ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

Improving the Security of Caesar Cipher Using Row Shift and Column Transformation

Ahmad Rufa'i, A.A Ibrahim, Zaid Ibrahim, Saidu Yakubu

Assistant Lecturer, Dept of Mathematics, Sokoto State University, Nigeria

Professor, Dept of Mathematics, Sokoto State University, Nigeria

Lecturer, Dept of Mathematics, Sokoto State University, Nigeria

Assistant Lecturer, Dept of Mathematics, College of Nursing and midwifery, Sokoto, Nigeria

ABSTRACT: Data security has become a very important aspect in recent years due to drastic progress in the use of internet. Many ciphers have been developed to provide data security but all the conventional encryption techniques have proved to be weak and amenable to attack even by use of brute force and traditional cryptanalysis. Caesar cipher is the simplest and weakest because it can be simply attacked by brute force cryptanalysis. This work proposes an improvement over Caesar cipher by using row shift and column transformations. The improvement will no doubt eliminate the weakness of the Caesar cipher and provide cipher text that is harder to crack.

KEYWORDS*:* Caesar cipher, Brute force attack, Row Shifting, Column Transformation, Self inverse.

I. INTRODUCTION

In recent time, the internet has positioned itself to providing essential communication between millions of people and is being increasingly used as a tool for paperless transaction in business, private or governmental offices by means of e-mail messages, e-cash transactions and so on. Due to this development there is a great need for transmission of data through internet in various businesses, private and governmental sectors. Part of this information is sensitive and confidential like banking transactions, credit information, governmental information and so on. Moreover, sensitive information is transferred over web using e-mails and so on.The confidentiality, authentication and integrity of such important information need to be maintained and protected. To protect this type of sensitive information from an unauthorized access, experts have come up with solutions embodied in the concept of 'cryptography'. Cryptography is the study of sending and receiving secret messages.

The aim of cryptography is to send messages across a channel so that only the intended recipient of the message can read it. In addition, when a message is received, the recipient usually requires some assurance that the message is authentic; that is, that it has not been sent by someone who is trying to deceive the recipient. The message to be sent is called the plaintext message. The disguised message is called the ciphertext. The plaintext and the ciphertext are both written in an alphabet, consisting of letters or characters. Characters can include not only the familiar alphabetic characters A,…,Z and a,…, z but also digits, punctuation marks, and blanks.

A cryptosystem, or cipher, has two parts: encryption, the process of transforming a plaintext message to a ciphertext message, and decryption, the reverse transformation of changing a ciphertext message into a plaintext message [1]. Caesar cipher is one of the most widely known encryption and decryption cipher. It is also the simplest and weakest cipher [2].

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

The process of encryption and decryption of data is shown below:

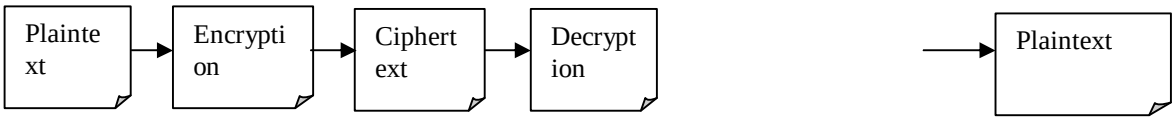

Fig.1.1.1. Encryption and Decryption [5]

By using cryptography many goals can be achieved. These goals can be either all achievable in some applications at the same time or only one of them being achieved. The goals of cryptography include:

(i) Confidentiality: this is the most important goal which ensures that nobody can understand the received message except the one who has the deciphering key.

(ii) Authentication: this is the process of providing the identity that assures communicating entity is the one that it claimed to be, which applies to both entities and information itself.

(iii) Data Integrity: this is a service which addresses the unauthorized alteration of data

(iv) Non-Repudiation: it is a mechanism used to prove that the sender really sent message and message was received by the specified party, so the recipient cannot claim the message was not sent.

(v) Access control: it is the process of preventing an unauthorized use of resources. This goal controls who can access the resources [6].

