An Extension to Traditional Playfair Cryptographic Method

Ravindra Babu K[1], S. Uday Kumar [2], A. Vinay Babu [3], I.V.N.S Aditya[4] , P. Komuraiah[5]
[1]Research Scholar (JTNUH) & Professor in CSE, VITS SET, Kareemnagar, AP, India.
[2]Deputy Director, Professor in CSE. SNIST, JNTUH. Hyderabad, Andhra Pradesh, India.
[3]Director, Admissions, Jawaharlal Nehru Technological University, Hyderabad, Andhra Pradesh, India.
[4]Computer Science & Engineering, AZCET, Mancherial. [5]HOD IT, VITS SET, Kareemnagar, AP, India.

ABSTRACT
The theme of our research is to provide security for the data that contains alphanumeric values during its transmission. The best known multiple letter encryption cipher is the play fair, which treats the plain text as single units and translates these units into cipher text. It is highly difficult to the intruder to understand or to decrypt the cipher text.

In this we discussed about the existing play fair algorithm, its merits and demerits. The existing play fair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword. This algorithm can only allow the text that contains alphabets only. For this we have proposed an enhancement to the existing algorithm, that a 6 X 6 matrix can be constructed.

General Terms
Encryption, Decryption, Plaintext, Cipher text.

Keywords
Substitution, Transposition.

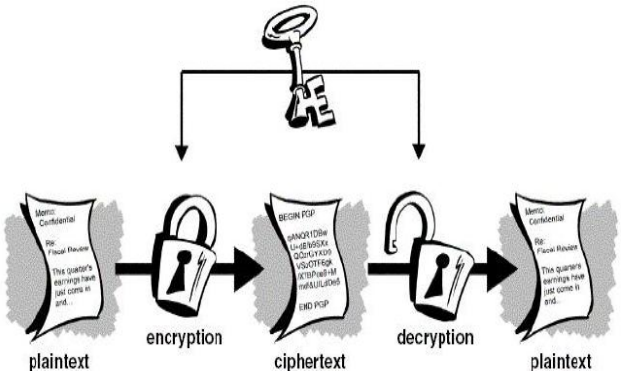
1. INTRODUCTION
In order to provide security to the information that is to be transmitted from sender to receiver we have several methods. The well known and highly used method for protecting the data during its transmission across the network is encryption.

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. [8]

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. [2]

The play fair cipher algorithm is based on the use of 5 X 5 matrix of letters constructed using a keyword. The matrix is constructed by filling the letters of keyword from left to right and top to bottom and filling in the remainder of matrix with the remaining alphabetic order. This algorithm can only allow the plain text containing alphabets, for this we have proposed an enhancement to the existing using a 6 X 6 matrix and that can allow the plain text containing of alphanumeric values. [3]

Fig 1: General cryptographic system.



2. EXISTING TECHNIQUES
All cryptographic algorithms are based on two general principals: 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.[7][1]

2.1 Transposition Cipher
These ciphers are block ciphers, which changes the position of particular characters or bits of the input block. For the encryption, the plaintext is broken into n symbols and a key specifies one of (n!-1) possible permutations. The deciphering is accomplished by using an inverse permutation which restores the original sequence. [8]

Transposition ciphers preserve the frequency distribution of single letters destroy the diagram and higher-order distributions.

These techniques are also combined with other ciphers to produce a more secure product cipher. The simplest such cipher is thee rail fence technique, in which the plain text is written down as a sequence of diagonals and then read off as a sequence of rows.

