ROW TRANSPOSITION CIPHER IMPLEMENTATION

Shiyun hu Student ID 1298223 New York Institute of Technology shu10@nyit.edu Jun Jie Wu Student ID 1298381 New York Institute of Technology jwu72@nyit.edu Leonardo Amorim de Lemos Student ID 1292678 New York Institute of Technology lamori01@nyit.edu

March 1, 2022

Abstract

The cipher appeared thousands of years ago but was heavily exploited from the 2nd World War. In our group project, we have learn one of the cryptography method in the transposition ciphers filed called Row Transposition cipher. Our group implements the Row Transposition cipher's encryption and decryption algorithm by using Java programming language.

I. Introduction

row transposition matrix(Figure 3).

Take the key 'NYITV' as an example (Figure

1), the algorithm uses the 26 English letters

to find the number sequence '14023'. Then,

the algorithm arranges the columns by the

order of this number sequence. The encryption

algorithm writes letters of message out in rows

over a specified number of columns which

equals the key length '5' (Figure 2). Then,

reorder columns in the matrix (Figure 3).

He cipher appeared thousands of years ago but was heavily exploited from the 2nd World War in which information exchanged between enemies, even encrypted, was intercepted and deciphered. There are two widely explored types of encryptions (transposition and substitution) that, when worked independently, can be solved quickly. Still, protocols have been created and improved that fundamentally use these two techniques repetitively. By definition, transposition cipher changes the plaintext order and rearranges to get ciphertext. In this group project, we used "Row Transposition Cipher," where you write your plaintext in rows of fixed length (key size), and we write by columns in key order. We can use the procedure to enhance the complexity of a more complex cipher-text.

Figure 1: Task1-Encryption Sequence Order

II. ENCRYPTION IMPLEMENTATION

To implement the row transposition encryption, we utilize the key as a sequence to switch the columns in a two-dimension matrix to form a

The reorder sequence is '20341' for decryption in the columns of 2D Matrix.

0	1	2	3	4		
N	Υ	I	Т	٧		
1	4	0	2	3		
R	Е	0	R	D	Е	R
2	0	3	4	1		

Figure 2: Task2-Decryption Sequence Order

Regards for the current assignment, the empty space would be replaced by the capital letter 'X'. Append the rows to form the ciphertext.

N	Υ	1	Т	٧
2	0	3	4	1
С	r	у	р	t
О	1	o	g	у
i	s	t	h	е
p	r	а	С	t
i	С	е	а	n
d	s	t	u	d
у	o	f	t	е
С	h	n	i	q
u	е	s	f	0
r	s	е	С	u
r	е	С	o	m
m	u	n	i	С
а	t	i	o	n
i	n	t	h	е
p	r	е	s	е
n	С	е	0	f
t	h	i	r	d
p	а	r	t	i
е	s	С	а	1
1	е	d	а	d
V	е	r	S	а

Figure 3: *Task1-Message Matrix*

The following figure 4 displays the encrypted message.

yotaetfnsecniteeircdrecoipidycurrm aipntpelvrpghcautifcoiohsortaasstye tndeqoumcneefdildaXrlsrcsoheseut nrchaseei

Figure 4: *Task1-Encrypted Message*

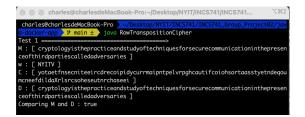


Figure 5: Task1-Output

Figure 5 shows the result of the encrypted plaintext. Further, we use the decrytion algorithm to double check the answer. The result match to the original text.

III. DECRYPTION IMPLEMENTATION

The decryption algorithm put the letters in columns by the key order '14023'; however, as we fill the columns in the order '20341'. Take '0' as an example, The '0' is filled up 1st in the 2nd column. The algorithm first writes the encrypted message out in rows. Then, it reads off the message by recording columns.

