www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 4 April, 2013 Page No. 956 -961

A Modified Version Of Extended Plafair Cipher (8x8)

[1]Gaurav Shrivastava[*], [2]Manoj Chouhan, [3]Manoj Dhawan

[1,2,3] Assistant Professor, Department of Information Technology , Shri Vaishnav Institute of Technology & Science, Indore, Madhya Pradesh, INDIA.
Email: - [1]gaurav2086@gmail.com, [2]manoj_mits85@yahoo.com , [3]manoj.mann07@gmail.com

ABSTRACT

In this paper we have some modification in Playfair Cipher Substitution Technique. We have proposed a method to enhance the Playfair cipher for more secure and efficient cryptography. We use 8X8 Playfair cipher and have made use of a Simple Columnar Transposition Technique with Multiple Rounds in 8X8 Playfair Cipher Substitution Technique and arranged a special symbol by overall Character Frequency Analysis (CFA) .

Keywords: Playfair Cipher, Simple Columnar Transposition Technique, Special Symbols, CFA

1. INTRODUCTION

In order to provide security to the information that is to be transmitted from sender to receiver we have several methods for it. The well known and highly used method for protecting the data during its transmission across the network is encryption. The conventional encryption system consists of plain text, encryption algorithm, secret key, cipher text and decryption algorithm. We need a strong encryption algorithm in order to encrypt the plain text into cipher text. The sender and receiver must have obtained the secret key in a secure fashion and must keep the key secure. [1]

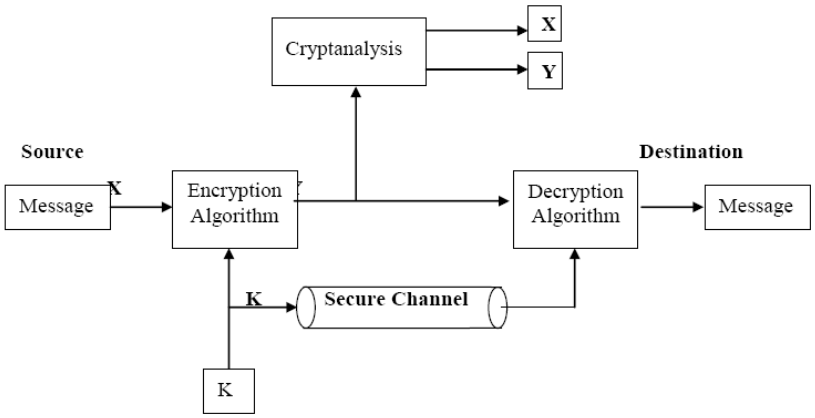
The cryptographic systems are generally classified according to the type of operations used for transforming plain text to cipher text, the number of keys used and the way in which the plain text is processed. Among all of the existing cryptographic systems play fair cipher got importance. [1]

This Existing Play Fair cipher is based on the use of a 5 X 5 matrix of letters constructed using a keyword. We use a 8X8 Playfair cipher and hence it would be using 64 grids. First we insert a alphabetic character (A-Z), and then insert numerical value (0-9) and then insert special symbols according to frequency analysis. This main advantage of the this scheme we use a Alphabetical, Numerical and Special Symbols. In Special symbols we arranged by overall Character Frequency Analysis.[2]

2. CRYPTOGRAPHY SCIENCE

The word is derived from the Greek crypto's, meaning hidden. Cryptography is a science of devising methods that allow information to be send in a secure from in such a way that the only person to able retrieve this information is the intended recipient. Encryption is based on algorithms that scramble information (Plaintext or Clear Text) into unreadable (Cipher Text) form. Decryption is the process of restoring the scrambled information to its original form. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide

information in storage or transit. Cryptographic systems are used to provide privacy and authentication in computer and communication systems. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. [3]



All Cryptographic algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, and group of bits or letters) is mapped into another element and in transposition, the elements of the plaintext have simply been re-arranged in different order; their position with relation to each other have been changed.

