IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 12, December 2015.
www.ijiset.com
ISSN 2348 – 7968

Securing Message Transactions through Modified Playfair Cipher Technique

Yahaya Bala Zakariyau [1], Zirra Peter Buba[2], Gregory Maksha Wajiga[3]

[1]Department of Mathematics and Computer Science, Federal University, Kashere Gombe,0182, Nigeria.
[2]Department of Mathematics and Computer Science, Federal University, Kashere Gombe,0182, Nigeria.
[3]Department of Mathematics and Computer Science, Federal University of Technology Yola, 640284, Nigeria.

Abstract

Secured message transactions are the procedures to transfer the messages among the communicating parties with message confidentiality, message authentication, and message integrity. One of the several approaches used to implement the mentioned security services is Cryptography. In this paper we modified the 5×5 matrix Playfair cipher to 17×17 matrix Playfair cipher. The modified cipher was implemented using java programming language. The result obtained revealed that, the modified 17×17 matrix Playfair cipher is more secure than the existing ones. This is because the modified system 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 attack the message. As a result, this system is recommended to be used by banks for their online transaction and other institutions that deal with sensitive data and information.

.**General Terms**: Encryption, Decryption, Plaintext, Ciphertext.

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

1. INTRODUCTION

In today's world 'information' has become indispensable to both individuals and organizations. When a message is stored or transmitted, there should be some mechanism to protect that information from hacking. If information reaches the wrong person there might arise a lot of problems. Hence there is a need to hide the message so that a third person cannot find out the exact message. Hence Cryptography plays an important part in message transaction in today's world. The word cryptography comes from the Greek origin. It is a combination of two words Crypto and

ISSN 2348 – 7968

Graphy. Crypto means Secret and Graphy means writing [4].

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Classical cryptography offers an insight into how cryptography evolved over the years An early substitution cipher was the Caesar cipher, in which each letter in the plaintext was replaced by a letter some fixed number of positions further down the alphabet. Suetonius reports that Julius Caesar used it with a shift of three to communicate with his generals. Atbash is an example of an early Hebrew cipher. The earliest known use of cryptography is some carved ciphertext on stone in Egypt (ca 1900 BCE), but this may have been done for the amusement of literate observers rather than as a way of concealing information. Cryptography is recommended in the Kama Sutra (ca 400

(Stallings, 2006). 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).

ISSN 2348 – 7968

BCE) as a way for lovers to communicate without inconvenient discovery. The Greeks of Classical times are said to have known of ciphers (e.g., the scytale transposition cipher claimed to have been used by the Spartan military). Steganography (i.e., hiding even the existence of a message so as to keep it confidential) was also first developed in ancient times. An early example, from Herodotus, concealed a message—a tattoo on a slave's shaved head—under the regrown hair. Another Greek method was developed by Polybius (now called the "Polybius Square"). More modern examples of steganography include the use of invisible ink, microdots, and digital watermarks to conceal information.

Ciphertexts produced by a classical cipher (and some modern ciphers) always reveal The playfair cipher is more complicated than the simple substitution cipher such as shift and affine. In the Playfair cipher, there is no single translation of each letter of the alphabet, Instead, letters are translated into

statistical information about the plaintext, which can often be used to break them. After the discovery of frequency analysis perhaps by the Arab mathematician and polymath, Al-Kindi (also known as *Alkindus*), in the 9th century, nearly all such ciphers became more or less readily breakable by any informed attacker. Essentially all ciphers remained vulnerable to cryptanalysis using the frequency analysis technique until the development of the polyalphabetic cipher, most clearly by Leon Battista Alberti around the year 1467. He also invented what was probably the first automatic cipher device, a wheel which implemented a partial realization of his invention. Playfair cipher is one of the most well known polyalphabetic cipher. Thus the subject of the thesis was chosen. other pairs of letters. Thus make it more secure than mono-alphabetic cipher.

ISSN 2348 – 7968

2. PLAYFAIR CIPHER

2.1 Existing 5 × 5 Matrix Playfair 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 6 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.

ISSN 2348 – 7968

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 Existing 7 × 4 Matrix Playfair Algorithms

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 7 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.

