Vol 8. No. 2 Issue 2 – August, 2015
African Journal of Computing & ICT

www.ajocict.net

17×17 Matrix Play Fair Cipher Technique for Securing Confidential Information

Y. B. Zakariyau & L. J. Muhammad
Department of Mathematics & Computer Science
Federal University, Kashere
Gombe State, Nigeria,
baladada57@yahoo.com lawan.jibril@fukashe.edu.ng

A. Garba
Information Lab
School of Computer Science and Electronics Engineering,
Peking University
Beijing China
abbaggumel@pku.edu.cn

I.A. Mohammed
Department of Computer Science
Yobe State University
Damaturu, Yobe State, Nigeria
ibrahimsallau@gmail.com

ABSTRACT

In today's digital world cryptography is widely used to secure confidential information in order to provide the privacy for the intended sender and receiver by managing the message with the public key. In this paper we propose Matrix Play Fair Cipher which is more secure than the existing ones. This is because it has a maximum key length of 289 characters and this range of key size yields 83521 possible keys that are strong enough to withstand attacks and this makes it very difficult for the eavesdropper to get the information.

Keywords: Playfair Cipher, Cryptography, Authentication, Encryption, Decryption, Plaintext, Ciphertext, Symmetric Key.

African Journal of Computing & ICT Reference Format:
Y. B. Zakariyau, L. J. Muhammad, I.A. Garba & I.A. Mohammed (2015): 17×17 Matrix Play Fair Cipher Technique for Securing Confidential Information. Afr J. of Comp & ICTs. Vol 8, No. 2, Issue 2. Pp 5-8.

1. INTRODUCTION

The Play fair cipher is a symmetric encryption technique and was the first literal digraph substitution cipher [5][9]. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Play fair who promoted the use of the cipher. The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher. The Play fair 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 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. The play fair cipher is more complicated than the simple substitution cipher such as shift and affine.

In the Play fair cipher, there is no single translation of each letter of the alphabet, instead, letters are translated into other pairs of letters. Thus make it more secure than mono-alphabetic cipher.

2. RELATED WORKS

2.1 5 × 5 Matrix Play fair Algorithm

The existing playfair cipher working on 5 × 5 matrix is constructed with a keyword "CRYPTO". The Table 6 below shows the construction of 5 × 5 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 as shown in Table 1 below.

TABLE 1: A 5 × 5 Matrix Playfair

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

Source: [2]

In this algorithm, the letters I & J are counted as one character. It is seen that the rules of encryption applies a 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.

Therefore, the 5×5 playfair exhibit the following rules

i. 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.
ii. 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
iii. 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) [3].

It has also the following limitations

i. It considers the letters I and J as one character.
ii. 26 letters alone can take as keyword without duplicates.
iii. Space between two words in the plaintext is not considered as one character.
iv. It cannot use special characters and numbers.
v. It only used uppercase alphabets.
vi. A spare letter X is added when the plaintext word consists of odd number of character. In the decryption process this X is ignored.
vii. 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.
viii. X is used a filler letter while repeating letter falls in the same pair are separated.

The 5 × 5 playfair can be broken, given a few hundred letters because it has much of plaintext structure [5]

2.2 7 × 4 Matrix Play fair Algorithm

A keyword is used to construct 7 × 4 matrix using letters and symbols „*" and „#" which is the base for this Playfair Algorithm. The 7 × 4 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 below, the last cell is filled by the symbol "#" and the remaining cell that is before the last cell is filled by the symbol "*" [1].

TABLE 2: A 7 × 4 Matrix Playfair

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

Source: [1].

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

i. When same letters fall in a pair it adds * so that the message BALLS become BAL*LS.
ii. 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.

Therefore, the 7 × 4 matrix plafair has the following limitations

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

The 7 × 4 playfair can be broken, given a few hundred letters because it has much of plaintext structure [5]

2.3 6 × 6 Matrix Play fair Algorithm

This play fair algorithm is based on the use of a 6 × 6 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 8 [2]. 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 play fair 5 × 5 matrix are used to encrypt the plaintext as shown in the Table 3 below.

TABLE 3: A 6 × 6 Matrix Play fair

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	Y	0	1	2	3
4	5	6	7	8	9

Source: [2]

Therefore, the 6 × 6 matrix playfair has the following limitations

i. This 6 × 6 matrix can only take 36 characters as a keyword without duplicates.
ii. Space between two words in plaintext is not considered as one character.
iii. The matrix cannot accept special character.
iv. It is not case sensitive.
v. 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.
vi. 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 [1].

To encrypt the plaintext, the rules of 5 x 5 playfair were employed with the following modification:

i. If the pair of plaintext are same, then "] " will be used as filler.
ii. If a word consists of odd number of characters then, the character "] " is added to complete the pairs, because "] " character cannot affect the Plaintext at the time of decipherment.

