Enhancing the Security of Caesar Cipher Algorithm by Designing a Hybrid Cryptography System

Md. Ebrahim Hossain
Assistant Professor,
Department of Computer Science and Engineering
Leading University, Sylhet-3110, Bangladesh

ABSTRACT

Cryptography is the art of protecting information by transforming it into an unreadable format. It is about constructing and analyzing protocols that prevent third parties or the public from reading private message. Caesar cipher is a substitution cipher that implements monoalphabetic substitutions. It is a very old encryption technique and major disadvantage of caesar cipher is the repeating nature of its keys. In this paper an advanced encryption algorithm is proposed which improves the security of caesar method by combining traditional playfair approach and a modern cipher method like stream cipher. When applying the proposed method, three different key is used which makes the algorithm more strong.

Keywords

Substitution Cipher, Plaintext, Ciphertext, Key, Stream Cipher.

1. INTRODUCTION

Data Communication is the process of exchanging information between sender and receiver via some form of transmission medium. It includes five components for a successful data communication system such as Message, Sender, Receiver, Transmission medium and Protocol.

Effectiveness of a data communication process vastly depends on the security of data provided by the system. Three security goals of any system is Confidentiality, Integrity and Availability. Confidentiality is the most common aspect of information security. It allows authorized users to access sensitive and protected data. The data sent over the network should not be accessed by any unauthorized users. Integrity confirms that changes need to be done by the authorized entities only and through authorized mechanisms, nobody else should modify the data. The third aspect of data security is the data must be available to the authorized users, information is useless if it cannot be accessed.

Security of a system can be breached using two types of attacks. One is passive attack and the other is active attack. In passive attack the third party attempts to learn or make use of the information from the system but does not affect the system resource. This type of attack is difficult to detect as they do not involve any alteration of data. On the other hand active attack attempts to alter system resources. To avoid these types of attack, different security mechanism like encipherment, digital signature, data integrity, authorization exchange, routing control, access control etc can be implemented in a system.

Here comes the need of hiding original message from third party and cryptography does this using different techniques. Encryption is the process of transforming information from readable to unreadable format and Decryption is the process of transforming data from unreadable format to readable format. Some sort of key is used by cryptographic algorithms which is string of bits to transform plaintext to ciphertext and vice versa. If same key is used for both encryption and decryption process, it is called symmetric cryptography. And if different key is used, then it is called asymmetric cryptography. In case of asymmetric cryptography one key is called public key which is known to all and the other key is called private key which is known only to particular person.

Symmetric encryption also referred to as conventional encryption is of two types. One is substitution technique and the other is transposition technique. Substitution technique is the one in which the letters of the plaintext are replaced by other letters or by numbers or symbols. In monoalphabetic substitution cipher, relation between a character in the plaintext to a symbol is ciphertext is always one to one. On the other hand each occurrence of a character in polyalphabetic substitution cipher may have different substitute. Transposition technique is nothing but performing some sort of permutation on the plaintext letters.

2. RELATED WORKS

This paper discusses the combination of caesar cipher and polyalphabetic substitution cipher to enhance the security of caesar mechanism. Previously different researches had searched for different combinations.

Shivam Vatshayan, Raza Abbas Haidri and Jitendra Kumar Verma (2020) introduced a new hybrid security cipher by combining Polybius cipher and vignere cipher. [1]

Fairouz Mushtaq Sher Ali and Falah Hassan Sarhan (2014) showed in their paper the combination of modern cipher method like stream cipher with vignere approach. They also used binary form instead of characters where the plaintext, ciphertext and key are string of bits.[2]

O.E. Omolara, A.I. Oludare and S.E. Abdulahi (2014) proposed a hybrid version of classical and modern cipher properties. A combination of caesar cipher and vignere cipher with diffusion and confusion is proposed in this paper. [3]

Fairouz Mushtaq Sher Ali (2014) proposed an advanced encryption algorithm by combining with modern cipher method like stream cipher to improve the security of playfair method. It used bit oriented method instead of character oriented method where the plaintext, ciphertext and the key are strings of bits. [4]

3. ENCRYPTION PROCESS

The structure of proposed encryption algorithm is stated below.

