Improvement of 16X16 Playfair Cipher using Random Number Generator

Shivangi Sharma
Galgotias College of Engineering
and Technology,
Greater Noida

Shubhda Shambhavi
Galgotias College of Engineering
and Technology,
Greater Noida

Saurabhi Chaudhary
Galgotias College of Engineering
and Technology,
Greater Noida

Amreen Khan
Galgotias College of Engineering
and Technology,
Greater Noida

ABSTRACT

This paper deals with the modification of Playfair cipher. The existing methods of Playfair cipher have been studied such as those implemented on 5X5, 7X4 and 6X6 Playfair matrix. The study of existing methods shows that they suffer from several drawbacks such as limited matrix size, limited key size, prone to brute force attack and frequency analysis. In this paper, the presented encryption mechanism makes the cryptanalysis a very complex process. This has been achieved by first, inserting all the 256 ASCII characters in a sequential order within a 16X16 matrix and second, by changing the rotation mechanism for encryption and decryption. The encrypted text obtained is almost unreadable.

General Terms

Encryption, Decryption, Plaintext, Ciphertext.

Keywords

Playfair Cipher, Substitution, Cryptography, Network Security, Symmetric Key.

1. INTRODUCTION

Etymologically speaking, the word cryptography comes from the Greek origin. It is a combination of two words Crypto and Graphy. Crypto means Secret and Graphy means Writing [1]

Cryptography is the art of converting plaintext to a cipher text with the help of an encryption algorithm. The process has been depicted in Figure 1. Cryptography is segmented into Symmetric key and Asymmetric key cryptography. It is further defined that same key used for encryption and decryption is called Symmetric key cryptography. Otherwise it is called Asymmetric key cryptography. This paper use substitution / replacement Playfair cipher of symmetric key cryptography [2].

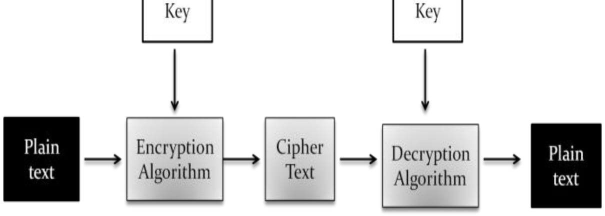

Figure 1: Encryption / Decryption Process

2. PLAYFAIR CIPHER

The Playfair cipher was invented by Charles Wheatstone in 1854. It is a symmetric substitution cipher i.e. a single key is used for both encryption and decryption. A Playfair cipher uses a 5X5 matrix and encrypts pairs of letters called digraphs. The 5 by 5 table contains a key word or phrase. The table is generated by first filling in the spaces with the letters of the keyword without including any duplicate letters and then filling in rest of the letters in alphabetical order. ‘I’ and ‘J’ are placed in same column so that all the 26 characters can be filled in a 5X5 matrix. The encryption in a Playfair cipher is done by using the following process.[2]

This process is also known as the conversion process:

1. If a digraph contains same letters then add an ‘X’ between them and re-pair the letters.
2. If the letters of the digraph appear consecutively in a row then replace them with the letters to their immediate right. In case the letter is the last letter in the row, than replace it with first letter from the left of the same row.
3. If the letters of the digraph appear consecutively in a column then replace them with the letter to their immediate below. In case the letter is the last letter in the column, than replace it with first letter from the top of the same column.
4. If the letters are on different rows and columns, replace them with the letters on the same row such that, they lie in column of the other letter. Replacing the first letter of the digraph first.

2.1 Limitations of 5X5 matrix:

- It considers the letters I and J or L and M as one character.
- 26 letters alone can take as keyword without duplicates.
- Space between two words in the plaintext is not considered as one character.
- It cannot use special characters and numbers.
- It only uses uppercase alphabets.
- A spare letter X is added when the plaintext word consists of odd number of character. In the decryption process this X is ignored. X is a valid character and creates confusion because it could be a part of plaintext, so we cannot simply remove X in decryption process.

