P	U	A

The second intermediary cipher text we obtain after first Myszkowski transposition is
C_2 = FYECGKPVBABBKWTDWRMFC3VDULLMHP

STEP 3: In the third step, we subject the second intermediary cipher text (C_2) to another Myszkowski transposition using K_2 to obtain the final encrypted text (C).

4	3	1	5	4	2
F	Y	E	C	G	K
P	V	B	A	B	B
K	W	T	D	W	R
M	F	C	3	V	D
U	L	L	M	H	P

The final cipher text is
C=EBTCLKBRDPYVWFLFGPBKWMVUHCAD3M

Decryption

The decryption process is the reverse of encryption.

STEP 1: In the first step, the first intermediary plain text (P_1) is read out by applying the reverse of Myszkowski transposition using the key K_2 on the final cipher text (C).

4	3	1	5	4	2
F	Y	E	C	G	K
P	V	B	A	B	B
K	W	T	D	W	R
M	F	C	3	V	D
U	L	L	M	H	P

The text is written out column by column and the order depends on the key (K_2). The text is then read in a row-wise manner.
The first intermediary plain text (P_1) is
P_1 = FYECGKPVBABBKWTDWRMFC3VDULLMHP

STEP 2: In step 2, the first intermediary plain text is subjected to reverse Myszkowski transposition to obtain the second intermediary plain text (P_2).

4	3	1	5	4	2
D	B	F	L	W	K
R	B	Y	L	M	P
F	K	E	M	C	V
3	W	C	H	V	B
D	T	G	P	U	A

The second intermediary plain text (P_2) is
P_2 = DBFLWKRBYLMPFKEMCV3WCHVBDTGPUA

STEP 3: In this step, the second intermediary plain text (P_2) is subjected to playfair cipher analysis to obtain the original text. We make use of the same playfair cipher table as shown in Figure 3.

The decrypted text (P) is
P = CRYPTOGRAPHYANDNETWORKSECURITY

Test Case 2

Plain Text (P)	MYBIRTHDATEIS24MAY1993
Keyword (K_1)	STORIES
Key 2	242132

Encryption

STEP 1: In the first step, we apply playfair cipher to the original text to obtain the first intermediary cipher text (C_1). The playfair matrix that will be used is shown below.

S	T	O	R	I	E
A	B	C	D	F	G
H	J	K	L	M	N
P	Q	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Fig 4: Playfair cipher table for Example 2

The digraphs obtained are

MY BI RT HD AT EI S2 4M AY 19 93

The first intermediary cipher text we obtain is
C_1 = H2FTIOLABSSEIY8HH437E9

STEP 2: In the second step, we subject the first intermediary cipher text (C_1) to Myszkowski transposition using K_2 to obtain the second intermediary cipher text (C_2).

2	4	2	1	3	2
H	2	F	T	I	O
L	A	B	S	S	E
I	Y	8	H	H	4
3	7	E	9		

The second intermediary cipher text we obtain after first Myszkowski transposition is
C_2 = TSH9HFOLBEI843EISH2AY7

STEP 3: In the third step, we subject the second intermediary cipher text (C_2) to another Myszkowski transposition using K_2 to obtain the final encrypted text (C).

2	4	2	1	3	2
T	S	H	9	H	F
O	L	B	E	I	8
4	3	E	I	S	H
2	A	Y	7		

The final cipher text is
C=9EI7THFOB84EH2YHISSL3A

Decryption

STEP 1: In the first step, the first intermediary plain text (P_1) is read out by applying the reverse of Myszkowski transposition using the key K_2 on the final cipher text (C).

2	4	2	1	3	2
T	S	H	9	H	F
O	L	B	E	I	8
4	3	E	I	S	H
2	A	Y	7		

The text is written out column by column and the order depends on the key (K_2). The text is then read in a row-wise manner.
The first intermediary plain text (P_1) is
P_1 = TSH9HFOLBEI843EISH2AY7

STEP 2: In step 2, the first intermediary plain text (P_1) is subjected to another reverse Myszkowski transposition using K_2 to obtain the second intermediary plain text (P_2).

2	4	2	1	3	2
H	2	F	T	I	O
L	A	B	S	S	E
I	Y	8	H	H	4
3	7	E	9		

The second intermediary plain text (P_2) is
P_2 = H2FTIOLABSSEIY8HH437E9

STEP 3: In this step, the second intermediary plain text (P_2) is subjected to playfair cipher analysis to obtain the original text. We make use of the same playfair cipher table as shown in figure 4.

