Extension of Playfair Cipher using 16X16 Matrix

S.S.Dhenakaran, PhD.
Assistant Professor
Computer Science and Engineering
Alagappa University, Karaikudi, India.

M. Ilayaraja
Research Scholar
Computer Science and Engineering,
Alagappa University, Karaikudi, India.

ABSTRACT
The role of Cryptography in today's digital world is significant. It secures information mathematically by mangling message with key. The privacy of intended sender and receiver information is protected from eavesdropper. The objective of the paper is playfair cipher. The existing methods of playfair cipher are studied. The restrictions of earlier works a playfair cipher using 5X5 matrix, 7X4 matrix and 6X6 matrix are overcome in the proposed work. The proposed method plays a 16X16 matrix giving strength to playfair cipher. The proposed work is an enhancement to the existing algorithms that uses 16X16 matrix to pick cipher characters. It makes use of alphabets both lower and uppercase characters, number and special characters for constructing the contents of the matrix.

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 deals with creating documents that can be shared secretly over public communication channels. The present Scenario, everyone needs to encrypt the message at the sender side and decrypt it at the receiver side to preserve security and privacy. So cryptography is the study of creating and using encryption and decryption techniques. In cryptography the term plaintext is used for the original message that is to be transformed. The message which has been transformed is called Ciphertext. An encryption algorithm works with a key to transform the plaintext into ciphertext. Decryption algorithm works in the reverse order and converts the ciphertext into plaintext [5].

The encryption /decryption algorithm is to encrypt/decrypt the message with the help of a key. The process of converting plaintext into ciphertext is called enciphering or encryption. The process of retaining the plaintext from the ciphertext is called deciphering or decryption. The following figure shows the encryption and decryption process.

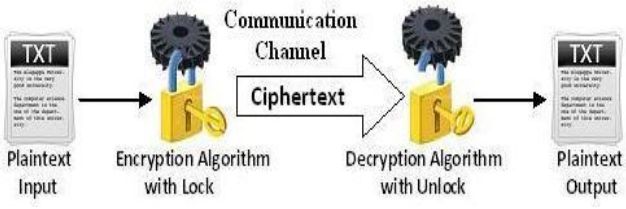

Fig 1. Encryption / Decryption Process

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 [1].

2. PLAYFAIR CIPHER
Playfair cipher that is a substitution cipher was first developed by Charles Wheatstone in 1854. Later it was promoted by Lord Playfair. Now it is called playfair cipher [2].

2.1 Existing Playfair Algorithm using 5x5 Matrix
The existing playfair cipher working on 5x5 matrix is constructed with a keyword "CRYPTO". The Table 1 below shows the construction of 5x5 matrix using the keyword "CRYPTO" plus the uppercase alphabets satisfying the rules of preparing the table. The matrix is first filled by the keyword from left to right and the remaining cells are filled by the uppercase alphabets ignoring the letters of keyword.

Table 1. Playfair 5x5 Matrix

C	R	Y	P	T
O	A	B	D	E
F	G	H	I/J	K
L	M	N	Q	S
U	V	W	X	Z

In this algorithm, the letters I & J are counted as one character. It is seen that the rules of encryption applies an pair of plaintext characters. So, it needs always even number of characters in plaintext message. In case, the message counts odd number of characters a spare letter X is added at the end of the plaintext message.

Further repeating plaintext letters in the same pair are separated with a filler letter, such as X, so that the word COMMUNICATE would be treated as CO MX MU NI CA TE.

2.1.1 Rules
a) Plaintext letters that fall in the same row of the matrix are replaced / substituted by the letter to the right, with the first element of the row circularly following the last. For example pt is encrypted as TC.

b) Plain text letters that fall in the same column are replaced by the letter beneath, with the top element of the row circularly following in the last. For example, cu is encrypted as OC.

c) Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, oh becomes BF, and fd becomes IO (or JO, as the enciphered wishes) [2].

2.1.2 Limitations of 5x5 Matrix

- It considers the letters I and J 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 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.

