Experiment No. 9

Write a program to implement simple columnar transposition technique.

I. Minimum Theoretical Background

Transposition Technique doesn't replace alphabets from Plaintext , It perform some permutation on Plaintext.

Transposition cipher types:

1. Rail Fence cipher.
2. Route cipher.
3. Columnar transposition.
4. Double transposition.
5. Myszkowski transposition.
6. Disrupted transposition.
7. Grilles.
8. Scytale.

Columnar Transposition:

In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword.

For example, the keyword ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the keyword ZEBRAS and the message WE ARE DISCOVERED. FLEE AT ONCE. In a regular columnar transposition, we write this into the grid as follows:

6 3 2 4 1 5

W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U

Providing five nulls (QKJEU), these letters can be randomly selected as they just fill out the incomplete columns and are not part of the message. The cipher text is then read off as:

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE
In the irregular case, the columns are not completed by nulls:
6 3 2 4 1 5

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

E

This results in the following cipher text:

EVLNA CDTES EAROF ODEEC WIREE
To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length. Then he can write the message out in columns again, and then re-order the columns by reforming the key word.

In a variation, the message is blocked into segments that are the key length long and to each segment the same permutation (given by the key) is applied. This is equivalent to a columnar transposition where the read-out is by rows instead of columns.

Columnar transposition continued to be used for serious purposes as a component of more complex ciphers at least into the 1950s.

Code:

```
#include<stdio.h>
int check(int x,int y)
{
int a,b,c;
if(x%y==0)
return 0;
a=x/y;
b=y*(a+1);
c=b-x;
return c;
}
void main()
{
int l1,i,d,j;
printf("\nEnter the length of the key. ");
scanf("%d",&l1);
int sequence[l1];
printf("\nEnter the sequence key. ");
for(i=0;i<l1;++i)
{
scanf("%d",&sequence[i]);
}
int order[l1];
for(i=1;i<=l1;++i)
{
for(j=0;j<l1;++j)
{
if(sequence[j]==i)
order[i-1]=j;
}
}
printf("\nEnter the depth. ");
scanf("%d",&d);
int l2;
printf("\nEnter the length of String without spaces . ");
scanf("%d",&l2);
int temp1=check(l2,l1);
int r=(l2+temp1)/l1;
```

```
char p[l2+temp1];
char p1[r][l1];
//char p2[r][l1];
if(temp1>0)
printf("\nYou need to enter %d bogus characters.So enter total %d characters.
",temp1,(l2+temp1));

else
printf("\nEnter the string. ");
for(i=-1;i<(l2+temp1);++i)
{
scanf("%c",&p[i]);
}
int count=0;
while(d>0)
{
count=0;
for(i=0;i<r;++i)
{
for(j=0;j<l1;++j)
{
p1[i][j]=p[count];
count=count+1;
}
}
printf("\n\n\n");
for(i=0;i<r;++i)
{
for(j=0;j<l1;++j)
{
printf("%c ",p1[i][j]);
}
printf("\n");
}
count=0;
for(i=0;i<l1;++i)
{
for(j=0;j<r;++j)
{
p[count]=p1[j][order[i]];
count=count+1;
}
}
```

```
for (i=0;i<(l2+temp1);++i)
printf("%c ",p[i]);
d=d-1;
}
}
```

Output:

Enter the length of the key. 7

Enter the sequence key. 4 3 1 2 5 6 7
Enter the depth. 2
Enter the length of String without spaces . 23

You need to enter 5 bogus characters.So enter total 28 characters. attackpostponeduntiltwoamxyz

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

t t n a a p t m t s u o a o d w c o i x k n l y p e t z
t t n a a p t
m t s u o a o
d w c o i x k
n l y p e t z
n s c y a u o p t t w l t m d n a o i e p a x t t o k z

II. Conclusion

We have conclude that how should we perform Simple Columnar Transposition.

III. Exercise

1. What is columnar transposition?

2. How does transposition cipher work?

3. Why a pure transposition cipher is easily recognized?

4. What is simple transposition?

5. What is Ciphers?

6. What is Cryptanalysis?

7. What is Resources?

Answers

……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....
……....

…….

…….

…….

…….

…….

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

……..

Marks obtained			Dated signature of Teacher
Process Related (15)	**Product Related (10)**	**Total(25)**	