3. CLASSIC CRYPTOGRAPHY

The earliest forms of secret writing required little more than local pen and paper analogs, as most people could not read. More literacy, or literate opponents, required actual cryptography. The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message (e.g., 'hello world' becomes 'ehlol owrdl' in a trivially simple rearrangement scheme), and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet).[6]

A. Substitution Technique

In cryptography, a substitution cipher is a method of encryption by which units of plaintext are replaced with cipher text according to a regular system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution.

There are a number of different types of substitution cipher available like Caesar Cipher, Mono-alphabetic Cipher, Homophonic Substitution Cipher, Polygram Substitution Cipher, Polyalphabetic Substitution Cipher, Playfair Cipher and Hill Cipher. [6]

B. Transposition Technique

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically a objective function is used on the characters' positions to encrypt and an inverse function to decrypt.

There are a number of different types of Transposition cipher available like Rail Fence Cipher, Simple Columnar Transposition, Vernam Cipher, Double transposition, Myszkowski Transposition, Disrupted Transposition. [6]

4. EXISTING PLAYFAIR CIPHER

The Playfair cipher or Playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher. The scheme was invented in 1854 by

Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher. The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use. The Playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. Frequency analysis can still be undertaken, but on the 600[1] possible digraphs rather than the 26 possible monographs. The frequency analysis of digraphs is possible, but considerably more difficult – and it generally requires a much larger cipher text in order to be useful. [5]

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (usually omitting "Q" to reduce the alphabet to fit; other versions put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center. The keyword together with the conventions for filling in the 5 by 5 table constitute the cipher key. [5] To encrypt a message, one would break the message into digraphs (groups of 2 letters) such that, for example, "Hello World" becomes "HE LL OW OR LD", and map them out on the key table. If needed, append a "Z" to complete the final digraph. The two letters of the digraph are considered as the opposite corners of a rectangle in the key table. Note the relative position of the corners of this rectangle. Then apply the following 4 rules, in order, to each pair of letters in the plaintext:

1. If both letters are the same, add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any uncommon monograph will do.
2. If the letters appear on the same row of your table, replace them with the letters to their immediate right respectively.
3. If the letters appear on the same column of your table, replace them with the letters immediately below respectively.
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined 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 letter of the plaintext pair.

To decrypt, use the INVERSE (opposite) of the last 3 rules, and the 1st as-is (dropping any extra "X"s (or "Q"s) that don't make sense in the final message when finished). [5]

5. 8X8 PLAYFAIR CIPHER

Playfair cipher using 8*8 matrix and hence it would be using 64 grids. The proposed system not only encrypts the alphabets but also the numerals and special characters. It also shows space between words where required. The system uses different blocks for different alphabet, numerals and symbols. In Proposed System, it is used at the time of encryption to provide space between two words, ^ is used for stuffing between two alphabets if they are repeated in a pair and ^ will also be used to put at the end to get the last alphabet in pair if the total length comes out to be odd. At the time of decryption it will be replaced by blank space of one alphabet and the symbol ^ will be discarded. Rules for encoding and decoding will be same as that for existing playfair cipher.[1]

6. SPECIAL SYMBOLS FREQUENCY ANALYSIS

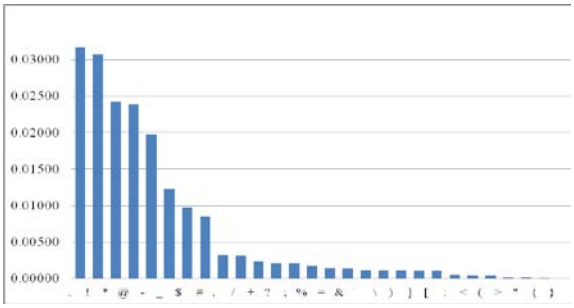


FIG 2 : SYMBOLS FREQUENCY ANALYSIS [4]

7. BRIEF DISCRIPTION OF OUR PROPOSAL

This extended play fair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword. We use a 8X8 Playfair cipher and hence it would be using 64 grids. First we insert a alphabetic character (A-Z), and then insert numerical value (0-9) and then insert special symbols according to frequency analysis.

The 8X8 metrics are shown in below

Alphabets
Numerical
Symbols

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	.	!	*	@
-	_	$	#	,	/	+	?
;	%	=	&	‘	\	)	[
]	:	<	(	>	“	{	}

In above metrics we apply a Simple Columnar Transposition Technique with Multiple Rounds.