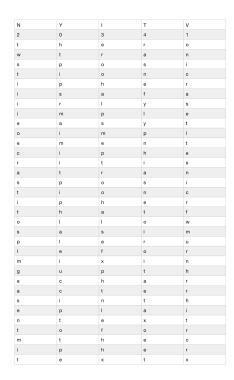


Figure 6: Task2-Decrypted Row Transposition Matrix

therowtranspositioncipherisafairlysi mpleeasytoimplementcipheritisatran spositioncipherthatfollowsasimpleru leformixingupthecharactersintheplai ntexttoformtheciphertextx

Figure 7: Task2-Decrypted Message

The above is the declassified information.

The first part finds the decoding sequence from the key 'NYITV'. Then, write the encrypted message into a 2D RowTranspositionMatrix. Next, use the RowTranspositionMatrix to record the rearrangement of the RowTranspositionMatrix. In the last step, utilize the StringBuilder to build the encrypted message line by line through the RowMatrix. The following is the pseudocode for the row transposition cipher algorithm:

```
Row Transposition Decryption Algorithm 1
```

```
input: 'w': Key and 'C' Encrypted plain-text
output: Decrypted plain-text
 1: function RTCDECRYPTION(w, C)
         keylen \leftarrow w.length()
 2:
         keyArray \leftarrow key.toCharArray()
 3:
 4:
         messageArray \leftarrow C.toCharArray()
 5:
         keyPosition \leftarrow int[keylen]
 6:
 7:
         Sort the keyArray
 8:
         Strings \leftarrow String.valueOf(keyArray)
 9:
10:
         for each char c in dArray do
11:
             keyPosition[x] \leftarrow s.indexOf(c)
12:
13:
             Increament x by 1
14:
         cols \leftarrow keylen
         rows \leftarrow 0 if C's length mod cols equals 0 then \triangleright calculate rows
15:
16:
17:
             rows \leftarrow C.length()/cols
18:

    ▷ calculate columns

19:
             rows \leftarrow C.length()/cols + 1
20:
21:
         RowMatrix \leftarrow char[rows][cols]
22:
23:
         for i to rows do
             for \; \texttt{j} \; \; \texttt{to} \; \; \texttt{cols} \; do
24:
25:
                 if count k equals message C's length then
                     while k equals message's length and j
26:
27:
                     less than cols keep add 'X' to
28:
                     RowMatrix[i][j]
29:
                     break
                     assign\ RowMatrix[i][j]\ from
30:
31:
                     messageArray[k]
32:
                     Increament k by 1
33:
34:
         StringBuilder\ str \leftarrow StringBuilder()
35:
         for i to rows do
36:
             for j to cols do
37:
                 if RowMatrix[i][j] unequal to 'X' then
                     str.append(RowMatrix[i][j]) \\
38:
         return str
                                               Decrypted message is str
```

The following figure 10 shows the result of the decrypted plaintext. Further, use the encryption algorithm to double-check the answer. The result matches the original encrypted text.



Figure 8: Task2-Output

IV. Conclusion

With the growing use of computers and the internet, and an increasing need to transmit information quickly and securely, the use of encryption through existing protocols (AES, RSA, 3DES, etc.) information security that uses the two types of transposition mentioned (transposition and substitution).

In the project, we can see that using only one round of encryption and a minor key (5 letters), the information is already quite challenging to decipher, and with the use of the protocols mentioned above that repeatedly use the types of transposition, it becomes almost impossible to decipher the messages.

We also demonstrate in the project that the information is decrypted, just doing the inverse of the encryption procedure that needs to be done by the person who will receive the message.

REFERENCES

[1]N. Hamza, "Row transposition ciphers - ppt download," SlidePlayer. [Online]. Available: https://slideplayer.com/slide/13205094/. [Accessed: 28-Feb-2022].

[2]"Transposition cipher," Wikipedia, 23-Feb-2022. [Online]. Available: https://en.wikipedia.org/wiki/Transposition_cipher. [Accessed 28-Feb-2022].