ISSN 2348 – 7968

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.

2.3 Existing 6 × 6 Matrix Playfair Algorithm

This playfair 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 3 [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 playfair 5 × 5 matrix are used to encrypt the plaintext as shown in the Table 8 below

.

TABLE 3: A 6 × 6 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	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.
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].

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

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.

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

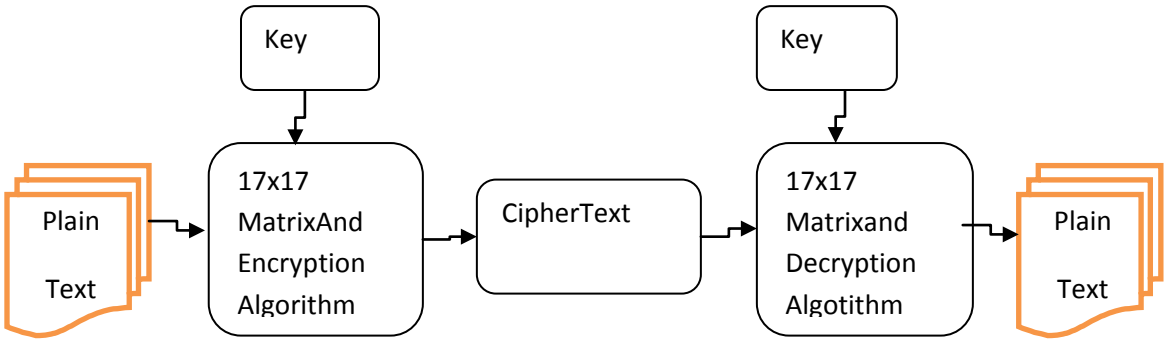
i. If the pair of plaintext are same, then "] " will be used as filler.

ISSN 2348 – 7968

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. Modified System Architecture

Figure 1 below shows the architecture of the new system



4. Figure 1: **Modified System Architecture**

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

ISSN 2348 – 7968

character is replaced by the character that lies in its own row and column occupied by the other plaintext character.

find the Plaintext from Ciphertext without knowing the keyword.

3.4 Advantages of the Modified System

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

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. RESULT

To overcome the drawbacks in the traditional Playfair Cipher as discussed in the last chapters, a modified playfair cipher which uses a 17 x 17 matrix has been developed using Java programming language.

The 17 x 17 matrix contains almost all the printable characters. This includes lowercase and uppercase alphabets, punctuation marks, numerical and special characters. The order of placement of different groups of characters can also be done so that the matrix formed by using the same secret keyword depends on the order of placement. This means that the ciphertext depends on the order of placement of different groups of characters. Below figures show the result obtained from the cipher.

Figure 2 below shows the input dialog for keyword where user is expected to type in his/her secrete keyword or sentence

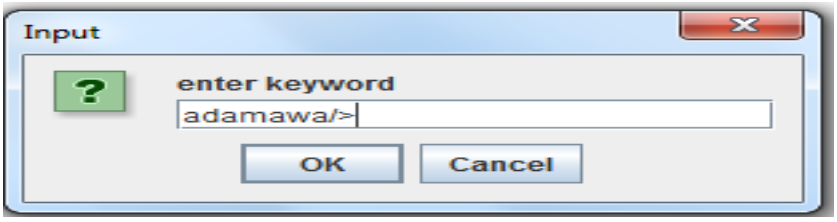


Figure 2: Input dialog for keyword

Figure 3 below shows the matrix generated based on the secrete key used:

ISSN 2348 – 7968

Figure 3: Matrix Generated

Figure 4 below shows the input dialog for plaintext where user is expected to type in his/ her plaintext:

