Implementation of Cryptography Technique using Columnar Transposition

Malay B. Pramanik
Department of Master of Computer Application
G. H. Raisoni College of Engineering
Nagpur, Maharashtra, India

Abstract
Cryptography is an art and science of converting original message into non-readable form. There are two techniques for converting data into non-readable form: 1) Transposition technique 2) Substitution technique. Transposition ciphers use the letters of the plaintext message, but they permute the order of the letters. Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns. In this Cryptography there is use of three aspects of Columnar Transposition; Single Transposition using ROT-13 applicable to message of the Algorithm, Double Transposition using Caesar Cipher in second round of an Algorithm and Triple Transposition were it combine both the concept and use reverse of the message in second round of the Algorithm.

Keywords
Cryptography, Substitution, Transposition, ROT-13, Caesar Cipher, Columnar Transposition, Shift Algorithm, Cipher text, Plaintext, Encryption, Decryption.

1. INTRODUCTION

The dramatic rise of internet has opened the possibilities that no one had imagined. Connect to any person, any organization or any computer, no matters how far from them. Internet cannot be used only for browsing purpose.[6] Sensitive information like banking transactions, credit card information and confidential data can be shared through internet. But still we are left with a difficult job of protecting network from variety of attacks. With the lots of efforts, network support staff came up with solution to our problem named "Cryptography". [4]Data that can be read and understood without any difficulty is called plain text or clear text. The method of encoding Plain text in such a way as to hide its content is called encryption. Encrypting plain text results in unreadable gibberish called cipher text. You use Encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plain text is called decryption.[1]

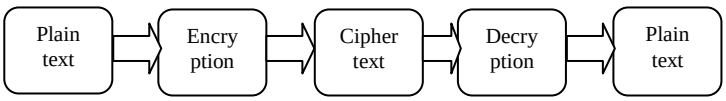

Fig1: Encryption & Decryption

There are two primary ways in which plaintext can be modified to corresponding Cipher text: Substitution and Transposition.A Substitution technique is one in which the letters of Plain text are replaced by other letters or by numbers.(Caesar Cipher , Hill Cipher, Monoalphabetic cipher etc).A Transposition technique is one in which the letters of the message are rearranged or permuted (Rail Fence method, Columnar method etc.)[2].

Transposition Ciphers are ciphers in which the plaintext message is rearranged by some means agree upon by the sender and receiver. Transposition ciphers differ from the mono-alphabetic ciphers (shift, affine, and substitution)[3] we have studied earlier. In mono-alphabetic ciphers, the letters are changed by creating a new alphabet (the cipher alphabet) and assigning new letters. In transposition ciphers, no new alphabet is created – the letters of the plaintext are just rearranged is some fashion. Simple Columnar Transpositions, Where the message is written horizontally in a fixed and agreed upon number of columns and then described letter by letter from the columns proceeding from left to right[7]. In general, given a simple columnar transposition with total letters and columns, we use the division algorithm to divide by to compute. In tableau form, this looks like:

$$\begin{array}{rl} & q \leftarrow \text{Quotient } q \\ \#\text{ Columns c} \rightarrow & c\overline{)\,n} \leftarrow \#\text{ letters } n \\ & \underline{-\,qc} \\ & r \leftarrow \text{Remainder } r \end{array}$$

Then, the first r columns contain q+1 letters each for a total of r (q+1) letters. The remaining c - r columns have q letters in each column for a total of (c – r) q total letters [8].

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 [9]. 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 [5]. 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. Transposition ciphers rearrange characters according to some scheme. This rearrangement was classically done with the aid of some type of geometric figure like rectangle. 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 rearranged width and then prepared a transposed version by taking the columns off in some order (by a numerical key).

2. 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 word 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".

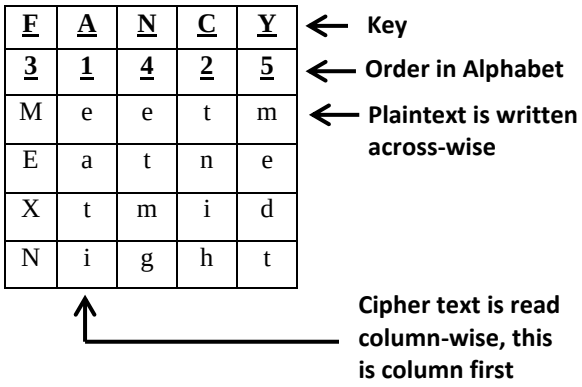

Fig2: Columnar Transposition

In this transposition, the plain text is simply placed in the column format as it is. But, in this paper there is use of ROT-13 concept to the plain text before converted it into matrix form. Even this Algorithm can also convert the numeric value as well as the special characters.