HOW TO APPLY MULTIPLE ROUNDS

1. Using the keyword we arrange the keyword character from left to right and fill the 5X5 matrices with remaining character.
2. We mark the first row of matrices with 1, 2,3,4,5 according the dictionary order.
3. Rearranged the first marked column in first row which makes the first round.
4. In next round we mark the second row according to step 2.
5. Then fallow the steps 2 to 4.
6. Follow the steps 2 to 5 for 5 round.

Example:-

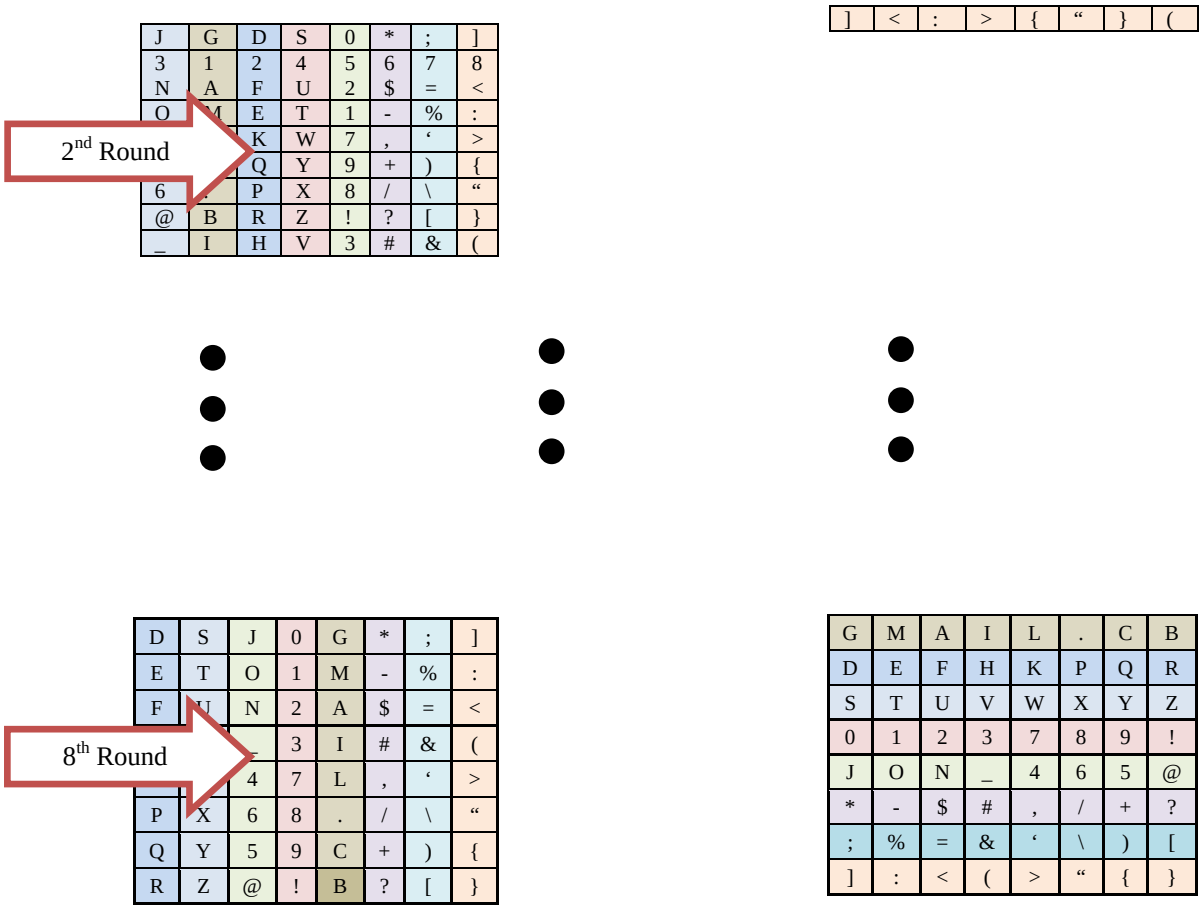
Key is "jon_465@gmail.com" the table becomes
Message is "A-143, City Center, Noida, India":
the table becomes using this key "jon_465@gmail.com"