Step 1: Start

Step 2: Read the plaintext, P

Step 3: Read Keyword, K1, K2 and K3 (Where K3 is the UNICODE of K2)

```
Step 4:   Apply Caesar equation $C = (P + K1)\ mod\ 26$ to encipher the plaintext.

Step 5:   Apply Playfair cipher algorithm on the output of step 4 using the second key, k2.

Step 6:   Divide the ciphertext (from step 5) into two equal part.

Step 7:   Apply Caesar equation $C = (P + K1)\ mod\ 26$ to encipher the first half.

Step 8:   Apply stream cipher to encipher each character in the second half as follows.
              i.   Convert each character to ASCII value and then find the corresponding binary value of it.
              ii.  Enciphering the characters using $C = (P \oplus K3)$ equation.
              iii. Convert the resulted binary numbers to its corresponding ASCII value and then to characters.

Step 9:   Merge the characters of step 7 and step 8.
Step 10:  End.
```

Note: In step 8, it may result ASCII values of some nonprintable characters, in that case special symbols are used to represent those ASCII values. [5]

3.1 Playfair Cipher Algorithm

In this proposed technique Playfair cipher algorithm is used in step 5. This algorithm was invented in 1854 by Charles wheatstone, but was name after Lord Playfair who promoted the use of cipher. The algorithm is stated below.

```
Step 1:   Create 5*5 matrix that is called grid of letters. The matrix is made by inserting the values of key and remaining alphabets into the matrix (row wise from left to right), where letter I and J will be combined together.

Step 2:   Convert the text into pairs of alphabet.
              i.   Pair cannot be made with same letters, in this case break the letters in single and add 'x' to the previous letter.
              ii.  If the letter is standing alone in the process of pairing, then add 'z' with the letter.

Step 3:   Code will be formed using 3 rules.
              i.   If both the alphabets are in the same row, replace them with alphabets to their immediate right.
              ii.  If both alphabets are in same column, replace them with alphabets immediately below them.
              iii. If not in same row or column replace them with alphabets in the same row respectively, but at other pair of corners.
```

3.2 Caesar Cipher

Caesar cipher is also called shift cipher or additive cipher. Each letter in the plaintext is replaced by a letter corresponding to a number of shifts in the alphabet. It is a monoalphabetic cipher. If the letters A-Z is replaced by the numbers 0-25, then the caesar encryption E using the key K can be written as

$$E_i = (P_i + K_i)\ mod\ 26 \text{ -------------------------------------- (i)}$$

And decryption D using the key k is

$$D_i = (E_i - K_i) mod\ 26 \text{ --------------------------------------- (ii)}$$

Here same key is used for both encryption and decryption.

3.3 Example

To illustrate the proposed encryption algorithm, the followings are considered.
Plaintext = ATTACK POSTPONED
Key, K1 = 3
Key,K2 = INTERNET
Key,K3=10010011001110101010010001011010010100111010 001011010100 (UNICODE of K2)
The following table is used to convert letters into numbers.

Table 1: Converting Letters into Numbers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25

Now implementing vignere equation on the plaintext in the following table.

Table 2: Caesar equation Implementation on Plaintext

Plaintext	Plaintext's value (P)	Key (K1)	Ciphertext's Value	Ciphertext
A	0	3	3	D
T	19	3	22	W
T	19	3	22	W
A	0	3	3	D
C	2	3	5	F
K	10	3	13	N
P	15	3	18	S
O	14	3	17	R
S	18	3	21	V
T	19	3	22	W
P	15	3	18	S
O	14	3	17	R
N	13	3	16	Q
E	4	3	7	H
D	3	3	6	G

So, the ciphrtext after implementing caesar equation is

DWWDFNSRVWSRQHG

Now implementing playfair algorithm using K2 on the above ciphertext. The playfair grid will be as following.