Encryption Algorithm

Step 1: Start
Step 2: Read Plain Text
Step 3: Apply ROT-13
Step 4: Generate plain text in ROT-13 format
Step 5: Choose the password for transposition
Step 6: The length of password and the length of the text is used to determine the no. of rows that will be created as the no. of column is already known as the no. of password letters
Step 7: The password is arranged in such a way as its occurrence in alphabet i.e. the alphabet closest to letter 'a' is assigned the first position in whatever column it is
Step 8: The Text is arranged into table, row wise
Step 9: The position of the alphabet is used to print out the text. The alphabet in the column corresponding to the alphabet arrangement is read first and the process is continued till the password position has been exhausted
Step 10: Generate Cipher Text
Step 11: Stop

Decryption Algorithm

Step 1: Start
Step 2: Generated Cipher text
Step 3: Password for Transposition same as taken in Encryption
Step 4: The length of the text and password are used to determine the number of alphabet that would be placed in the columns determined by the password arrangement.
Step 5: The plain text is achieved by reading the alphabets row by row.
Step 6: Generation of Plain text
Step 7: Apply ROT-13
Step 8: Generation of Original Plain Text
Step 9: Stop

Example for Encryption

Plain Text: we are discovered flee at once
Apply ROT-13,
Plain Text in ROT-13 Format:
jr ner qvfpbirerq syrr ng bapr
Password: zebras

z	e	b	r	a	S
6	3	2	4	1	5
j	r		n	e	r
	q	v	f	p	b
i	r	e	r	q	
s	y	r	r		n
g		b	a	p	r

Cipher Text: epq p verbrqry nfrrarb nrj isg

Example for Decryption

Cipher Text: epq p verbrqry nfrrarb nrj isg
Password: zebras

z	e	b	r	a	s
6	3	2	4	1	5
j	r		n	e	r
	q	v	f	p	b
i	r	e	r	q	
s	y	r	r		n
g		b	a	p	r

Plain Text: jr ner qvfpbirerq syrr ng bapr
Apply ROT-13,
Original Plain Text: we are discovered flee at once

3. DOUBLE TRANSPOSITION

A double transposition was often used to make the cryptography stronger. This is simply a columnar transposition applied twice. The same key can be used for both transpositions, or two different keys can be used.

In this transposition, there is use of Caesar Cipher concept to the plain text before converted it into matrix form in the second rotation.

Encryption Algorithm

Step 1: Start
Step 2: Read Plain Text
Step 3: Choose the password for transposition
Step 4: The length of password and the length of the text is used to determine the no. of rows that will be created as the no. of column is already known as the no. of password letters

Step 5: The password is arranged in such a way as its occurrence in alphabet i.e. the alphabet closest to letter 'a' is assigned the first position in whatever column it is
Step 6: The Text is arranged into table, row wise
Step 7: The position of the alphabet is used to print out the text. The alphabet in the column corresponding to the alphabet arrangement is read first and the process is continued till the password position has been exhausted
Step 8: Generate First Cipher Text
Step 9: Choose another password or apply same password for the second transposition
Step 10: Apply Caesar Cipher Shift
Step 11: Repeat Step 4 to Step 7
Step 12: Generate Final Cipher Text
Step 13: Stop

Decryption Algorithm

Step 1: Start
Step 2: Generated Cipher text
Step 3: Password for Transposition same as taken in Encryption
Step 4: The length of the text and password are used to determine the number of alphabet that would be placed in the columns determined by the password arrangement.
Step 5: The plain text is achieved by reading the alphabets row by row.
Step 6: Generation of first Plain text
Step 7: Password for second Transposition or use same password
Step 8: Apply Caesar Cipher Shift
Step 9: Repeat Step 4 and Step 5
Step 10: Generate Final Plain Text
Step 11: Stop