1 J	3 O	2 N	8 _	4 4	6 6	5 5	7 @
G	M	A	I	L	.	C	B
D	E	F	H	K	P	Q	R
S	T	U	V	W	X	Y	Z
0	1	2	3	7	8	9	!
*	-	$	#	,	/	+	?
;	%	=	&	‘	\	)	[
]	:	<	(	>	“	{	}

1st Round

J	G	D	S	0	*	;	]
N	A	F	U	2	$	=	<
O	M	E	T	1	-	%	:
4	L	K	W	7	,	‘	>
5	C	Q	Y	9	+	)	{
6	.	P	X	8	/	\	“
@	B	R	Z	!	?	[	}
_	I	H	V	3	#	&	(

G	A	M	L	C	.	B	I
D	F	E	K	Q	P	R	H
J	N	O	4	5	6	@	_
S	U	T	W	Y	X	Z	V
0	2	1	7	9	8	!	3
*	$	-	,	+	/	?	#
;	=	%	‘	)	\	[	&



In above metrics we apply a Simple Columnar Transposition Technique with Multiple Rounds.

G	**M**	**A**	**I**	**L**	**.**	**C**	**B**
D	**E**	**F**	**H**	**K**	**P**	**Q**	**R**
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
0	**1**	**2**	**3**	**7**	**8**	**9**	**!**
J	**O**	**N**	**_**	**4**	**6**	**5**	**@**
*****	**-**	**$**	**#**	**,**	**/**	**+**	**?**
;	**%**	**=**	**&**	**‘**	****	**)**	**[**
]	**:**	**<**	**(**	**>**	**“**	**{**	**}**

Message is "A-143, City Center, Noida, India": becomes

Plain Text	A-	14	3,	CI	TY	CE	NT	ER	,N	OI	DA	,I	ND	IA
Cipher Text	M$	7O	7#	BL	UZ	MQ	OU	FD	$4	-M	FG	#L	JF	LI

Cipher text:- M$7O7#BLUZMQOUFD$4-MFG#LJFLI

8. RESULT

In this paper we enhanced 8X8 Playfair Cipher Technique with SCTTMR is observed that, it can be used for the plaintext with Multiple Rounds which makes the encryption complex and difficult to identify individual diagram. We

arranged symbols in Proper manner according to frequency analysis.

9. ADVANTAGE OF PRAPOSED PLAYFAIR TECHNIQUE

- We can Encrypt & Decrypt any type of plain text (Alphabetical, Numerical & Special Symbols)
- Identification of individual diagrams is difficult.
- Frequency analysis difficult.

10. CONCLUSION

In this paper, we have analyzed the extended Playfair 8*8 matrix. To solve the demerits in Playfair we have proposed and explained methods with examples. For this, we provide multiple rounds which make the complex encryption. Finally we named it as: '**A Modified Version of Extended Playfair Cipher (8X8)'**. The present version of the play fair technique will consider only text in English for conversion; we can also extend it to numbers and symbols for wide range of use.

11. REFRENCES

[1] Shiv Shakti Srivastava, Nitin Gupta, A Novel Approach to Security using Extended Playfair Cipher, International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011.

[2] 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

[3] Ravindra Babu Kallam, Dr.A. Vinaya Babu, Dr. S. Udaya Kumar, Sikharam Swetha, An Improved Playfair Cipher Cryptographic Substitution Algorithm,Volume 2, No. 1, Jan-Feb 2011 International Journal of Advanced Research in Computer Science, ISSN No. 0976-5697

[4] http://reusablesec.blogspot.in/2009/05/character-frequency-analysis-info.html

[5] http://en.wikipedia.org/wiki/Playfair_cipher.

[6] http://en.wikipedia.org/wiki/Cryptography

[7] Atul Kahate, Cryptography and Network Security, Second Edition, the McGraw-Hill Companies.

[8] William Stallings, Cryptography and Network Security, Prentice Hall of India Private Limited, New Delhi.