- X is used a filler letter while repeating letter falls in the same pair are separated.

3. PROPOSED METHOD

In the proposed method a 16X16 matrix is being used in which the matrix is shifted by some random value, due to which the corresponding positions of the letters are changed. This random number can lie between 0 and 16. It can be manually entered by the user and also can be generated by a random number generator function. The random number generated rotates the matrix by that particular value.

3.1 The Encryption algorithm:

1. Read the keyword.

2. Eliminate the repeated characters in keyword.

3. Construct a 16X16 matrix by filling the character of keyword from left to right and top to bottom.

4. Fill the reminder of matrix with the remaining characters from ASCII values 0 to 255.

5. Read a plaintext.

6. Divide the plaintext into pair of characters.

7. Add the character "Null" when odd number of character are present in the message.

8. Generate a random number using RAND function.

9. Shift the matrix from top to bottom towards left circularly by the first generated random number.

10. Encrypt the first diagraph using the following modified conversion process:

a) If a digraph contains same letters then add a '*' between them and re-pair the letters.

b) If the letters of the digraph appear consecutively in a row then replace them with the letters to right, shifted by the value of random number generated. In case the letter is the last letter in the row, than replace it with that letter which is random number position from the left of the same row.

c) If the letters of the digraph appear consecutively in a column then replace them with the letters below, shifted by the value of random number generated. In case the letter is the last letter in the column, than replace it with that letter which is random number position below in the same column.

d) If the letters are on different rows and columns, replace them with the letters on the same row such that, they lie in column of the other letter. Replacing the first letter of the digraph first.

11. Generate another random number and rotate a matrix by making a left shift circularly with the generated random number. Then encrypt another digraph using the conversion process and so on.

12. Send all the random numbers generated to the receiver.

3.2 The Decryption algorithm:

1. Read the keyword.

2. Eliminate the repeated characters in keyword.

3. Construct a matrix by filling the character of keyword from left to right and top to bottom.

4. Fill the reminder of matrix with the remaining characters from ASCII values 0 to 255.

5. Read the ciphertext.

6. Divide the ciphertext into pair of characters.

7. Add the character "Null" when odd number of character in the message. Use the received random numbers in reverse order to rotate the matrix.

8. Use the lastly generated random number to rotate the matrix from bottom to top using right shift circularly then decrypt firstly the last diagraph.

9. Again use the second last generated random number to rotate the matrix and decrypt the second last diagraph and so on in reverse order of diagraph and random number.

10. Decrypt using the conversion process.

11. Finally reverse the string and obtain the plaintext.

4. DEVLOPMENT OF THE MATRIX

The initial matrix would be developed by first taking a 16X16 matrix and then filling the matrix with all the ASCII values in a sequential manner. The complete matrix obtained has been depicted in **Table 1** [7].

Let the keyword be: Play:5☺. On inserting the keyword in the matrix, **Table 2** is obtained. Let the plaintext be Dell. Since 'l' occurs consecutively, we separate them with a '*' obtaining 3 diagraphs:

De l* l*

Initially, let the random number generated be 4 so that the matrix will be rotated circularly left by 4 positions as shown in **Table 3**. Now, to encrypt the second digraph the above obtained Table 3 is rotated by random number 6 (say) by which we obtain **Table 4**.

Using the conversion process on Table 4, the cipher text of the second digraph 'l*' is obtained as 'P+'

Similarly, in order to encrypt the third digraph, the above obtained Table 4 is rotated by random number 8 thus, obtaining **Table 5**.

Using the conversion process, the cipher text of the third digraph 'l'* is also obtained as 'P+'.

Thus, 'Dell' is encrypted to 'CfP+P+'

5. CRYPTANALYSIS

In 5x5 Playfair cipher , cryptanalysis is done through two processes. First is brute force attack and second is frequency analysis. In brute force attack we apply a number of permutation and combinations while in frequency analysis number of occurrences of letters in English alphabets are found and compared to maximum occurrence of each letter in plaintext. Also, the number of permutation applied on each digraph is 676 combinations, which can be easily broken in few hours.

