Journal of Communications Technology, Electronics and Computer Science, Issue 8, 2016
ISSN 2457-905X

Modified Caesar Cipher using Rectangular Method For Enhanced Security

Priya Verma, Gurjot Singh Gaba, Himanshu Monga
Discipline of Electronics and Communication Engineering
Lovely Professional University
Phagwara, Punjab, India
himanshumonga@gmail.com

***Abstract*— The most challenging area in today's era is security over the network because now days all the industrialists, corporate sectors shares their precious information through internet. Researchers have designed various encryption techniques like Caesar cipher, play fair cipher, hill cipher, one time pad cipher, alpine cipher etc. to secure the information. Caesar cipher gets easily affected from any brute force attacker. By considering the cons of the existing Caesar cipher, a new technique is proposed in this paper which enhances its strength and puts stronger impact on the cipher text result which makes difficulty for a brute force attacker to determine the original plaintext back.**

***Keywords*— Cryptography, Encryption, Caesar cipher, Brute force attack, Plaintext, Cipher text.**

I. Introduction

CRYPTOGRAPHY i.e. 'secret writing' is the best way to protect our information from an attacker [1].Various key components of cryptography are plaintext, secret key, cipher text, encryption algorithm and decryption algorithm [10] as portrayed in figure 1. The original message which user wants to encrypt is called plaintext that is encrypted with a key called as secret key. Sender shares the secret key only with the receiver so that the information should stay protected. Broadly two types of attackers are identified i.e. Cryptanalysis and Brute force attacker. Brute force attacker tries all the possible combinations of keys until the plaintext is recovered from the cipher text [3].

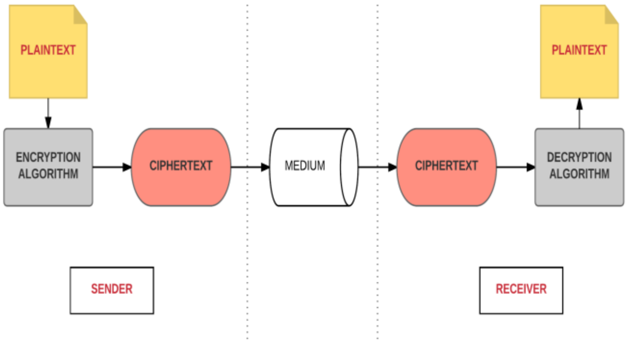

Fig. 1. Concept of Cryptography.

Among many encryption techniques, Caesar Cipher [2] is one of the techniques used to encrypt the information. In this technique, each character of the plaintext is shifted with some mounted number of locations down the alphabet. The shifting of characters in the Caesar cipher depends on the key value. Key value lies between 1 to 26. Due to less number of keys in Caesar cipher, any brute force attacker can try all the possible combinations of key sets and evaluates the original message back easily [4]. It provides very less security of information. So to overcome the limitations of the existing techniques of Caesar cipher, a new technique is proposed in this paper called as MCC (Modified Caesar Cipher). The existing Caesar Cipher [7] was conceptualized in the past by using simple criteria:

PLAINTEXT	GET READY FOR THE PARTY OK
KEY	3
CIPHERTEXT	JHW UHDGB IRU WKH SDUWB RN

II. Caesar Cipher & Its Extensions

Yashpal Singh Rajput (2014), et al. in paper entitled "An Improved Cryptographic Technique to Encrypt Text using Double Encryption" discussed an improved scheme to encrypt the plaintext for highest security. In this paper, a new encryption technique is created in which Caesar cipher is integrated with Hill cipher algorithm to make encryption technique more secure and stronger than earlier techniques. Initially, some improvements are applied on the existing Caesar cipher by applying dynamic key for each letter in a string. The dynamic key depends on the length of the string to be encrypted and for each letter in the string to be encrypted key changes as encryption proceeds through the length of the string. The use of variable and dynamic key for each letter makes the system more secure and unbreakable. Secondly, in phase 2, classical hill cipher is applied which uses 3 X 3 key matrix for encryption. Use of Hill cipher makes the string unstructured due to which it becomes difficult to get the original text string. So the message encrypted in this technique cannot be decrypted by cryptanalyst and brute force attack technique [11].

Ochoche Abraham (2012**),** et al. in paper entitled "An improved Caesar cipher algorithm (ICC)" proposed an idea to strengthen the Caesar cipher by creating cipher text after removing the space in plaintext. The positions of the spaces are recorded before removal. Latter, plaintext is converted into cipher text by Caesar cipher technique. Thus, in this technique, we get two results one is cipher text and other is integer value that represent the location of space. During decryption process, firstly the text is decrypted using the Caesar decryption procedure and then spaces are inserted in the plain text according to integer value. Main strength of ICC is that it requires less computing resource. Due to this property, it finds its applications for the low powered devices likes mobiles [5].

