# One Algorithm to Cipher Messages in Columnar and Fixed Period-d Transposition Cipher

**J.N. Jassim, H. J. Muhsen**
**Computer Science, College of Education ,Ibn Al-Haitham**
**University of Baghdad**

## Abstract

One of ciphering systems depends on transposition of letters in plain text to generate cipher text. The programming of transposition depends mainly on 2-dimension matrix in either methods but the difference is in columnar .We print columns in the matrix according to their numbers in key but in the fixed, the cipher text will be obtained by printing matrix by rows.

## Introduction

Many solvers shy away from transposition, because such problems do not give quite as much opportunity for analytical reasoning. Solutions often depend upon exhaustive trails of various widths, or finding the exact method of inscription.

In this research we will discuss two types of transposition ciphering, they are columnar transposition and fixed period-d and make comparisons between them in the ways of ciphering and deciphering in methods and programming , they seem that one of them as part of the other.

**Definition**

Transposition ciphers rearrange characters according to some scheme. This rearrangement was classically done with the aid of some type of geometric figure like rectangle.
Encipherment proceeded into two steps as shown next:-

Plain text ----------→ figure ----------→ cipher text
Write-in take-off

**First step**

The plain text was written into the figure according to some "write-in" path.

**Second step**

The cipher text was taken off the figure according to some "take-off" path.

These two steps proceed according to key; this key consisted of the figure together with the write-in and take-off paths. The geometrical figure was often a 2-dimension array (matrix).

**Types of transposition ciphers**

There are many types of transposition ciphers:-

1- Columnar transposition.
2- Double columnar transposition.
3- Monoliteral transposition.
4- Polyliteral transposition.
5- Message reversal.
6- Route transposition.

**Columnar transposition**

The plain text was written into a matrix by rows. The cipher text is obtained by taking off the columns in some order.

The most common method is merely to write the message (from left to right),on a prearranged width and then prepared a transposed version by taking the columns off in some order (by a numerical key).

The practical consideration dictates that we should have no great number of rows in excess to the number of columns. For example a message of 50 letters might be put into a format from 6 to 8 wide and 7 to 9 deep, for instance 6 rows and 9 columns or other way around, or 7 * 8 in either directions. For example the plain text "ship equipment on the fourth of July " ,this massage consists of 30 letters , it may take many sizes of rows * columns 10*3 , 3*10 , 6*5 , 5*6 , 2*15 ,15*2 . If the text consists of odd number of letters (e.g. 29) then there will be added another letter like (X) to the end of plain text.

If we arrange this text according to columns then the text will be 6*5

| No. of columns | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| No. | 1 | s | u | t | f | o |
| Of | 2 | h | I | o | o | f |
| Rows | 3 | I | p | n | u | j |
| | 4 | p | m | t | r | u |
| | 5 | e | e | h | t | l |
| | 6 | q | n | e | h | y |

If we arrange this text according to rows then the figure will be 6*5

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | s | h | I | p | e |
| 2 | q | u | I | p | m |
| 3 | e | n | t | o | n |
| 4 | t | h | e | f | o |
| 5 | u | r | t | h | o |
| 6 | f | j | u | l | y |

In the second figure if we have key = 24513 then we will copy message by columns such as this:-

Reading column 2 as first column, then reading column 4 as second, then column 5, then column 1 and last column 3.

Then the cipher text will be:-

" hunhrj ppofhl emnooy sqetuf iitetu"

Col. 2 col. 4 col. 5 col. 1 col.3

Here we change only the order but the frequency count on the cipher version is the same as the plain text.

In the previous example, we take completely filled rectangle but if the text is "this is transposition "it will take the following figure:-

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | t | h | I | s |
| 2 | I | s | t | r |
| 3 | a | n | s | p |
| 4 | o | s | I | t |
| 5 | I | o | n | |

In this text there are some columns 5 in deep while others are only 4 , the rectangle is not completely filled ,so we will add another letter "X" to the text which would make the solution more difficult.

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | t | h | I | s |
| 2 | I | s | t | r |
| 3 | a | n | s | p |
| 4 | o | s | I | t |
| 5 | I | o | n | x |

There is another shape of columnar transposition which is fixed period-d

Fixed period-d

In this type of cipher the characters are permuted in a plain text with a fixed period-d. The plain text will be divided into many blocks of d characters.

Let Zd be the integers 1 through d, and let

F:Zd Zd be a permutation over Zd .