Example for Encryption

Plain Text: we are discovered flee at once
Password 1: zebras

z	e	b	r	a	s
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

Cipher Text 1: rcd c ireoedel aseeneo aew vft
Password 2: stripe
Apply Caesar Cipher Shift,
Cipher Text 1 in Caesar Cipher Shift Format:
ufg f luhrhgho dvhhqhr dhz yiw

s	t	r	i	p	e
5	6	4	2	3	1
u	f	g		f	
l	u	h	r	h	g
h	o		d	v	h
h	q	h	r		d
h	z		y	i	w

Cipher Text: ghdw rdryfhv igh h ulhhhfuoqz

Example for Decryption

Cipher Text: ghdw rdryfhv igh h ulhhhfuoqz
Password 1: stripe

s	t	r	i	p	e
5	6	4	2	3	1
u	f	g		f	
l	u	h	r	h	g
h	o		d	v	h
h	q	h	r		d
h	z		y	i	w

Plain Text 1: ufg f luhrhgho dvhhqhr dhz yiw
Apply Caesar Cipher Shift,
Plain Text 1 in Caesar Cipher Shift Format:
rcd c ireoedel aseeneo aew vft
Password 2: zebras

z	e	b	r	a	s
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

Plain Text: we are discovered flee at once

4. TRIPLE TRANSPOSITION

A Triple Transposition is a combination of Columnar and Double Transposition. There is a use of three different methods for three different round of transposition. Each round Encrypt or Decrypt the message using their own Algorithm. In first round ROT-13 will apply to both Key and Message and the Encrypted or Decrypted Message from the first round of Transposition will pass through the second round where Reverse String operation will apply to both the aspect then in third round Caesar Cipher Shift Algorithm is applied to the text which is generated from second round of Transposition. And finally there is generation of complex form of Cipher Text using Triple Transposition.

Encryption Algorithm

Step 1: Start
Step 2: Read Plain Text
Step 3: Choose the password for transposition
Step 4: Apply ROT-13 to both Key and Plain Text

Step 5: The length of password and the length of the text is used to determine the no. of rows that will be created as the no. of column is already known as the no. of password letters
Step 6: The password is arranged in such a way as its occurrence in alphabet i.e. the alphabet closest to letter 'a' is assigned the first position in whatever column it is
Step 7: The Text is arranged into table, row wise
Step 8: The position of the alphabet is used to print out the text. The alphabet in the column corresponding to the alphabet arrangement is read first and the process is continued till the password position has been exhausted
Step 9: Generate First Cipher Text
Step 10: Choose another password or apply same password for the second transposition
Step 11: Apply Reverse Operation to Both aspects
Step 12: Repeat Step 5 to Step 8
Step 13: Generate second Cipher Text
Step 14: Choose another password or apply same password for the third transposition
Step 15: Apply Caesar Cipher Shift to both Key and Plain Text
Step 16: Repeat Step 5 to Step 8
Step 17: Stop

Decryption Algorithm

Step 1: Start
Step 2: Generated Cipher text
Step 3: Password for Transposition same as taken in Encryption
Step 4: Apply Caesar Cipher Shift to both Key and Plain Text
Step 5: The length of the text and password are used to determine the number of alphabet that would be placed in the columns determined by the password arrangement.
Step 6: The plain text is achieved by reading the alphabets row by row.
Step 7: Generation of first Plain text
Step 8: Password for second Transposition or use same password
Step 9: Apply Reverse Operation to Both aspects
Step 10: Repeat Step 5 and Step 6
Step 11: Generation of second Plain Text
Step 12: Password for third Transposition or use same password
Step 13: Apply ROT-13 to both Key and Plain Text
Step 14: Repeat Step 5 and Step 6
Step 15: Generation of final Plain Text
Step 16: Stop

Example for Encryption

Plain Text: we are discovered flee at once
Password 1: zebras
Apply ROT-13,
Plain Text in ROT-13 Format:
jr ner qvfpbirerq syrr ng bapr
Password 1 in ROT-13 Format:
mroenf

m	**r**	**o**	**e**	**n**	**f**
3	**6**	**5**	**1**	**4**	**2**
j	**r**		**n**	**e**	**r**
	q	**v**	**f**	**p**	**b**

i	**r**	**e**	**r**	**q**	
s	**y**	**r**	**r**		**n**
g		**b**	**a**	**p**	**r**

Cipher Text 1: nfrrarb nrj isgepq p verbrqry
Password 2:stripe
Apply Reverse operation,
Cipher Text 1 in Reverse Format:
yrqrbrev p qpegsi jrn brarrfn
Password 2 in Reverse Format:
epirts

e	**p**	**i**	**r**	**t**	**s**
1	**3**	**2**	**4**	**6**	**5**
	y	**r**	**q**	**r**	**b**
r	**e**	**v**		**p**	
q	**p**	**e**	**g**	**s**	**i**
	j	**r**	**n**		**b**
r	**a**	**r**	**r**	**f**	**n**