2.2 Existing Playfair Algorithm using 7x4 Matrix

A keyword is used to construct 7x4 matrix using letters and symbols '*' and '#' which is the base for this Playfair Algorithm. The 7x4 matrix is constructed by filling keyword with no repeating letters. Here the keyword "CRYPTO" is used. The remaining spaces are filled with the rest of alphabets. As shown in the table 2, the last cell is filled by the symbol "#" and the remaining cell that is before the last cell is filled by the symbol "*" [3].

Table 2. Playfair 7x4 Matrix

C	R	Y	P
T	O	A	B
D	E	F	G
H	I	J	K
L	M	N	Q
S	U	V	W
X	Z	*	#

The same rules of playfair 5x5 matrix are used here to encrypt the plaintext with the following modification.

- When same letters fall in a pair it adds "*" so that the message BALLS become BAL*LS.
- If a word consists of odd number of letters, it will add symbol "#" to complete the pair. So BIT becomes BI T#. The symbol # is simply ignored when the ciphertext is decrypted.

2.2.1 Limitations of 7x4 Matrix

- 26 characters only can take as a keyword without any repetition.
- The space between two words in the plaintext is not considered as one character.
- It cannot use numbers and special characters except '*' and '#'.
- It is not case sensitive.
- It ignores the symbols '*' and '#' at the time of decipherment.

2.3 Existing Playfair Algorith using 6x6 Matrix

This playfair algorithm is based on the use of a 6x6 matrix using letters and numbers. Here also the keyword "CRYPTO" is used. The matrix is constructed by filling the letters of the keyword from left to right and from top to bottom, remaining cells of the matrix are filled by uppercase alphabets and numbers ignoring the letters of the keyword as in Table 3 [4].

This algorithm cannot consider the letters I and J as one character. Place I and J in two different cells in order to avoid the ambiguity at the time of decipherment. The rules of playfair 5x5 matrix are used to encrypt the plaintext.

Table 3. Playfair 6x6 Matrix

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

2.3.1 The Existing Playfair Algorithm using 6x6 Matrix overcome the problem of 5x5 Matrix

- Letters I and J are counted as two letters.
- The alphabets and numbers are used in the plaintext and the keyword.

2.3.2 Limitations of 6x6 Matrix

- This 6x6 matrix can only take 36 characters as a keyword without duplicates.
- Space between two words in plaintext is not considered as one character.
- The matrix cannot accept special character.
- It is not case sensitive.
- When plaintext word consists of odd number of characters, a spare letter X is added with the word to complete the pair. In the decryption process this X is simply ignored. This creates confusion because X is a valid character and it can be a part of plaintext, so we cannot simply remove it in decryption process.
- When repeating plaintext letters that fall in the same pair are separated by a filler letter, such as X. This

letter X affects the plaintext at the time of decipherment.

3. THE PROPOSED PLAYFAIR CIPHER USING 16X16 MATRIX

This algorithm can accept the Plaintext containing Alphabets (capital letters and small letters), Numbers and Special characters. So the user can easily encrypt combination of alphabets, numbers and characters efficiently.

To encrypt the plaintext, the rules of 5x5 are followed with the following modification:

- While repeating plaintext characters that are in the same pair, the first character is replaced by the character to the right, with the first element of the row circularly following the last. The second character is replaced by the character to the left, with the last element of the row circularly following the first.
- If a word consists of odd number of characters, it will add the character "Null" to complete the pairs, because "Null" character cannot affect the Plaintext at the time of decipherment.

Algorithm

1. Read a 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 a plaintext.
6. Divide the plaintext into pair of characters.
7. Add the character "Null" when odd number of character in the message.
8. The conversion process:
   a) If the pair of plaintext falls in the same row of the matrix are replaced by the character to the right, with the first element of the row circularly following left.
   b) If the pair of plaintext fall in the same column of the matrix are replaced by the character beneath, with the top element of the row circularly following in the last.
   c) If the pair of plaintext are same, the first character replaced by the character to the right. The second character replaced by the character to the left.
   d) If the pair of plaintext appears on the different row and column, each plaintext character is replaced by the character that lies in its own row and column occupied by the other plaintext character.

This Playfair algorithm is based on the use of 16x16 matrix of characters constructed using a keyword. The matrix is constructed by filling the characters of keyword (minus duplicates) from left to right and from top to bottom. Then it is filling the remaining characters in ascending order from ASCII value 0 to 255, as shown in Table 4 and Table 5.

