Security Enhancement-Using Modified Caesar Box

Gauri S Telang
Dept of Mathematics
PES's Modern College of Engineering, Pune-05

Abstract- *Caesar box is encryption method used to protect plain text message from antagonist. But by using some manual methods or computer techniques Caesar box can be decodes. In this paper we are introducing algorithm for modified Caesar box using matrices*

I. INTRODUCTION

Cryptography is a science of hiding information into more secure form so that only that person can read this information who is the intended to receive.

Original text is called as plain Text. Text after coding is called ciphered text, and Deciphering is process of retrieving original text from ciphered text [1].

Julius Caesar was one of the first people to write the code to increase the security in time of war. Julius Caesar had invented some new methods of coding from which Caesar cipher is widely used and more popular among the cryptographers. Second method he invented was Caesar Box Cipher which is a Columnar Transposition Cipher.

i. Caesar Cipher [2],[3] :

In this method Caesar was using shifting key 3 to cipher the text .That is using following mathematical equation,

$$C \equiv (P + 3) \bmod 26$$

Where,

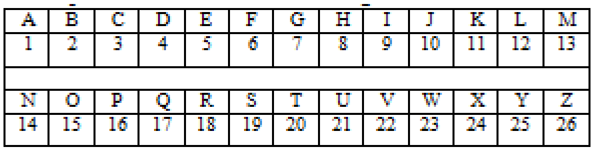
C is ciphered text

P is plain text
For example:

Consider a following text for cipher

INDIA IS BEAUTIFUL

To cipher the text consider following code



A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Here using above table we have,

Plain text 'I' has number 9 to convert it to cipher t text we use

$$C \equiv (P + 3) \bmod 26$$
$$C \equiv (9 + 3) \bmod 26$$
$$C\equiv 12 \bmod 26$$

Therefore for plain text I ciphered text is L

Similarly, for each plain text we have ciphered text as follows

i → L , n→Q , d→G, i→L, a→D, i→L, s→V, b→E, e→H,
a→D, u→X, t→W, i→L, f→I, u→X, l→O

Therefore the coded message is

LQGLD LV EHDXWLIXO

To decipher the massage one can use mathematical expression

$$P \equiv (C - 3) \bmod 26$$

ii. Caesar Box cipher:

To Cipher the text:

Step 1) In Caesar Box cipher plain text of n^2alphabets are considered that is text having 4, 9, 16, 25 … alphabets.

Consider plain text massage

INDIA IS BEAUTIFUL

This text contains 16 alphabets

Step 2) Write this text in n × n matrix form row wise. Then above text will be

I	N	D	I
A	I	S	B
E	A	U	T
I	F	U	L

Step 3) To cipher the text write these alphabets column wise starting with first row Ciphered Text of above text massage is

IAEIN IA FDSUUIBTL

To decipher the above text:

Step 1) First check whether the text contain n^2 number of letters and then consider ciphered text in n × n matrix form column wise.

Consider the text:

IAEIN IA FDSUUIBTL

Then matrix form is given as

I	N	D	I
A	I	S	B
E	A	U	T
I	F	U	L

Step 2) Write text letters row wise

INDIAISBEAUTIFUL

There for the original text is

INDIA IS BEAUTIFUL

II. MODIFIED CAESAR BOX CIPHER

In this paper we can see modified method of Caesar box.

i. Algorithm for Modified Caesar Box to cipher the Text:

Step 1) Enter code of n^2alphabets

For example:

I LIKE MATHEMATICS

Step 2) Write text in form of n × n matrix form starting from left to write row-wise.

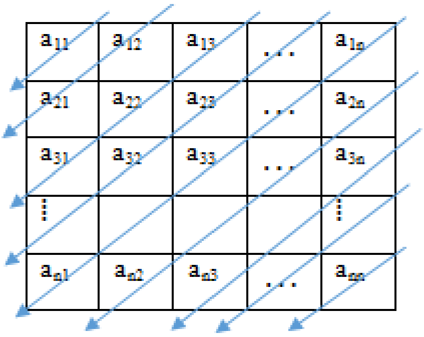
Let a string of n^2 letters say

$a_{11}, a_{12}, a_{13}, \ldots, a_{1n}, a_{21}, a_{22}, a_{23}, \ldots, a_{2n}, a_{31}, a_{32}, a_{33}, \ldots, a_{3n}, a_{n1}, a_{n2}, a_{n3}, \ldots, a_{nn}$.

Then the matrix form of this string is

a_{11}	a_{12}	a_{13}	$\ldots$	a_{1n}
a_{21}	a_{22}	a_{23}	$\ldots$	a_{2n}
a_{31}	a_{32}	a_{33}	$\ldots$	a_{3n}
$\vdots$				$\vdots$
a_{n1}	a_{n2}	a_{n3}	$\ldots$	a_{nn}

Step 3) to cipher the text start writing letters from diagonally staring with first row



a_{11}	a_{12}	a_{13}	$\ldots$	a_{1n}
a_{21}	a_{22}	a_{23}	$\ldots$	a_{2n}
a_{31}	a_{32}	a_{33}	$\ldots$	a_{3n}
$\vdots$				$\vdots$
a_{n1}	a_{n2}	a_{n3}	$\ldots$	a_{nn}

Then the ciphered text is

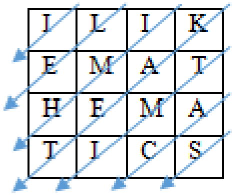
$a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, a_{41}, a_{23}, a_{32}, \ldots, a_{1n}, a_{2(n-1)}, \ldots, a_{n1}, \ldots, a_{n(n-1)}, a_{nn}$.