II. REVIEW OF THE LITERATURE

The earliest form of cryptography was the simple writing of a message that cannot be read by other people. In fact, the word 'cryptography' comes from two Greek words 'cryptos' and 'graphein' which means hidden and writing respectively. The need to conceal message has been with us since we move out of caves, started living in groups and decided to take this civilization idea seriously [1]. The Greek's idea was to wrap a tape around a stick and then write the message on the wound tape. When the tape was unwounded the writing would be meaningless. The receiver of the message would of course have a stick of the same diameter and use it to decipher message [5].

The Roman method of cryptography was known as Caesar cipher, named after Julius Caeser who apparently used it to communicate with his generals. It is one of the earliest known and simplest ciphers. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,

Plaintext: MEET ME AFTER THE TOGA PARTY
Ciphertext:PHHW PH DIWHU WKH WRJD SDUWB

If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys. Figure below shows the results of applying this strategy to the example ciphertext. In this case, the plaintext leaps out as occupying the third line [5].

KEY
1 OGGV OG CHVGT VJG VQIC RCTVA

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

2 NFFU NF BGUFS UIF UPHB QBSUZ
3 MEET ME AFTER THE TOGA PARTY
4 LDDS LD ZESDQ SGD SNFZ OZQSX

Many ciphers have been developed to protect the confidential information, but almost all the conventional ciphers are proved to be weak and amenable to attack even by the use of brute force and traditional cryptanalysis. Hence there is a need to develop stronger and more secure ciphers that will overcome the shortcomings and weaknesses of the conventional ciphers, either by modification, combination and so on.

III. PROPOSED WORK

In this work Caesar cipher will be combined with row shift, column transformation and additional key.

A. Row shift

This involves shifting the rows of the grid from right to left the first row does not shift at all.

B. Column transformation

In column transformation we take each column separately and replace it with one where each entry is the sum of all other entries in the column. The addition is exclusive OR after turning each letter to binary digits.

C. Encryption algorithm

Step I: Encrypt the plaintext using the Caesar cipher.
Step II: Write the encrypted message as $m \times m$ grid (top to bottom and left to right).
Step III: Shift the rows of the grid (R-L) using shift of nth row = $(n-1)$ shift.
Step IV: add secret Key(s).
Step V: Transform each column.

D. Decryption algorithm

Step I: Read the ciphertext and write as $m \times m$ grid (top to bottom and left to right).
Step II: Transform each Column.
Step III: add Secret key(s).
Step IV: Shift the rows of the grid (L-R) using shift of nth row = $(n-1)$ shift.
Step V: Write all the component of the matrix in a straight line (from top to bottom and left to right), and decrypt using Caesar cipher

IV. ENCRYPTION AND DECRYPTION USING PROPOSED SYSTEM

. Correspondence Table (character – binary number)

Character	Binary
η	00000
A	00001
B	00010
C	00011
D	00100
E	00101
F	00110
G	00111
H	01000
I	01001
J	01010

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

K	**01011**
L	**01100**
M	**01101**
N	**01110**
O	**01111**
P	**10000**
Q	**10001**
R	**10010**
S	**10011**
T	**10100**
U	**10101**
V	**10110**
W	**10111**
X	**11000**
Y	**11001**
Z	**11010**
Space(_)	**11011**
!	**11100**
.	**11101**
,	**11110**
?	**11111**

A. Encryption

Suppose we want to encrypt “YES IT WORKS !!” using keys CONFERENCE XX!!! and TRANSFORMATIONXY

!HV,LW,ZRUNV

$$\begin{pmatrix} ! & L & R & , \\ H & W & N & \eta \\ V & , & U & \eta \\ , & Z & V & C \end{pmatrix} \Rightarrow \begin{pmatrix} ! & L & R & , \\ W & N & \eta & H \\ U & \eta & V & , \\ C, & , & Z & V \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} ! & L & R & , \\ H & W & N & \eta \\ V & , & U & \eta \\ , & Z & V & C \end{pmatrix} + \begin{pmatrix} C & E & C & X \\ O & R & E & ! \\ N & E & \_ & ! \\ F & N & X & ! \end{pmatrix}$$

$$!+C = +\begin{array}{r} 11100 \\ \underline{00011} \\ 11111 = ? \end{array} \qquad W + O = +\begin{array}{r} 10111 \\ \underline{01111} \\ 11000 = X \end{array}$$

$$U + N = +\begin{array}{r} 10101 \\ \underline{01110} \end{array} \qquad C + F = +\begin{array}{r} 00011 \\ \underline{00101} \end{array}$$

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

11011= _ 00101= E

Continuing in this way we get

L + E = I N + R = !