Cipher Text 2: rq rrverryepjaq gnrb ibnrps f
Password 3:milanp
Apply Caesar CipherShift,
Cipher Text 2 in Caesar Cipher Shift Format:
ut uuyhuuhsmdt jque lequsv i
Password 3 in Caesar Cipher Shift Format:
plodqs

p	**l**	**o**	**d**	**q**	**s**
4	**2**	**3**	**1**	**5**	**6**
	u	**t**		**u**	**u**
y	**h**	**u**	**u**	**h**	**s**
r	**n**	**d**	**t**		**j**
q	**u**	**e**		**l**	**e**
q	**u**	**s**	**v**		**i**

Cipher Text: ut vuhnuutudes yrqquh l usjei

Example for Decryption

Cipher Text: ut vuhnuutudes yrqquh l usjei
Password 1:milanp
Apply Caesar Cipher Shift,
Password 1 in Caesar Cipher Shift Format:
plodqs

p	**l**	**o**	**d**	**q**	**s**
4	**2**	**3**	**1**	**5**	**6**
	u	**t**		**u**	**u**
y	**h**	**u**	**u**	**h**	**s**
r	**n**	**d**	**t**		**j**
q	**u**	**e**		**l**	**e**
q	**u**	**s**	**v**		**i**

Plain Text 1: ut uuyhuuhsmdt jque lequsv i

Apply Caesar Cipher Shift,

Plain Text 1 in Caesar Cipher Shift Format:

rq rrverryepjaq gnrb ibnrps f

Password 2:stripe

Apply Reverse operation,

Password 2 in Reverse Format:

epirts

e	**p**	**i**	**r**	**t**	**s**
1	**3**	**2**	**4**	**6**	**5**
	y	**r**	**q**	**r**	**b**
r	**e**	**v**		**p**	
q	**p**	**e**	**g**	**s**	**i**
	j	**r**	**n**		**b**
r	**a**	**r**	**r**	**f**	**n**

Plain Text 2:yrqrbrev p qpegsi jrn brarrfn

Apply Reverse operation,

Plain Text 2 in Reverse Format:

nfrrarb nrj isgepq p verbrqry

Password 3: zebras

Apply ROT-13,

Password 1 in ROT-13 Format:

mroenf

m	**r**	**o**	**e**	**n**	**f**
3	**6**	**5**	**1**	**4**	**2**
j	**r**		**n**	**e**	**r**
	q	**v**	**f**	**p**	**b**
i	**r**	**e**	**r**	**q**	
s	**y**	**r**	**r**		**n**
g		**b**	**a**	**p**	**r**

Plain Text 3: jr ner qvfpbirerq syrr ng bapr

Apply ROT-13,

Plain-Text: we are discovered flee at once

5. ADVANTAGES

- Overcome all the limitations of Caesar cipher.
- The result cannot be easily reconstructed.
- To understand the algorithm is not very complex.
- It is more difficult to crypt analyze.
- It provide more complexity to the message

6. DISADVANTAGES

- Complex method by performing three stage of Encryption Method.
- Difficult to implement as simple Caesar cipher.

7. CONCLUSION

Caesar cipher is simplest type of cipher and mostly used and ROT13 is also a type Caesar Cipher method with 13 Shift. Transposition method is mostly combined with other techniques. Both substitution method and transposition method encryption are easily performed with the power of computers. The combination classic techniques provide more secure and strong cipher. The final cipher text is so strong that is very difficult to break. Substitution method only replaces the letter with any other letter and transposition method only change position of characters. The above described method is the combination of both the transposition and substitution method which provides much more secure cipher.

8. REFERENCES

[1] R.I Salawu & S.O Adetona, "The Art and Science of Secured Communication", Institute of Security of Nigeria, Nigeria 2007

[2] James Irvine & David Harie, "Data Communications & Network: An Engineering Approach", John Wiley & Sons ltd., 2002

[3] Brian J. Winkel, Cipher A. Deavours, David Kahn, and Louis Kruh "The German Enigma Cipher Machine: Beginnings, Success, and Ultimate Failure", Artech House, August 2005.

[4] Tyma Paul, "Software Development Secure", Start Newsletter, Feb 2003.

[5] Madsen Wayne, "An International Survey of Encryption Policy", 1998

[6] S.O Adetona, "Messages Secrecy in Electioneering environment", proceedings of Institute of Security, Nigeria,2009

[7] Stamper, David, "Essential of Data Communication", Saratoga Group

[8] Eric Maiwald, "Network Security a Beginner's Guide", Second Edition, McGraw Hill, Osborne, 2003.

[9] Ed Tittel, "Theory and Problems of Computer Networking", McGraw Hill, Osborne, 2002