

An Extended Algorithm based on PlayFair Cipher

Yanhong Shang

Computer Science Department, Tangshan Normal
University, Tangshan, China
E-mail: yh_shang@126.com

Lilei Lu

Computer Science Department, Tangshan Normal
University, Tangshan, China
E-mail: lu_li_lei@yahoo.com.cn

Abstract—This article proposed an improved solution to Playfair cipher algorithm. The algorithm extended former encrypting form from digram to integrated three letters. In this article the authors presented the improved encryption algorithm and finished its program in C programming language. At the end of the article, typical test data are displayed in order to testify the correctness of the algorithm.

Keywords—Playfair; encryption; algorithm

I. INTRODUCTION

With the development of Internet technology, Information Security is greatly focused on by people day after day. Cipher as an ancient technology is put on the agenda unavoidably. Although in recent cryptology perspective, the Playfair cipher system which widely used by American army and English Army during the World War I is not secure enough, its design fundamental can be mostly referenced in recent cipher. The authors of this article put forward an extended algorithm after researching the Playfair encryption process.

II. PLAYFAIR CIPHER ALGORITHM

The Playfair cipher algorithm regards digram in plaintext as one unit and transformed these units into integrated cryptograph letters. It uses a 5*5 matrix of letters for substitution. The matrix of letters is structured as following: select a keyword (key) to fill in it in alphabetic order from left to right and from top to bottom. During the process, the repeated letters appeared only once, that is, if a letter appeared for the second time, it is ignored and the remaining letters are filled in the matrix of letters in alphabetic order. The letter I and J are filled in the same position in the matrix of letters. In fact, the matrix of letters forms a table. Agree as follows: the first column of the table is also regarded as the last column which stands on the right, and the first row of the table is also regarded as the last row which stands at the bottom. When encrypting a couple plaintext letters such as P and Q, we deal with them separately as follows according to their different positions appeared in the matrix of letters:

(1) If P and Q are in the same row, the corresponding ciphertext is the letter which just stands on the right of P and Q.

(2) If P and Q are in the same column, the corresponding ciphertext is the letter which just stands at the bottom of P and Q.

(3) If P and Q are not in the same row and also not in the same column, at first we should form a regular rectangle using P and Q as diagonal, then we get two letters as the

corresponding ciphertext which stand at both ends in another diagonal. Of course, the encrypted letter and its plaintext letter (P or Q) stand in the same row.

(4) If P and Q are in the same position, then we insert the certain letter defined beforehand and then process.

(5) If the number of letters is odd, add the certain letter defined beforehand and then process.

Decryption process is the opposite process of encryption.

III. IMPROVED PLAYFAIR ALGORITHM

The existing Playfair cipher is based on digram and uses a 5*5 matrix of letters. Enlightened by this, we consider to using three letters as one unit to replace the original digram and using 3*3*3 cube of letters for substitution. The 3*3*3 cube of letters is constructed as follows: select a keyword (key) to fill in its every vertex, middle point of every edge, center point of every surface in alphabetic order from left to right and from top to bottom and from front to back. During the process, the repeated letters appeared just once, that is, if a letter appeared for the second time, it is ignored and the remaining letters are filled in the matrix of letters in alphabetic order.

When encrypting three letters in plaintext, we deal with every letter separately as follows according to their different position appeared in the cube of letters:

(1) When three letters in plaintext are in the same surface (here we define the surface as one of the six surfaces of the cube), the ciphertext contains all corresponding letters which lie on the opposite surface.

(2) When two of three letters in plaintext are in the same surface, the ciphertext contains two parts: one part includes the two corresponding letters which lie on the opposite surface compared with the coplanar plaintext letters; the other part includes the ciphertext of the noncoplanar letter which lie on the opposite surface center.

(3) When three letters can be viewed as belonging to two coplanar parts, the first appeared coplanar part is prior to the second coplanar part. If the two coplanar parts appear simultaneously, we consider them in an order from left to right, top to bottom and front to back.

(4) If three letters in plaintext are noncoplanar one another, the ciphertext contains symmetrical letter of every plaintext letter, which lie on the opposite surface.

(5) If two letters in plaintext are same and adjacent, insert the certain letter defined beforehand between them (consider selecting the letter which appears less frequently in alphabet).