η + E = E , + N = P

R + C = Q η + E = E

V + _ = M Z + X = B

, + X = F H + ! = T

, + ! = B V + ! = J

Thus,

$$\begin{pmatrix} ? & I & Q & F \\ X & ! & E & T \\ \_ & E & M & B \\ E & P & B & J \end{pmatrix}$$

Similarly, adding the second key we have

$$\begin{pmatrix} ? & I & Q & F \\ X & ! & E & T \\ \_ & E & M & B \\ E & P & B & J \end{pmatrix} + \begin{pmatrix} T & S & M & O \\ R & F & A & N \\ A & O & T & X \\ N & R & I & Y \end{pmatrix}$$

? + T = K X + R = J

_ + A = Z E + N = K

I + S = Z ! + F = Z

E + O = J P + R = B

Q + M = ! E + A = D

M+ T = Y B + I = K

F + O = I T + N = Z

B + X = Z J + Y = S

Thus, $\begin{pmatrix} K & Z & ! & I \\ J & Z & D & Z \\ Z & J & Y & Z \\ K & B & K & S \end{pmatrix}$

Column transformation

$$\begin{pmatrix} K \\ J \\ Z \\ K \end{pmatrix} \Rightarrow \begin{pmatrix} J+Z+K \\ Z+K+K \\ K+K+J \\ K+J+Z \end{pmatrix} \Rightarrow \begin{pmatrix} \_ \\ Z \\ J \\ \_ \end{pmatrix}$$

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

$$\begin{array}{ll} 01010 & 11010 \\ \Rightarrow +11010 & +01011 \\ \underline{01011} & \underline{01011} \\ 11011 = \_ & 11010 = Z \end{array}$$

$$\begin{array}{ll} 01011 & 01011 \\ +01011 & +01010 \\ \underline{01010} & \underline{11010} \\ 01010 = J & 11011 = \_ \end{array}$$

For the second column

$$\begin{pmatrix} Z \\ Z \\ J \\ B \end{pmatrix} \Rightarrow \begin{pmatrix} R \\ R \\ B \\ J \end{pmatrix}$$

For the third column

$$\begin{pmatrix} ! \\ D \\ Y \\ Z \end{pmatrix} \Rightarrow \begin{pmatrix} V \\ N \\ S \\ A \end{pmatrix}$$

For the last column

$$\begin{pmatrix} I \\ Z \\ Z \\ S \end{pmatrix} \Rightarrow \begin{pmatrix} S \\ \eta \\ \eta \\ I \end{pmatrix}$$

Thus, $\begin{pmatrix} \_ & R & V & S \\ Z & R & N & \eta \\ J & B & S & \eta \\ \_ & J & A & I \end{pmatrix}$

Which gives our ciphertext as: _ZJ_RRBJVNSAS$\eta\eta I$

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

B. Decryption

_ZJ_RRBJVNSAS$\eta\eta I$

$$\begin{pmatrix} \_ & R & V & S \\ Z & R & N & \eta \\ J & B & S & \eta \\ \_ & J & A & I \end{pmatrix}$$

Now, for column transformation we have,

$$\begin{pmatrix} \_ \\ Z \\ J \\ \_ \end{pmatrix} \Rightarrow \begin{pmatrix} Z+J+\_ \\ J+\_+\_ \\ \_+\_+Z \\ \_+Z+J \end{pmatrix} \Rightarrow \begin{pmatrix} K \\ J \\ Z \\ K \end{pmatrix}$$

Because,

$$\begin{array}{r} 11010 \\ +\,01010 \\ \hline 11011 \end{array} \qquad 01011 = K$$

$$\begin{array}{r} 01010 \\ +\,11011 \\ \hline 11011 \end{array} \qquad 01010 = J$$

$$\begin{array}{r} 11011 \\ +\,11011 \\ \hline 11010 \end{array} \qquad 11010 = Z$$

$$\begin{array}{r} 11011 \\ +\,11010 \\ \hline 01010 \end{array} \qquad 01011 = K$$