But in 16x16 Playfair, as we are using all the 256 ASCII values which will take more time to apply brute force attack on each pair of diagraphs because each diagraph take 676 combinations. The frequency analysis of 16x16 is very typical, as the frequency analysis of alphabets is available but not that of ASCII symbols.

Also, in the proposed method, the conversion process has been slightly altered i.e. in the original conversion process; if the letters of the digraph appear consecutively in a column then they are replaced with the letter to their immediate below. In case the letter is the last letter in the column, then it is replaced with first letter from the top of the same column.

But in the proposed method, if the letters of the digraph appear consecutively in a row then replace them with the letters to right, shifted by the value of random number generated. In case the letter is the last letter in the row, than replace it with that letter which is random number position from the left of the same row. If the letters of the digraph appear consecutively in a column then replace them with the letters below, shifted by the value of random number generated. In case the letter is the last letter in the column, than replace it with that letter which is random number position below in the same column.

6. CONCLUSION

The implementation of advanced encryption algorithm generates cipher text which is very complex. It is concluded that by changing the encryption mechanism by including a random number, the complexity of the encrypted text can be significantly increased.

Table 6: Comparison between Proposed and Existing method

S.No.	Properties	Existing method (5x5,6x6,7x4)	Proposed method(16x16)
1	Encryption technique	Normal	Modified
2	Frequency analysis	Possible with alphabets	Not possible due to symbols
3	Key size	25,36,28	256
4	Matrix size	25,36,28	256
5	Random numbers	Not used	Used
6	Rotation	Not used	Used

The above depicted table clearly shows the difference between existing methods of encryption used in 5X5, 6X6, 7X4, 16X16 matrix and proposed method that changes the encryption mechanism and increases the keysize. The advantages of proposed method can be enlisted as follows:

- The conversion process has been altered which enhances the complexity of the ciphertext.
- The matrix is rotated by a certain random number before encrypting[8].
- It allows more than 26 characters as keyword.
- The letters ‘I’ and ‘J’ are not treated as same characters.
- It considers the space between two words in plaintext as one character.
- This proposed scheme is case sensitive.
- The user can easily encrypt and decrypt the combination of alphabets, numbers and special characters efficiently as the same time, the complexity of cryptanalysis is uncompromised.

It can be safely concluded that the proposed method is very much efficient than the existing method by the virtue of its extended matrix, increased key size and modified encryption mechanism.

7. ACKNOWLEDGMENTS

We are extremely thankful to our project guide Ms. Amreen Khan for her invaluable help and guidance throughout the duration of the practical project. We are especially grateful to her for always welcoming new ideas and offering constructive suggestions which carried us through to achieve the completion of the project. We thank her for taking out time from her busy schedule to help us out. Without her, this project could not have been done.

8. REFERENCES

[1] Andrew S. Tanenbaum, Networks Computer, 5th edition, Pearson Education, ISBN-10: 0132553171.

[2] William Stallings, “Cryptography and Network Security Principles and Practice”, 4th Edition, Prentice Hall,2006.

[3] Aftab Alam, Sehat Ullah, Ishtiaq Wahid, & Shah Khalid “Universal Playfair Cipher Using MXN Matrix”. International Journal of Advanced Computer Science, Vol.1, No.3, Pp.113-117, Sep.2011.

[4] 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.

[5] Muhammad Salam, Nasir Rashid, Shah Khalid, Muhammad Raees Khan, “A NXM Version of 5X5 Playfair Cipher for any Natural Language (Urdu as Special Case)”. World Academy of Science, Engineering and Technology 73 2011.

[6] A. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam, “A Modified Version of Playfair Cipher Using 7×4 Matrix”. International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.

[7] S.S.Dhenakaran, M. Ilayaraja, “Extension of Playfair Cipher using 16X16 Matrix”. International Journal of Computer Applications (0975 – 888) Volume 48– No.7, June 2012.

[8] 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 .