Shahid Bashir Dar (2014), et al. in paper entitled "Enhancing the Security of Caesar Cipher Using Double Substitution Method" demonstrates that adding complexity in functioning of the algorithm can strengthen its impact to withstand against severe attacks. Double substitution is performed in order to make Caesar cipher more secure and stronger so that it can be protected from cryptanalyst and brute force attack. Initially, the plaintext is reshaped in the form of matrix. Order of the columns is determined by the key 'K_1'. By reading the message column by column, we get the cipher text CT_1. Then shift each character of the CT_1 by using key value k_2 which gives the final ciphertext CT_2. The decryption is carried out in the reverse manner. This method uses very less structured permutation and claims to overcome the limitations of simple Caesar cipher [9].

III. Modified Caesar Cipher (MCC)

In existing Caesar cipher, every character of the plaintext is interchanged by a character with some other character in the language. It has only 26 possible set of keys to encipher the data. So by trying all the possible set of keys, brute force attacker can easily attack on it [6]. To overcome the limitations of already existing Caesar ciphers, a new technique is proposed in this paper which is coined as MCC.

A. Encryption methodology

The process involves the following working steps:-

a) Write the plaintext in the form of rectangle row by row.
b) Read off the rows in column wise in the descending order of the key values K_1.
c) We get the first partial cipher text CT_1.
d) Start writing the CT_1 in the form of rectangle row by row in reverse order.
e) Again, read off the rows in column wise in descending order of the key values K_2.
f) We get the second partial cipher text result CT_2.
g) Divide the entire row into equal parts.
h) Keep the first, last and the middle column as it is and interchange the rest of the columns diagonally.
i) Shift the characters of the first row with the following pattern described below:

Characters	1st	2nd	3rd	4th	5th	6th	7th
Locations	3	1	8	6	9	4	5

j) Shift the characters of the second row with the following pattern defined below:-

Characters	1st	2nd	3rd	4th	5th	6th	7th
Locations	6	2	4	9	7	8	1

k) Shift the characters of the third row with the following pattern defined below:-

Characters	1st	2nd	3rd	4th	5th	6th	7th
Locations	4	6	1	8	9	7	3

l) At the last, combine them all in one row. We get final cipher text result CT_3.

B. Decryption methodology

In many cryptography techniques, the decryption process is different from the encryption process which creates trouble for the recipient. But in the proposed technique the decryption process is just the inverse of the encryption process.

IV. Results and Discussions

The most important challenge is to transmit the message successfully over the network without disclosure of information to the third party [8]. The following example described below shows the enhanced form of results of the cipher text obtained after applying the proposed technique MCC which improves the performance as compared to existing Caesar cipher and does not allow the attacker to crack the message easily.

A. Encryption Process

Let us suppose the key and the message we want to encrypt is:

MESSAGE	GET READY FOR THE PARTY OK
KEY (K_1)	2 7 5 6 4 3 1

a) First Stage of Encryption

KEY	**2**	**7**	**5**	**6**	**4**	**3**	**1**
PLAINTEXT	**G**	**E**	**T**	**R**	**E**	**A**	**D**
	Y	**F**	**O**	**R**	**T**	**H**	**E**
	P	**A**	**R**	**T**	**Y**	**O**	**K**

First Partial ciphertext result (CT_1) is:

EFA RRTTO RET YAH OGYPD EK

b) Second Stage of Encryption

MESSAGE	EFA RRTTO RET YAH OGYPD EK
KEY (K_1)	8 9 14 12 17 15 13

KEY	**8**	**9**	**14**	**12**	**17**	**15**	**13**
CIPHERTEXT	**K**	**E**	**D**	**P**	**Y**	**G**	**O**
	H	**A**	**Y**	**T**	**E**	**R**	**O**
	T	**T**	**R**	**R**	**A**	**F**	**E**

Second Partial ciphertext result (CT_2) is:

YEA GRFDY ROO EPT REATK HT

Divide the (CT_2) into equal parts

A	→	YEAGRFD
B	→	YROOEPT
C	→	REATKHT

Keep the first, last and middle column as it is and then interchange the rest of the columns diagonally.

X	→	YORGPED
Y	→	YAEOFRT
Z	→	RORTPET

Shift the characters of X, Y and Z according to the pattern defined above in the encryption process.

P	→	BPZMYII
Q	→	ECIXMZU
R	→	VUSBYLW

Final cipher text is obtained after combining and writing the P, Q and R in one row.