The following example uses Playfair 16x16 Matrix

Key	-	Playfair.(Sample)
Plaintext as a single word	-	Cryptography
Ciphertext	-	:feuq])yeZ
Plaintext as a phrase	-	American Online Service
Ciphertext	-	?e).p\lo∟Uü♥lt▲m).up\)☺
Plaintext as a sentence	-	Hardwork has a future pay off, Laziness pays off now.
Ciphertext	-	Gye]xqPu3~fo¶▬vuå◘▲ey§sa(&↓Umoltf]~▬eyfq¶~iy!!~qx(☺
Plaintext as a Email Id	-	m.ilayaraja_2012@gmail.com
Ciphertext	-	p(rayfy.☺Y(Y3123Bcpyrap^za

Table 4. PlayFair 16X16 Matrix

P	l	a	y	f	i	r	.	(	S	m	p	e	)	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	Q	R	T	U	V
W	X	Y	Z	[	\	]	^	_	`	b	c	d	g	h	j
k	n	o	q	s	t	u	v	w	x	z	{	|	}	~	DEL
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	T	Φ	Θ	Ω	δ	∞	φ	ε	∩
≡	±	≥	≤	⌠	⌡	÷	≈	°	∙	·	√	ⁿ	²	■	

The following example uses sentence for keyword using Playfair 16x16 Matrix

Key: Alagappa University was established by the Govt. of Tamil Nadu during the year 1985 in Karaikudi, Sivagangai District.

Plaintext as a single word - Cryptography
Ciphertext - RAw p8psg 5l

Plaintext as a phrase - American Online Service
Ciphertext - ibrsp♥giiJiavirU♣asep♥ ♣

Plaintext as a sentence - Hardwork has a future pay off, Laziness pays off now.
Ciphertext - FgalpKA♠l.gtUgU.8elerU gwU.Th☺UJe\virttU gwtp.T.UiKp►

Plaintext as a Email Id - m.ilayaraja_2012@gmail.com
Ciphertext - Nfvagwgsn\ \32G=2ydivao.N

Table 5. PlayFair 16X16 Matrix

A	l	a	g	p	space	U	n	i	v	e	r	s	t	y	w
b	h	d	G	o	.	f	T	m	N	u	1	9	8	5	K
k	,	S	D	c	NUL	☺	☻	♥	♦	♣	♠	•	◘	○	◙
♂	♀	♪	♫	☼	►	◄	↕	‼	¶	§	▬	↨	↑	↓	→
←	∟	↔	▲	▼	!	“	#	$	%	&	‘	(	)	*	+
-	/	0	2	3	4	6	7	:	;	<	=	>	?	@	B
C	E	F	H	I	J	L	M	O	P	Q	R	V	W	X	Y
Z	[	\	]	^	_	`	j	q	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	T	Φ	Θ	Ω	δ	∞	φ	ε	∩
≡	±	≥	≤	⌠	⌡	÷	≈	°	∙	·	√	ⁿ	²	■	

3.1 List of Advantages in my Proposal

- It allows more than 36 characters as keyword.
- It considers the space between two words in plaintext as one character.
- The user can easily encrypt and decrypt the combination of alphabets, numbers and special characters efficiently.
- Letters, digits and special characters are used to construct 16x16 matrix.
- It is case sensitive.
- The letters I and J are considered as two different letters.
- To compare with the previous algorithms, here the keyword length is very large, so it is very difficult to find the Plaintext from Ciphertext without knowing a keyword.
- This algorithm adds the Null character to complete the pair, because the “Null” character cannot affect the plaintext at the end of the word or sentence.
- This algorithm cannot separate a repeating Plaintext letters with a filter letter.

4. CONCLUSION

In this paper, it is attempted to use the basic playfair cipher and proposed an enhanced playfair cipher dropping the restricting of previous playfairs using 5x5, 6x6 and 7x4 matrices. The result of cipher is looking hard than the previous ciphers. It is concluded that the selection of cumbersome keyword can generate full of machine symbols in the cipher. For future enhancement to this application two different keys can be applied for encryption and decryption. Public key used for encrypt the file and private key used for decrypt it. Also, other more advanced encryption operations can be included to enhance the security of information.

5. 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 Jourrnal 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.