For example, to encipher the message—"**we are discovered flee at once** "with a rail fence of depth 3, we write the following

```
W . . . E . . . C . . . R . . . L . . . T . . . . E
. E . R . D . S . O . E . E . F . E . A . O . . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

The encrypted message:WECRLTEERDSOEEFEAOCAIVDEN

A more complex scheme is to write the message in a rectangle, row by row and read the message column. The order of the columns then becomes the key to the algorithm.

Example:

Key: 4 3 1 2 5 6 7

Plain text: a t t a c k p

o s t p o n e

d u n t i l t

w o a m x y z

2.2 Substitution Ciphers

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plain text is a sequence of bits then substitution involves replacing plaintext bit patterns with ciphertext bits patterns.

The well known use of a substitution cipher and the simplest was invented by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. [4]

For example:

Plaintext: task completed

Ciphertext: wdvn frpsohwhg

In this technique alphabets are wrapped around for the alphabets x, y and z so that the letter following Z is A.

We can define the transformation by listing all possibilities, as follows

Plain:

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

Cipher:

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

3. EXISTING PLAYFAIR ALGORITHM

The existing play fair cipher algorithm is based on with use of 5 X 5 matrix of letters constructed using a keyword. In this a keyword 'MONARCHY' is used, the matrix is constructed by filling the letters of keyword from left to right and top to bottom and filling in the remainder of matrix with the remaining alphabetic order, as Table 1. [8]

Table1: Existing PlayFair 5X5 Matrix

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

In this the letters I/J count as one letter. Plain text is encrypted two letters at a time according to the rules:

Repeating plaintext letters that would fall in the same pair are separated with a filler letter, such as x, so that balloon would be enciphered as a ba lx lo on.

Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularity following the last. For example ar is encrypted as Rm.

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

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, hs becomes BP, and ea becomes IM(or JM, as the enciphered wishes). [5], [6]

3.1 Confines Observed in Existing algorithm

CASE 1:

This algorithm can only useful for the plain text containing of alphabets but it is failed for the plain text containing of alpha numeric values. That means the plain text that is to be encrypted can only have alphabets but should not contain digits or numbers.

Example: from1972

Here we can not encrypt the digits 1,2,7,9 with the existing playfair algorithm.

CASE 2:

The existing PlayFair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword. The 5 X 5 matrix can only allow 25 characters, hence the letters I/J count as one. If we encrypt the plain text which is having the letter I/J and when we decrypt the ciphertext at the receive end, the receiver will be under ambiguity whether to consider I or J in his text, because the meaning can be changed with the change of the letters.

Example: Major and Maior, the word 'Major' is an adjective where as Maior is a noun, hence the user may get ambiguity at the time of decipherment whether to chose Major or Maior.

To overcome the existing system limitations we have proposed an extension to existing PlayFair algorithm.

3.2 Brief Description of Our Proposal

This extended play fair algorithm is based on the use of a 6 X 6 matrix of letters constructed using a keyword. The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and the filling in the remainder of the matrix with the remaining letters in alphabetic order and digits in ascending order form 0 to 9 as shown in table 2.

The digits 0 to 9 can be placed next cells of the alphabet z in an ascending order. In this we have not counted I/J as one letter instead we are placing both I and J in two different cells in order to avoid the ambiguity to the user at the time of decipherment.

This algorithm can allow the plain text containing of alpha numeric values; hence the user can easily encrypt alpha numeric values efficiently.

The plain text containing contact numbers, date of birth, house numbers and other numerical values can be easily and efficiently encrypted using this algorithm.

Table 2: Proposed extended PlayFair 6X6 Matrix

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

We are providing an efficient solution to the above mentioned two problems as follows.

CASE 1:

The user may encrypt digits along with the characters through the Extended PlayFair cipher, because the extended algorithm using 6X6 matrix, which can allow even digits into it.

Example: Consider the plain text: from1972

Cipher text will be: CE CM 37 81

CASE 2:

In this we have not counted I and J as one letter instead we are placing both I and J in two different cells in order to avoid the ambiguity to the user at the time of decipherment.

Example: When the user encrypted the text 'Major', the same 'Major'will be obtained at the time of decipherment without any ambiguity.

4. RESULTS

Through this extended PlayFair algorithm we can encrypt the plain text containing alphanumeric values very efficiently. The user does not face any ambiguity at decipherment, because the characters i and j are placed in separate cells of the matrix.

5. CONCLUSION

Finally through this paper we have pointed the traditional PlayFair algorithm, its merits and demerits. In order to overcome the demerits, we have proposed an extension to traditional PlayFair cipher algorithm, can be used more efficiently even for the plain text containing of alphanumeric values.

6. ACKNOWLEDGMENTS

The first author would like to thank his beloved parents and family members for their overwhelming support all along. He also likes to thank the Chairmen Sri. Anada Rao, C.O.O Dr. Z. J. Khan and the Principal Prof. Venkatarami reddy, VITS SET for their overwhelming support all along.

7. REFERENCES

[1] Derek Bruff, Ph.D, The Playfair Cipher Revealed Wynne MLAS 280-07 Cryptography July 13, 2009.

[2] Dr. Bruff, Playfair Cipher. FYWS Cryptology October 27, 2010.

[3] Kallam Ravindra Babu, Dr. S.Udaya Kumar, Dr. A.Vinaya Babu, A Survey on Cryptography and Steganography Methods for Information Security. International Journal of Computer Applications (0975 – 8887) Volume 12– No.2, November 2010

[4] Samir Kumar Bandyopadhyay, Tuhin Utsab Paul and Avishek Raychoudhury, Genetic Algorithm Based Substitution Technique of Image Steganography. Volume 1, No. 5, December 2010. Journal of Global Research in Computer Science Research Paper.

[5] V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani, Modified Playfair Cipher Involving Interweaving and Iteration. International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December, 2009. 1793-8201.

[6] V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani, Modified Playfair Cipher for a Large Block of Plaintext. International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December, 2009.

[7] William Stallings, Cryptography and Network Security, 5th impression, 2008.

[8] Kallam Ravindra Babu, Dr. S.Udaya Kumar, Dr. A.Vinaya Babu, An improved Playfair Cipher Cryptographic Substitution Algorithm, IJARCS, Volume 2, No-1, January -February-2011,pages:211to214.