Table 3: Playfair Grid

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

Now Pairing the ciphertext we get the following pairs
DW WD FN SR VW SR QH GZ
Using Playfair algorithm on the pairs we get
BY YB BR EU WX EU KP MV
So, now the ciphertext is BYYBBREUWXEUKPMV.

According to the proposed algorithm we have to divide the above ciphertext into two equal half. Then implement caesar equation on the first half.
First half = BYYBBREU
Second Half = WXEUKPMV
Now implementing caesar equation on the first half using the same key we get.

Table 4: Implementing Caesar Equation on First Half

Plaintext	B	Y	Y	B	B	R	E	U
Plaintext's value (P)	1	24	24	1	1	17	4	20
Key (K1)	3	3	3	3	3	3	3	3
Ciphertext's Value	4	1	1	4	4	20	7	23
Ciphertext	E	B	B	E	E	U	H	X

Ciphertext for the first half from the above table is EBBEEUHX

Now from the proposed algorithm we need to construct the following table to encipher the second half.

Table 5: XOR Operation of second half with K3

Plain text (P)	ASCII equivalent of P	P_{Bin}	K3	$C_{Bin} = (P_{Bin} \oplus K2$	ASCII equivalent of C_{Bin}	Cipher text
W	87	1010 111	1001 001	0011110	30	(RS)
X	88	1011 000	1001 110	0010110	22	(SYN)
E	69	1000 101	1010 100	0010001	17	(DC1)
U	85	1010 101	1000 101	0010000	16	(DLE)
K	75	1001 011	1010 010	0011001	25	(EM)
P	80	1010 000	1001 110	0011110	30	(RS)
M	77	1001 101	1000 101	0001000	8	(BS)
V	86	1010 110	1010 100	0000010	2	(STX)

After combining the ciphertext of first half and second half we get the final ciphertext as
EBBEEUHX(RS)(SYN)(DC1)(DLE)(EM)(RS)(BS)(STX)

4 COMPARISON WITH THE EXISTING METHODS

In general the existing combination ciphers combine substitution ciphers with transposition cipher which is based on classical ciphers only. This type of cipher makes the decryption process much easier for the attacker. On the other hand, there is no use of binary key in the classical cipher which makes the technique more vulnerable. In our proposed encryption algorithm, we combined classical cipher like caesar method with another one called playfair method. Then the resulting cipher is divided into two parts where the first part is enciphered using caesar method and the second part is enciphered using the UNICODE of the third key. The whole process has made the encryption and decryption much difficult.

5 CONCLUSIONS

The paper proposes a new version of caesar cipher based on the combination of caesar method and playfair method where binary key is used to make the encipherment more difficult. The proposed technique is supposed to secure more security than the traditional technique.

6 REFERENCES

[1] Shivam Vatshayan, Raza Abbas Haidri, Jitendra Kumar Verma (2020). Design of Hybrid Cryptography System based on Vignere Cipher and Polybius Cipher. Published by International Conference on Computational Performance Evaluation, North Eastern Hill University, Shilong, Meghalaya, India.

[2] Fairouz Mushtaq Sher Ali, Falah Hassan Sarhan. Enhancing Security of Vignere Cipher by Stream Cipher. Published by International Journal of Computer Applications (0975-8887), Volume-100, No. 1, August 2014.

[3] O.E. Omolara, A.I. Oludare and S.E. Abdulahi (2014). Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication. Published by Computer Engineering and Intelligent Systems. ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online), Vol.5, No.5, 2014.

[4] Fairouz Mushtaq Sher Ali (2014). Enhancing the Security of Playfair Cipher by Stream Cipher. Published by Journal of AL Qadisiyah for Computer Science and Mathematics, Volume-6, No-2, Year-2014.

[5] Self-Study: ASCII Symbol of non-printable characters. URL: https://en.wikipedia.org/wiki/C0_and_C1_control_codes#SOH. Retreived Date: 15 July, 2021.