3. PROPOSED 17×17 MATRIX PLAY FAIR CIPHER TECHNIQUE

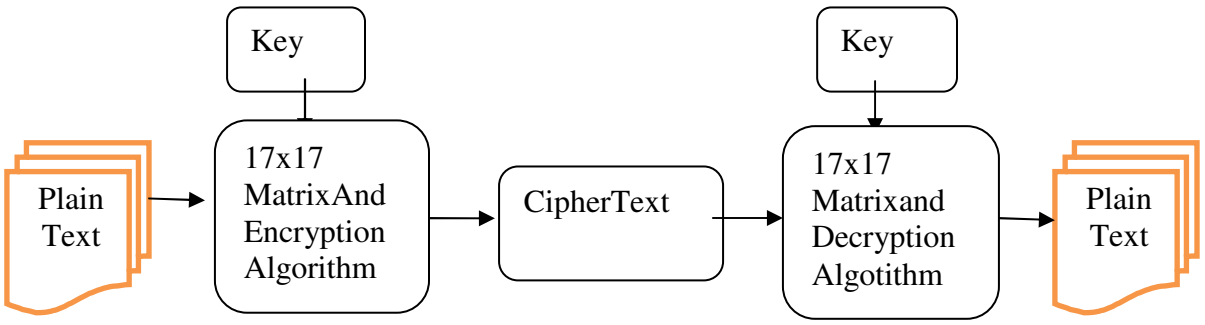

Figure 1 below shows the architecture of the proposed 17×17 Matrix Play fair Cipher Technique

3.1 Algorithm for Generating Matrix

i. Read a keyword.
ii. Eliminate the repeated characters in keyword.
iii. Construct a matrix by filling the character of keyword from left to right and top to bottom.
iv. Fill the reminder of matrix with the remaining characters from ASCII values 0 to 255.

3.2 Algorithms for Encryption

i. Read a plaintext.
ii. Divide the plaintext into pair of characters.
iii. Add the character "] " when odd number of character in the message.
iv. 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.
v. 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 column circularly following in the last.
vi. 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.

3.3 Algorithm for Decryption

i. If the pair of ciphertext falls in the same row of the matrix are replaced by the character to the left, with the first element of the row circularly following right.
ii. If the pair of ciphertext fall in the same column of the matrix are replaced by the character at top, with the bottom element of the column circularly following in the last.
iii. If the pair of ciphertext 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.

3.4 Advantages of the Proposed 17×17 Matrix Play fair Cipher Technique

i. It allows more than 64 characters as keyword.
ii. The user can easily encrypt and decrypt the combination of alphabets, numbers and special characters efficiently.
iii. The system can accept large keyword length, therefore, it is very difficult to find the Plaintext from Ciphertext without knowing the keyword.
iv. This algorithm adds the "] " character to complete the pair, because the "] character cannot affect the plaintext at the end of the word Or sentence.
v. The new system considers space between two words in plaintext as character.

4. CONCLUSION

In conclusion, the proposed 17×17 matrix Playfair cipher will be more secure than the existing ones. This is because the lager the matrix the longer the key sizes and this generally make encrypted text more difficult to be decrypted without the appropriate key. The technique has a maximum key length of 289 characters and this range of key size yields keys that are strong enough to withstand attacks using current technologies.

REFERENCES

[1] Aftab, A., Sehat, U., Ishtiaq, W. and Shah, K. (2011). Universal Playfair Cipher Using MXN Matrix. International Journal of Advanced Computer Science, 1(3), 113-117.
[2] Gamal, T. E.. A public key cryptosystem and a signature scheme based on discrete logarithms. In Advances in Cryptology –proceedings of CRYPTO 84, volume 196 of Lecture Notes in Computer Science, pages 10–18. Springer-Verlag New York, Inc., 1985
[3] Ravindra, B. K., Uday, S. K., Vinay, A. B., Aditya, I. V. and Komuraiah, P. (2011). An Extension to Traditional Playfair Cryptographic Method. International Journal of Computer Applications 17(5), 75 – 87.
[4] Stallings, W. (2006). Cryptography and Network Security: Principles and Practice (4th ed.). Prentice Hall: New York
[5] Stallings, W. (2004). Cryptography and Network Security – Principles and Practices (3rd ed.). Pearson Education: Boston
[6] Stallings, W. (2003), Cryptography and Network Security, (3rd ed.). Pearson Education: Boston
[7] Sinkov, A. (1998). Elementary Cryptanalysis: A Mathematical Approach (2nd ed.). USA, The Mathematical Association of America.