The key for the cipher is given by the pair k= (d, f). Successive blocks of d characters are enciphered by permuting the characters according to f. Thus, a plain text message

M=m1 …..md md+1 ….mzd

Is enciphered as:-

E(k) = mf(1) …..mf(d) mf(d+1) …….md+f(d)

For example:-

Suppose that d=4 and F gives the permutation:-

I : 1 2 3 4

F(i): 2 4 1 3

Thus the first plain text character is moved to the third position in the cipher text, the second plain text character to first position, the third plain text character is moved to the fourth position and fourth character is moved to second position in cipher text.

For example the following plain text will be enciphered as follows:-

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

“m y f i r s t p l a i n t e x t“

When d=4 and key=2413 then

M = m y f i r s t p l a i n t e x t

Ek( M )= y i m f s p r t a n t i e t t x

This plain text is broken into groups of four letters, the actual cipher text would be transmitted as a continuous stream of characters to hide the period.

Choosing numerical key in transposition cipher.

The numerical key is formed in many ways ,these are some:-

1- Choosing some keywords ( for example LONDON ) if the columns are only four , then eliminate the similar letters if these letters are the same . In our example ON will be eliminated .The other letters ( LOND ) will be numerated as their order in alphabet , we would put 1 under the lowest letter in alphabetical ( in LOND letter D will take number 1 , 2 would be placed under the next earliest letter L ,similarly 3 goes under N and 4 under O) then the key will be LOND-----→2431 .
2- Choosing some random number, its rank equals to the number of columns in matrix or its equals to the period d. To determine the expected number of character required to break a permutation cipher with period d, there are d! Possible arrangements of d characters.

**Programming and execution**

We can use only one program to obtain cipher text in both methods columnar and fixed period-d for many reasons which are:-

1- Each of them depends on permutation of letters with others in the same text.

2- Each block in fixed period-d is one row in matrix of columnar, then if we apply the key function on all matrix, it seems as if we apply the same key function on all blocks of the fixed as period-d, if the long of d is equal to the number of columns in matrix as we will see in the following program and execution of ciphering plain message in both methods in one execution.

Then we can use the same program for both methods if we have the same number of columns and long of period d, if columns are 4 and each block with 4 letters, and have the same numerical key

The algorithme and flowchart

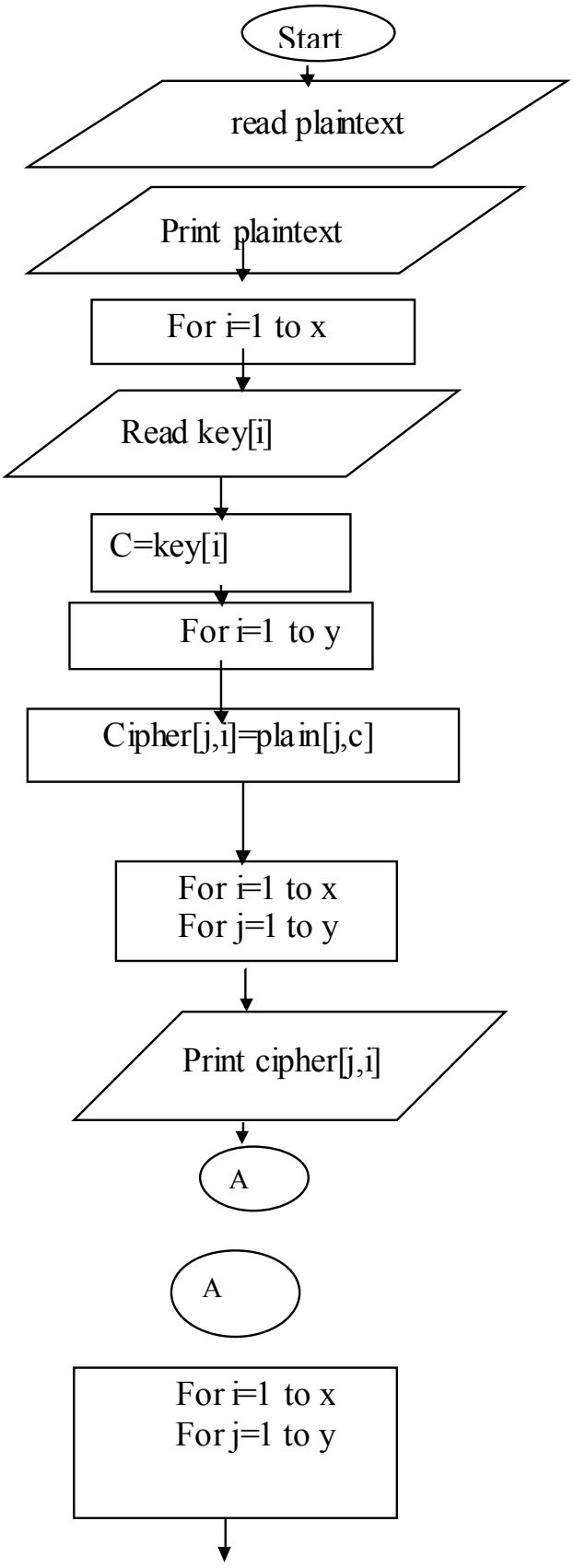
1-start
2-read plain text {x columns, y rows}
3-print plain text
4- read key[1..x]
5- for i=1 to x
6 c=key[i]
7- for j=1 to y
8- ciphertext[j,i]=plaintext[j,c]
9- for i=1 to x
10- for j=1 to y
11- print ciphertext[j,i]
12- for i=1 to y
13-for j=1 to x
14- print ciphertext[I,j]
15- end