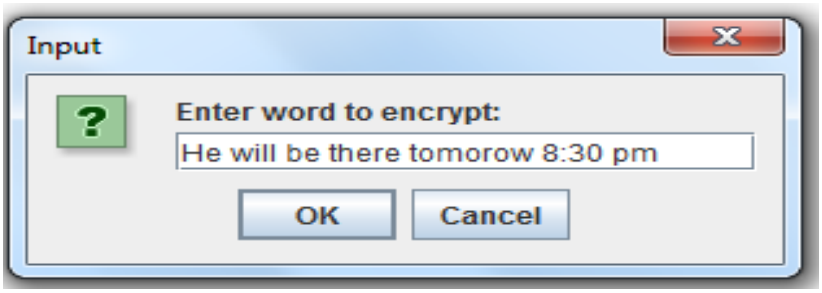


Figure 4: Input Dialog for Plaintext

Figure 5 below displays the encrypted text:

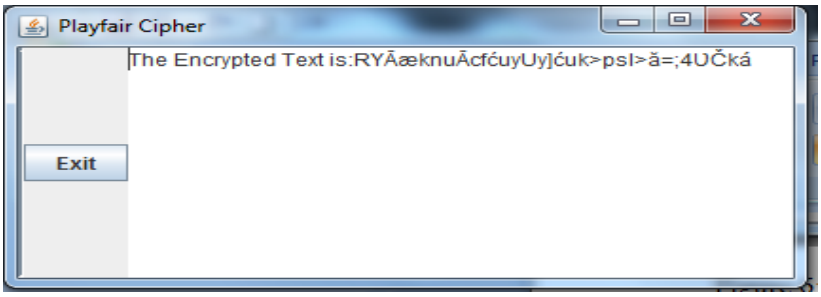


Figure 5: Encryption Output

(5) Figure 6 below displays the plaintext obtained from ciphertext:

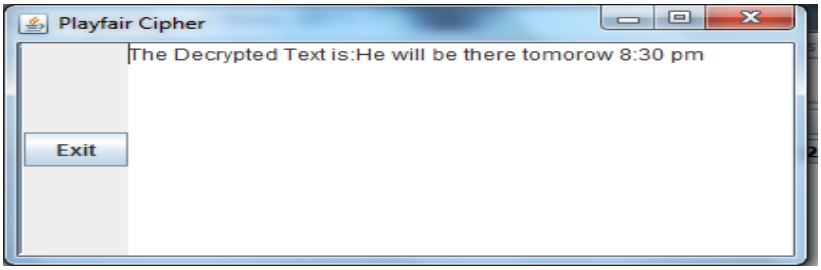


Figure 6: Decryption Output

5. DISCUSSION

Figure 3 above shows the matrix generated by the system based on the secrete keyword and it can be observed that the order of placement of characters in the matrix depends on the keyword used. And this is in conformity with the assertion of [2]. Who state that, the cryptographic system should only depend on the secrecy of the keys, and not on the secrecy of the encryption and decryption algorithms.

Figure 4 above shows the input dialog for plaintext. It can be observed that, the system can accept the combination of both numbers and alphabets to encrypt. Thus make the system more flexible.

Figure 5 above shows the encrypted message. It can be observed that, the character “e” which appears more frequent in the plaintext does not appear more frequent in the cipher text. And this is in conformity with the assertion of [6] who stated that, if the most frequently used letter in the plaintext does not appear to be the most frequently occurring one in the ciphertext then, the system is difficult to be attacked by frequency distribution Analysis.

6. CONCLUSION

In conclusion, the modified 17×17 matrix Playfair cipher is 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 decrypt without the appropriate key. This modified system 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

.

7. 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] Ravindra, B. K., Uday, S. K., Vinay, A. B., Aditya, I. V. and Komuraiah, P. (2011).

ISSN 2348 – 7968

An Extension to Traditional Playfair Cryptographic Method. *International Journal of Computer Applications* 17(5), 75 – 87.

[3] Stallings, W. (2006). *Cryptography and Network Security: Principles and Practice* (4th ed.). Prentice Hall: New York

[4] Stallings, W. (2004). *Cryptography and Network Security – Principles and Practices* (3rd ed.). Pearson Education: Boston

[5] Stallings, W. (2003), *Cryptography and Network Security, (*3rd ed.). Pearson Education: Boston

[6] Sinkov, A. (1998). *Elementary Cryptanalysis: A Mathematical Approach* (2nd ed.). USA The Mathematical Association of America.