Continuing this way we have,

Second column:

$$\begin{pmatrix} R \\ R \\ B \\ T \end{pmatrix} \Rightarrow \begin{pmatrix} Z \\ Z \\ J \\ R \end{pmatrix}$$

Third column:

$$\begin{pmatrix} V \\ N \\ S \\ A \end{pmatrix} \Rightarrow \begin{pmatrix} ! \\ D \\ Y \\ K \end{pmatrix}$$

Fourth column:

$$\begin{pmatrix} S \\ \eta \\ \eta \\ I \end{pmatrix} \Rightarrow \begin{pmatrix} I \\ Z \\ Z \\ S \end{pmatrix}$$

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

$$\Rightarrow \begin{pmatrix} K & Z & ! & I \\ J & Z & D & Z \\ Z & J & Y & Z \\ K & B & K & S \end{pmatrix}$$

Adding with the second key we have,

$$\begin{pmatrix} K & Z & ! & I \\ J & Z & D & Z \\ Z & J & Y & Z \\ K & B & K & S \end{pmatrix} + \begin{pmatrix} T & S & M & O \\ R & F & A & N \\ A & O & T & X \\ N & R & I & Y \end{pmatrix}$$

K + T = ?
Z + A = _
Z + S = I
J + O = E
! + M = Q
Y + T = M
I + O = F
Z + X = B

J + R = X
K + N = E
Z + F = !
B + R = P
D + A = E
K + I = B
Z + N = T
S + Y = J

Adding with the first key we have,

$$\begin{pmatrix} ? & I & Q & F \\ X & ! & E & T \\ \_ & E & M & B \\ E & P & B & J \end{pmatrix} + \begin{pmatrix} C & E & C & X \\ O & R & E & ! \\ N & E & \_ & ! \\ F & N & X & ! \end{pmatrix}$$

$\Rightarrow$? + C = !
_ + N = U
I + E = L
E + E = η
Q + C = R
M + _ = V
F + X = ,
B + ! = ,

X + O = W
E + F = P
! + R = N
P + N = ,
E + E = η
B + X = Z
T + ! = H
J + ! = V

Thus, $\begin{pmatrix} ! & L & R & , \\ W & N & \eta & H \\ U & \eta & V & , \\ C, & , & Z & V \end{pmatrix}$

We now shift the rows (R – L) using shift of nth row = $(n-1)$ shift.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

$$\begin{pmatrix} ! & L & R & , \\ H & W & N & \eta \\ V & , & U & \eta \\ , & Z & V & C \end{pmatrix}$$

Decrypting using Caesar cipher we have,

YES IT WORKS !!

Hence, the original text.

V. CONCLUSION

The improved method is a combination of Caesar cipher with row shift, column transformation and additional key(s) that provides secured and strong cipher. The improved system resulting from the merger of Caesar cipher, row shift, column transformation and addition of additional key(s) is becoming more complicated than some algorithms operated to work independently. The advantage of the system is that, it provides better security because even if some component ciphers are broken or some of the secret keys are recognized, the confidentiality of the original data can still be maintained.

REFERENCES

[1] Judson, W.T., (2010). Abstract Algebra Theory and Aplications, Austin State University, P. 100 – 101.
[2] Goyal, K. and Kinger, S. (2013). Modified Caesar cipher for better security enhancement, International Jouranal of Computer Application, 3, 28-29.
[3] Ajit, S., Nandal, A. and Malik, S. (2012). Implementation of Caesar cipher with Rail Fence for Enhancing Data security. International Journal of Advanced Research in Computer Software Engineering, 2(12), 78-80.
[4] Srikantaswamy, S.G. and Phaneendra, H.D. (2012). Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption. International Journal on Cryptography and Information Security (IJCIS), 2(4), 40-46.
[5] Stallings, W. Cryptography and Network security, principles and practice. Fifth edition, Prentice Hall, New York, pp. 243-323.
[6] AbuTaha, M., Farajallah, R.T. and Mohammed, O. (2011). Survey Paper: Cryptography is TheScience of Information Security. International Journal of Computer Science and Security, 5(3), 298-304.