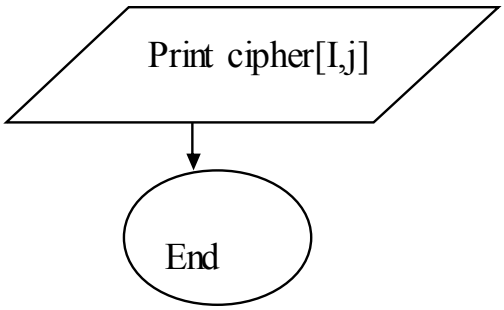
When we execute this algorithm, it will give us results in both ways columnar and fixed period-d.

```
program to cipher plain text
enter your plain text without spaces
type # at end of text
helloeverybodyintheworlds#
enter no. of columns:4
enter no. of rows :6
the matrix of plain text is:6*4
    h  e  l  l
    o  e  v  e
    r  y  b  o
    d  y  i  n
    t  h  e  w
    o  r  l  d

---------------------------------
enter the key of 4 numbers
3 1 2 4

the cipher text in simple columnar transposition is:
  lvbiel  hordto  eeyyhr  leonud
the cipher text in fixed period d is:
  lhel   voee   bryo   idyn   ethw   lord
```


Start
read plaintext
Print plaintext
For i=1 to x
Read key[i]
C=key[i]
For i=1 to y
Cipher[j,i]=plain[j,c]
For i=1 to x
For j=1 to y
Print cipher[j,i]
A
A
For i=1 to x
For j=1 to y




**Development of program**

This program is simple, it treats only basic idea of both methods of ciphering. We can add many features to it like:-

1- The user can choose which one of cipher he wants either columnar or fixed period-d.
2- The user reads only his message and the program will compute the size of matrix, number of columns and rows and size of block for period d.
3- Decipher of receiving cipher message and output plain message.
4- Open files for output ciphering messages and deciphering messages.

**Differences and Similarities**

1- Like columnar transposition, periodic permutation ciphers can be viewed as transpositions of the columns of a matrix in which the plain text is written by rows and one column.
2- With periodic permutations, the cipher text is taken off by rows, this is more efficient for computer application because each row (block ) can be enciphered and deciphered independently.
3- With columnar transposition the entire matrix must be generated for enciphering and deciphering.
4- Each block in fixed period-d represents one row in columnar transposition, then if we apply the permutation on block according to key, this is similar to applying key on all rows in matrix, as we see there is only one cipher matrix for both.
5- The difference between the two ways only in printing results, in columnar we print column after column according to key and in fixed period-d we print matrix row by row.

# References

1- Denning,D.E.R. (1983) Cryptography & data security, Purclue university
2- Frank ,W.Lewis, (1992) Solving Cipher Problems Aegean park press California.
3- Beker,H.;Piper,F.,1998 Cipher systems :The protection of communication
4- مقدمة الى امن المعلومات , بروس بوزورث; ترجمة الدبوني مبثم محمد; سليمان اديب حمدون ; بدرخان، ستار
طبع الدار العربية للطباعة –بغداد

مجلة ابن الهيثم للعلوم الصرفة والتطبيقية المجلد22 (2) 2009

# خوارزمية واحدة لتشفير الرسائل بطريقتي الابدال العمودي البسيط والفترة الثابتة-d

جنان نصيف جاسم ، هيفاء جاسم محسن
قسم الحاسبات،كلية التربية- ابن الهيثم ،جامعة بغداد

## الخلاصة

حيث dالابدال العمودي هو احدى طرق تشفير الرسائل ومن انواعه الابدال العمودي البسيط والفترة الثابتة ان فكرة البحث تعتمد على تصميم برنامج واحد او خوارزمية واحدة لتشفير النصوص بكلا الطريقتين واظهار النتائج للنص المشفر