Final ciphertext Result:

BPZ MYIIE CIX MZU VUSBY LW

B. Decryption Process

CIPHERTEXT:- BPZ MYIIE CIX MZU VUSBY LW

Divide the cipher text result into equal parts :

A	→	BPZMYII
B	→	ECIXMZU
C	→	VUSBYLW

Subtract the number of locations from the character set of A, B, and C according to the pattern defined in the encryption. We get the result as

D	→	YORGPED
E	→	YAEOFRT
F	→	RORTPET

Keep the first, last and middle column as it is and interchange the rest of the columns diagonally, we get,

G	→	YEAGRFD
H	→	YROOEPT
I	→	REATKHT

Read it off into a single row. We get the first partial plaintext result:

MESSAGE	YEA GRFDY ROO EPT REATK HT
KEY (K_1)	**8 9 14 12 17 15 13**

YEA GRFDY ROO EPT REATK HT

Apply the next procedure to obtain the plaintext.

a) First stage of decryption

The second partial plaintext result obtained after writing it into single row starting from the last character of the rectangle in the reverse order is presented below

MESSAGE	EFA RRTTO RET YAH OGYPD EK
KEY (K_1)	**2 7 5 6 4 3 1**

KEY	**2**	**7**	**5**	**6**	**4**	**3**	**1**
PLAINTEXT	**G**	**E**	**T**	**R**	**E**	**A**	**D**
	Y	**F**	**O**	**R**	**T**	**H**	**E**
	P	**A**	**R**	**T**	**Y**	**O**	**K**

EFA RRTTO RET YAH OGYPD EK

b) Second stage of decryption

The original plaintext (PT_1) is obtained after writing it into single row starting from the first character of the rectangle.
Original Plaintext obtained from the process is:

<GET READY FOR THE PARTY OK>

TABLE I. Feature Comparison of the Existing and Proposed Technique.

EXISTING CAESAR CIPHER [7]	MODIFIED CAESAR CIPHER (PROPOSED TECHNIQUE)
Single value of key is used for shifting the characters of plaintext	Multiple values of keys are chosen for shifting purpose
It can be easily crypt analyze	It is difficult to crypt analyze
Attacker can easily decrypt the key	Decryption of the key is tough
Provides less security	More secure
Less complexity	More complexity
Brute force attack is possible	Brute force attack is not possible

Various differences between the existing Caesar cipher and proposed technique are discussed in Table I. Our proposed technique is more secure because of its more complexity in the algorithm, due to this brute force attack is also not possible while the existing algorithm of Caesar cipher has less complexity and can be easily cracked by an attacker. From the all discussions, it is clear that the proposed technique has more lifetime and efficient in terms of reliability and security.

V. Conclusions

Caesar cipher is a very simple technique used for encryption in cryptography, but it is insecure due to less number of keys, and it is more prone to attacks. To surpass the limitations of the existing Caesar cipher algorithms, a new technique is designed in this paper named as MCC. From the discussions, we can clearly see that our proposed technique (MCC) has performed both the substitution and transposition on the plaintext message and used two different keys for the encryption which makes the ciphertext stronger and secure that could not be easily determined by an attacker.

References

[1] R. Mane "A Review on Cryptography Algorithms, Attacks and Encryption Tools,"*International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, no. 9, pp.8509-8514, 2015.

[2] G. Gupta, R. Chawla, "Review on Encryption Ciphers of Cryptography in Network Security,"*International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 7, pp.1-26, 2012.

[3] S.Chandra, "Acomparative survey of Symmetric and Asymmetric Key Cryptography," *International conference on Electronics, Communication and Computational Engineering (ICECCE)*, Hosur, pp. 83–93, 2014.

[4] S. Shakti, "Encryption using different techniques," *International Journal in Multidisciplinary and Academic Research (SSIJMAR)*, vol. 2, no. 1, pp. 1-9, 2013.

[5] O. Abraham, Ganiyu O. Shefiu, "An improved Caesar cipher algorithm," *International Journal of engineering science and advanced technology*, vol. 2, pp.1199-1202, 2012.

[6] Lim Chong Han, N.M. Mahyuddin, "An Implementation of Caesar Cipher and XOR Encryption Technique in a Secure Wireless Communication," *2^{nd} International conference on Electronic Design (ICED)*, Penang, pp.111-116, 2014.

[7] Rajan, D. Balakumaran, "Advancement in Caesar cipher by randomization and delta formation," I*nternational conference on Information communication and Embedded systems (ICICES)*, Chennai, pp.1-4, 2014.

[8] K. Goyal, S. Kinger, "Modified Caesar Cipher for Better Security Enhancement," *International Journal of Computer Applications*, vol. 73, no. 3, pp. 27-31, 2013.

[9] S.B. Dar, "Enhancing the Security of Caesar Cipher Using Double Substitution Method," *International Journal of Computer Science & Engineering Technology*, vol. 5, no. 7, pp.772-774, 2014.

[10] William Stallings, "Cryptography and Network Security: Principles & Practices", New York, NY: Pearson Education, 2006.

[11] Y. S. Rajput, "An Improved Cryptographic Technique to Encrypt Text using Double Encryption," *International journal of Computer Applications*, vol.86, no. 6, pp.24-28, 2014.