The decrypted text (P) is
P = MYBIRTHDATEIS24MAY1993

V. COMPARISON WITH CLASSICAL PLAYFAIR CIPHER

- The traditional playfair cipher uses a 5x5 matrix where ‘I’ and ‘J’ are treated as a single character. This causes ambiguity at decipherment. This drawback is rectified in the proposed algorithm. It uses a 6x6 algorithm with all characters treated differently. Further, the matrix includes numbers from 0 to 9 making encryption more secure.

- In case of the traditional playfair cipher, it includes only one level of encryption which is substitution. In the proposed technique, there are three levels are encryption. First step includes substitution using playfair cipher table. The intermediary cipher text thus obtained is subjected to double Myszkowski transposition thereby enhancing the security of the text and making cryptanalysis difficult.

- The classical playfair cipher cannot encrypt text containing numeric values because the traditional playfair matrix lacks numeric values. The proposed algorithm has made encryption of numbers possible. Refer to Example 2 in Section 5.

VI. CONCLUSION

In this paper, the weaknesses of playfair cipher have been observed and attempts have been made to rectify them. This proposed algorithm enhances the security of the traditional playfair cipher. The plain text is subjected to three levels of encryption- substitution using playfair substitution cipher followed by double Myszkowski transposition.

The proposed technique makes use of a 6x6 playfair matrix in place of a 5x5 matrix which provides additional benefits in terms of security. Further, the cipher text thus obtained after playfair substitution is subjected to double Myszkowski transposition which improves its resistance to malicious attacks. Also, the proposed work helps encrypting texts containing numbers as a part. The classical playfair cipher lacked this ability. This is made possible due to the availability of numbers in the proposed playfair matrix.

The flaw in the proposed approach is that it ignores spaces and other special symbols at the time of encryption. This may result in data loss. In certain sentences, these symbols can carry high priority. After the cipher text in decrypted, these symbols will be absent from the plain text thus obtained. Thus, the decrypted text will suffer slight deviation from the original text.

As a part of future work, we would propose enhancement of the playfair matrix. This enhancement mainly refers to inclusion of all symbols having ASCII values between 0 and 255. Further, authors in [9][10][11][12][13] can consider introducing transposition to their proposed algorithms to improve security. We could also consider different transposition algorithms to be combined with playfair cipher.

REFERENCES

[1] William Stallings, "Cryptography and Network Security", 5th Edition

[2] Nigam Sangwan, "Text Encryption with Huffman Compression", International Journal of Computer Applications (0975 – 8887) Volume 54– No.6, September 2012

[3] Ayushi, "A Symmetric Key Cryptographic Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 15

[4] Andrew S Tanenbaum, "Computer Networks", 4th Edition

[5] Gary C. Kessler, "An Overview of Cryptography 2014" http://www.garykessler.net/library/crypto.html

[6] Atul Kahate, "Cryptography and Network Security", 2nd Edition

[7] An article on Playfair cipher is available at http://www.wisdom.weizmann.ac.il/~albi/cryptanalysis/lect3.htm

[8] Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh, "3D (4 X 4 X 4) - Playfair Cipher", International Journal of Computer Applications (0975 – 8887) Volume 51– No.2, August 2012

[9] Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I.V.N.S Aditya, P. Komuraiah, "An Extension to Traditional Playfair Cryptographic Method" International Journal of Computer Applications (0975 – 8887) Volume 17– No.5, March 2011.

[10] Sanjay Basu, Utpal Kumar Ray, "Modified Playfair Cipher using Rectangular Matrix", International Journal of Computer Applications (0975 – 8887) Volume 46– No.9, May 2012

[11] Arvind Kumar, Pawan Singh Mehra, Gagan Gupta, Aatif Jamshed, "Modified Block Playfair Cipher using Random Shift Key Generation", International Journal of Computer Applications (0975 – 8887) Volume 58– No.5, November 2012

[12] Shivangi Sharma, Shubhda Shambhavi, Saurabhi Chaudhary, Amreen Khan, "Improvement of 16X16 Playfair Cipher using Random Number Generator", International Journal of Computer Applications (0975 – 8887) Volume 94 – No 1, May 2014

[13] Surendra Singh Chauhan, Hawa Singh, Ram Niwas Gurjar, "Secure Key Exchange using RSA in Extended Playfair Cipher Technique", International Journal of Computer Applications (0975 – 8887) Volume 104 – No 15, October 2014

[14] An article on Myszkowski Transposition: cryptospecs.googlecode.com/svn/trunk/classical/specs/myszkowski.pdf

[15] M U Bokhari, Shadab Alam, Faheem Syeed Masoodi, "Cryptanalysis techniques for Stream Cipher: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 60– No.9, December 2012