(6) If the number of letters in plaintext can not be divided by three, add one or two certain letters defined beforehand at the end of plaintext till the number of letters in plaintext can be divided by three (consider selecting the letter which appears less frequently in alphabet).

Three different situations about encryption position are listed as Fig.1, Fig.2, Fig.3.

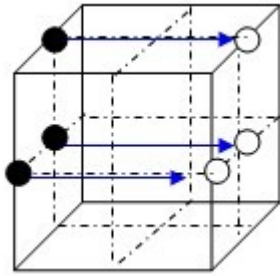


Figure 1 three coplanar letters

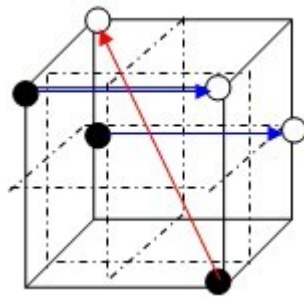


Figure 2 two coplanar letters

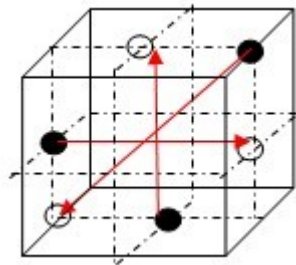


Figure 3 no coplanar letters

Among the below figures, ● represents the position of plaintext letter to be encrypted, ○ represents the position of encrypted letter.

Because decryption process is the opposite process of encryption, we do not discuss here again.

IV. EXPERIMENTAL DATA

We choose following data to encrypt. The plaintext to be encrypted is: Attack on Pearl Harbor tonight.

Three-letter plaintext groups are: Atz tac kon Pea rlH arb ort oni ght

Here we insert the defined letter “z” between two “t” in plaintext.

The key is: master key.

They are filled in the cube of letters as following Fig.4.

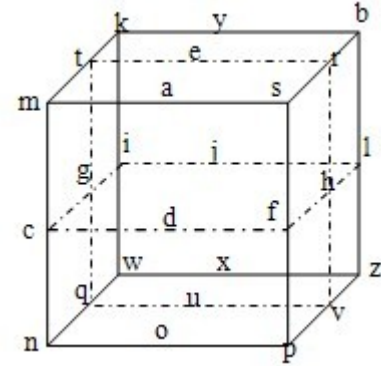


Figure 4 filled cube of letters

According to the above extended algorithm, we get the ciphertext as follows: oqm qol pxw k uo tig ovz yvq amf hgr.

The C language program about this encryption algorithm is as follows:

```
void search(int i,char d[26],char c[3][3][3])
//to find corresponding positions in three-dimensional
matrix for every letter in the plaintext
{int j = 0;
int i1, i2, i3;
int x[3], y[3], z[3];

while( j < i )
{for(i1=0; i1<3; i1++)
for(i2=0; i2<3; i2++)
for(i3=0; i3<3; i3++)
if( d[j] == c[i1][i2][i3] )
{ x[0] = i1;
x[1] = i2;
x[2] = i3; }
for(i1=0; i1<3; i1++)
for(i2=0; i2<3; i2++)
for(i3=0; i3<3; i3++)
if( d[j+1] == c[i1][i2][i3] )
{ y[0] = i1;
y[1] = i2;
y[2] = i3; }
for(i1=0; i1<3; i1++)
for(i2=0; i2<3; i2++)
for(i3=0; i3<3; i3++)
if( d[j+2] == c[i1][i2][i3] )
{ z[0] = i1;
z[1] = i2;
z[2] = i3; }
judge(x, y, z); //to judge if three letters are coplanar
```

```
display(x, y, z, c); //output (three letters in the same
group)
j = j + 3; }}
```

V. CONCLUSIONS

This article discusses an extended algorithm based on Playfair cipher system. Digram to be encrypted is changed into three letters which are viewed as one unit in the improved encryption algorithm. The algorithm is programmed in C programming language. The experimental data shows the

effectiveness of this extended algorithm. Next, we will analyze the algorithm in detail revolving around its merit and demerits and discuss whether it is effective to encryption of Chinese.

REFERENCES

- [1] Zhang Futai. Cryptology Tutorial. Wuhan University Publishing House.
- [2] Yangbo. Modern Cryptology. Tsing Hua University Publishing House.
- [3] Chen Lusheng. Modern Cryptology. Science Press.