Table 1: 16x16 Matrix containing ASCII values in sequential order

NUL	☺	☻	♥	♦	♣	♠	•	◘	○	◙	♂	♀	♪	♫	☼
►	◄	↕	‼	¶	§	▬	↨	↑	↓	→	←	∟	↔	▲	▼
Space	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
@	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	{	|	}	~	⌂
Ç	Ü	É	Â	Ä	À	Å	ç	ê	ë	È	ï	î	ì	Ä	Å
É	Æ	Æ	Ô	Ö	Ò	Û	ù	ÿ	Ö	Ü	¢	£	¥	₧	ƒ
á	Í	Ó	Ú	Ñ	Ñ	ª	º	¿	⌐	¬	½	¼	¡	«	»
░	▒	▓	│	┤	╡	╢	╖	╕	╣	║	╗	╝	╜	╛	┐
└	┴	┬	├	─	┼	╞	╟	╚	╔	╩	╦	╠	═	╬	╧
╨	╤	╥	╙	╘	╒	╓	╫	╪	┘	┌	█	▄	▌	▐	▀
α	ß	Γ	Π	Σ	Σ	µ	τ	Φ	Θ	Ω	δ	∞	φ	ε	∩
≡	±	≥	≤	⌠	⌡	÷	≈	°	·	·	√	^{n}	^{2}	■	

Table 2: Modified matrix containing keyword

P	L	a	y	:	5	☺	NUL	☻	♥	♦	♣	♠	•	◘	○
◙	♂	♀	♪	♫	☼	►	◄	↕	‼	¶	§	▬	↨	↑	↓
→	←	∟	↔	▲	▼	Space	!	"	#	$	%	&	'	(	)
*	+	,	-	.	/	0	1	2	3	4	6	7	8	9	;
<	=	>	?	@	A	B	C	D	E	F	G	H	I	J	K
L	M	N	O	Q	R	S	T	U	V	W	X	Y	Z	[	\
]	^	_	`	B	c	D	e	f	g	H	i	j	k	m	N
o	p	q	r	S	t	U	v	w	x	z	{	|	}	~	⌂
Ç	ü	é	â	Ä	à	Å	ç	ê	ë	è	ï	î	ì	Ä	Å
É	æ	Æ	ô	Ö	ò	Û	ù	ÿ	Ö	Ü	¢	£	¥	₧	ƒ
á	í	ó	ú	Ñ	Ñ	ª	º	¿	⌐	¬	½	¼	¡	«	»
░	▒	▓	│	┤	╡	╢	╖	╕	╣	║	╗	╝	╜	╛	┐
└	┴	┬	├	─	┼	╞	╟	╚	╔	╩	╦	╠	═	╬	╧
╨	╤	╥	╙	╘	╒	╓	╫	╪	┘	┌	█	▄	▌	▐	▀
α	ß	Γ	π	Σ	σ	µ	τ	Φ	Θ	Ω	δ	∞	φ	ε	∩
≡	±	≥	≤	⌠	⌡	÷	≈	°	·	·	√	^{n}	^{2}	■	

Table 3: Rotated matrix by random number 4

:	5	☺	NUL	☻	♥	♦	♣	♠	•	◘	○	◙	♂	♀	♪
♫	☼	►	◄	↕	‼	¶	§	▬	↨	↑	↓	→	←	∟	↔
▲	▼	space	!	"	#	$	%	&	'	(	)	*	+	,	-
.	/	0	1	2	3	4	6	7	8	9	;	<	=	>	?
@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_	`
b	c	d	E	f	g	H	i	j	k	m	n	O	p	q	r
s	t	u	V	w	x	Z	{	|	}	~	⌂	Ç	ü	é	â
ä	à	å	Ç	ê	ë	È	ï	î	ì	Ä	Å	É	æ	Æ	ô
ö	ò	û	Ù	ÿ	Ö	Ü	¢	£	¥	₧	ƒ	Á	í	ó	ú
ñ	Ñ	ª	º	¿	⌐	¬	½	¼	¡	«	»	░	▒	▓	│
┤	╡	╢	╖	╕	╣	║	╗	╝	╜	╛	┐	└	┴	┬	├
─	┼	╞	╟	╚	╔	╩	╦	╠	═	╬	╧	╨	╤	╥	╙
╘	╒	╓	╫	╪	┘	┌	█	▄	▌	▐	▀	A	ß	Γ	π
Σ	σ	µ	T	Φ	Θ	Ω	δ	∞	φ	ε	∩	≡	±	≥	≤
⌠	⌡	÷	≈	°	·	·	√	ⁿ	²	■		P	l	a	Y

