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

The 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 cypher 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.

II. Encryption Implementation

To implement the row transposition encryption, we utilizes the key as a sequence to switch the columns in a two-dimension matrix to form a row transposition matrix(Figure 3).

Take the key 'NYITV' as a 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 to the key length '5' (Figure 2). Then, reorder columns in the matrix (Figure 3).

								0				1					2		3		4	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
								I					N						T		V			Y	
N	Y	I	T	V																					
1	4	0	2	3																					

Figure 1: *Task1-Encryption Sequence Order*

The reorder sequence is 20341 to decryption by using the same row exchange method.

0	1	2	3	4		
N	Y	I	T	V		
1	4	0	2	3		
R	E	O	R	D	E	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	Y	I	T	V
2	0	3	4	1
c	r	y	p	t
o	l	o	g	y
i	s	t	h	e
p	r	a	c	t
i	c	e	a	n
d	s	t	u	d
y	o	f	t	e
c	h	n	i	q
u	e	s	f	o
r	s	e	c	u
r	e	c	o	m
m	u	n	i	c
a	t	i	o	n
i	n	t	h	e
p	r	e	s	e
n	c	e	o	f
t	h	i	r	d
p	a	r	t	i
e	s	c	a	l
l	e	d	a	d
v	e	r	s	a
r	i	e	s	X

Figure 3: *Task1-Message Matrix*

The following figure 4 displays the encrypted message.

yotaetfnsecniteeircdrecoipidycurrm
aipntpelvrpghcautifcoiohsortaasstye
tndeqoumcneefdildaXrlsrcsoheseut
nrchaseei

Figure 4: *Task1-Encrypted Message*

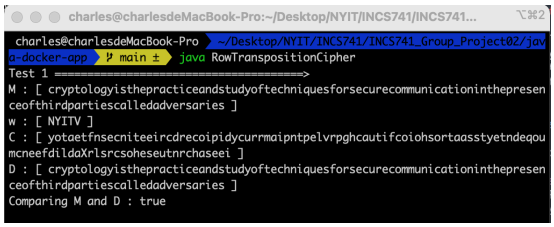

Figure 5: *Task1-Output*

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 is the reverse order of the encryption algorithm. The algorithm first writes the encrypted message out in rows. Then, it reads off the message by recording columns.

N	Y	I	T	V
2	0	3	4	1
t	h	e	r	o
w	t	r	a	n
s	p	o	s	i
t	i	o	n	c
i	p	h	e	r
i	s	a	f	a
i	r	l	y	s
i	m	p	l	e
e	a	s	y	t
o	i	m	p	l
e	m	e	n	t
c	i	p	h	e
r	i	t	i	s
a	t	r	a	n
s	p	o	s	i
t	i	o	n	c
i	p	h	e	r
t	h	a	t	f
o	l	l	o	w
s	a	s	i	m
p	l	e	r	u
l	e	f	o	r
m	i	x	i	n
g	u	p	t	h
e	c	h	a	r
a	c	t	e	r
s	i	n	t	h
e	p	l	a	i
n	t	e	x	t
t	o	f	o	r
m	t	h	e	c
i	p	h	e	r
t	e	x	t	x

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 matrix 'plainTextArray'. Next, use the RowTranspositionMatrix to record the rearrangement of the 'plainTextArray'. The last step, utilize the stringbuilder to build the encrpted message line by line through the RowTranspositionMatrix.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

```
function RTCDECRYPTION(w, C)
    keylen ← w.length()
    keyArray ← key.toCharArray()
    messageArray ← C.toCharArray()
    keyPosition ← int[keylen]

    Sort the keyArray
    Strings ← String.valueOf(keyArray)

    x ← 0
    for each char c in dArray do
        keyPosition[x] ← s.indexOf(c)
        Increament x by 1
    cols ← keylen
    rows ← 0
    if C's length mod cols equals 0 then        ▷ calculate rows
        rows ← C.length()/cols
    else                                        ▷ calculate columns
        rows ← C.length()/cols + 1

    RowMatrix ← char[rows][cols]
    k ← 0
    for i to rows do
        for j to cols do
            if count k equals message C's length then
                while k equals message's length and j
                less than cols keep add 'X' to
                RowMatrix[i][j]
                break
                assign RowMatrix[i][j] from
                messageArray[k]
                Increament k by 1

    StringBuilder str ← StringBuilder()
    for i to rows do
        for j to cols do
            if RowMatrix[i][j] != to 'X' then
                str.append(RowMatrix[i][j])
    return str                                  ▷ Decrypted message is str
```

The following figure 10 shows the result of the decrypted plaintext. Further, we use the encrytion algorithm to double check the answer. The result match to the original encrypted text.

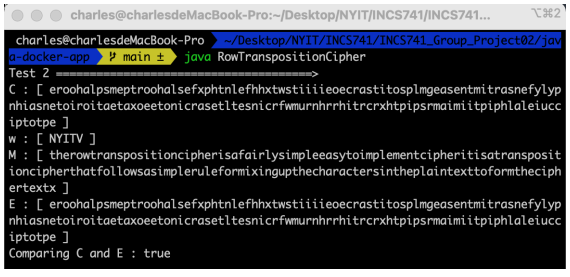

Figure 8: *Task2-Output*

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 this example, 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].