For example:

Consider text to cipher

I LIKE MATHEMATICS

Then matrix form of above string is



I	L	I	K
E	M	A	T
H	E	M	A
T	I	C	S

Then the ciphered text massage is I

I LEIM HKAETTMIACS

ii. Algorithm for Modified Caesar Box To Decipher the Text:

To decipher the text one can use following algorithm

Step 1) Enter ciphered text with n^2alphabets or characters
Say b_1, b_2, b_3, b_4 ,…, b_n^2

Step 2) Divide this text in 2n-1 partition having number of alphabets or characters as,
1, 2, 3, …,n-1,n,n-1,…,3,2,1 in each corresponding segment

That is ,

First partition will have 1 character,
Second partition will have 2 characters,
Third partition will have 3 characters,
$\vdots$
$(n-1)^{th}$ partition have n-1 characters,
n^{th} partition have n characters,
$(n+1)^{th}$ partition have n-1 characters,
$(n+2)^{th}$ partition have n-2 characters, …,
$\vdots$
$(2n-1)^{th}$partition will have 1 character
That is above string can be divided into 2n-1 sub part as follows

$b_{1,}$
$b_{2,}$ b_3
b_4 , b_5 , b_6
b_7 , b_8 ,b_9 ,b_{10}
$\vdots$
b_m ,b_{m+1} ,b_{m+2},…, b_{m+n-1}
$\vdots$
$b_{n^2-9}, b_{n^2-8}, b_{n^2-7}, b_{n^2-6}$
$b_{n^2-5}, b_{n^2-4}, b_{n^2-3}$
$b_{n^2-2} b_{n^2-1}$
b_{n^2}

Where $m = \frac{n(n-1)}{2} + 1$

Step 3) Take each partition and write these letters in n × n matrix diagonally that is in matrix form we have,

$$b_{11} = b_1,\ b_{12} = b_2\ ,\ b_{21} = b_3,$$
$$b_{13} = b_4\ ,\dots, b_{1n} = b_m\ ,\ \ b_{2(n-1)} = b_{m+1}$$
$$,\dots, b_{n1} = b_{m+n-1}, \dots, b_{nn} = b_{n^2}$$

Then matrix is given by

b_1	b_2	b_4	$\cdots$	b_m
b_3	b_5		b_{m+1}	
b_6		b_{m+2}		
$\vdots$				
b_{m+n-1}			$\cdots$	b_{n^2}

Step 4) to write deciphered code write all characters row-wise that is

$$b_1, b_2, b_4,\dots,$$
$$b_m, b_3, b_5, \dots, b_{m+1},\ \ b_6, \dots, b_{m+2}, b_{m+n-1}, \dots, b_{n^2}$$

For example

Enter the ciphered text,

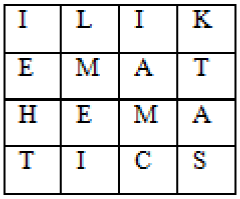
I LEIM HKAETTMIACS

Here $n^2 = 16$ therefore n = 4

So number of partitions is equal to:

$$2n - 1 = 2(4) - 1 = 7$$

Therefore partitions are I, LE, IMH, KAET, TMI, AC, S
Then matrix form of above partitions is



I	L	I	K
E	M	A	T
H	E	M	A
T	I	C	S

To write deciphered code, write all characters diagonally,
For example
Enter the ciphered text,

I LEIM HKAETTMIACS

Here $n^2 = 16$ therefore n = 4

So number of partitions is equal to

$$2n - 1 = 2(4) - 1 = 7$$

Therefore partitions are,

I, LE, IMH, KAET, TMI, AC, S

Then matrix form of above partitions is Writing this massage from left to right starting from first row

ILIKEMATHEMATICS

Therefore the deciphered massage is

I like mathematics.

III. CONCLUSION

In this paper we have discussed new method of Caesar box cipher which more difficult to decode than simple Caesar box in future one can uses this method to increase security in various places. And using combinations of this we can enhance security.

REFERENCES

[1] https://en.wikipedia.org/wiki/caesar_cipher

[2] https://en.wikipedia.org/wiki/cryptography

[3] https://www.wikihow.com/decode-a-caesar-box-code

[4] https://www.decode.fr/caesar_box_cipher

[5] Enas Ismael Imran, Farah Abdulameeraabdulkareem “Enhancement Caesar Cipher for better security” IOSR Journal of Computer Engineering (IOSR_JCE) Volume 16 Issue 3, Ver. V (May-Jun 2014)

[6] Atish Jain , Ronak Dedhia, Abhijit Patil “Enhancing the security of Caesar Cipher Substitution Method using a Randomized Approach for more secure Communication” International Journal Of Computer Applications(0975_8887) Volume 129-No.13 November 2015

[7] Kashish Goyal, Supriya Kinger “Modified Caesar Cipher for Better Security Enhancement” International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013 26

[8] Benni Purnama, Hetty Rohayani. AH “Anew Modified Caesar Cipher Cryptography Method With Legible Cipher text From A Massage To Be Encrypted” Procedia Computer science 59(2015)195-204