Table 4: Rotated by random number 6

♦	♣	♠	•	◘	○	◙	♂	♀	♪	♫	☼	►	◄	↕	‼
¶	§	▬	↨	↑	↓	→	←	∟	↔	▲	▼	space	!	"	#
$	%	&	'	(	)	*	+	,	-	.	/	0	1	2	3
4	6	7	8	9	;	<	=	>	?	@	A	B	C	D	E
F	G	H	I	J	K	L	M	N	O	Q	R	S	T	U	V
W	X	Y	Z	[	\	]	^	_	`	B	c	D	e	f	g
h	i	j	k	m	N	o	p	q	r	S	t	U	v	w	x
z	{	|	}	~	⌂	Ç	Ü	É	â	Ä	à	Å	ç	ê	Ë
È	ï	î	ì	Ä	Å	É	Æ	Æ	ô	Ö	ò	Û	ù	ÿ	Ö
Ü	¢	£	¥	₧	ƒ	á	Í	Ó	ú	Ñ	Ñ	ª	º	¿	⌐
¬	½	¼	¡	«	»	░	▒	▓	│	┤	╡	╢	╖	╕	╣
║	╗	╝	╜	╛	┐	└	┴	┬	├	─	┼	╞	╟	╚	╔
╩	╦	╠	═	╬	╧	╨	╤	╥	╙	╘	╒	╓	╫	╪	┘
┌	█	▄	▌	▐	▀	A	ß	Γ	π	Σ	σ	µ	τ	Φ	Θ
Ω	δ	∞	φ	ε	∩	≡	±	≥	≤	⌠	⌡	÷	≈	°	∙
·	√	^{n}	^{2}	■		P	l	a	y	:	5	☺	NUL	☻	♥

Table 5: Rotated by random number 8

♀	♪	♫	☼	►	◄	↕	‼	¶	§	▬	↨	↑	↓	→	←
∟	↔	▲	▼	space	!	"	#	$	%	&	'	(	)	*	+
,	-	.	/	0	1	2	3	4	6	7	8	9	;	<	=
>	?	@	A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^
_	`	b	c	D	E	F	g	h	i	j	k	M	n	o	p
q	r	s	t	U	V	W	x	z	{	|	}	~	⌂	Ç	ü
é	â	ä	à	Å	Ç	Ê	Ë	È	ï	î	ì	Ä	Å	É	æ
Æ	ô	ö	ò	Û	Ù	Ÿ	Ö	Ü	¢	£	¥	₧	ƒ	á	í
ó	ú	ñ	Ñ	ª	º	¿	⌐	¬	½	¼	¡	«	»	░	▒
▓	│	┤	╡	╢	╖	╕	╣	║	╗	╝	╜	╛	┐	└	┴
┬	├	─	┼	╞	╟	╚	╔	╩	╦	╠	═	╬	╧	╨	╤
╥	╙	╘	╒	╓	╫	╪	┘	┌	█	▄	▌	▐	▀	α	ß
Γ	π	Σ	σ	µ	Τ	Φ	Θ	Ω	δ	∞	φ	Ε	∩	≡	±
≥	≤	⌠	⌡	÷	≈	°	∙	·	√	^{n}	^{2}	■		P	L
a	y	:	5	☺	NUL	☻	♥	♦	♣	♠	•	◘	○	◙	♂