ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

A Novel & More Secure Caesar Cipher

Faizan Javaid Dar[1], Asif Javeed[2], Aamir Farooq Mir[3], Shahid Mohi ud Din[4]

Student, Department of Computer Engineering, SSM College of Engineering, Pattan, Kashmir, India[1,2,3]

Assistant Professor, Department of Computer Engineering, SSM College of Engineering, Pattan, Kashmir, India[4]

ABSTRACT: Cryptography is an art of secret writing. Plain text is converted into cipher text using different techniques.
Substitution and transposition are two techniques used to encrypt plain text into a non-readable cipher text. Caesar cipher is a basic substitution cipher. In this paper we have proposed a novel and more secure Caesar cipher. A single columnar transposition followed by a reverse operation and substitution is applied to get a more secure Caesar cipher.

KEYWORDS:Caesar Cipher, cryptography, symmetric & asymmetric ciphers, encryption, decryption.

I. INTRODUCTION

We are familiar that our society is completely based on the communication. Communication is the process of transmitting information from Source to destination. The Information to be transmitted must be secure in presence of adversaries i.e. from third parties. For achieving security goals such as confidentiality, integrity, and availability and preventing attacks, two techniques are prevalent today: cryptography and steganography. In this paper we are going to discuss only cryptography which is a general technique.

Cryptography is the art and science of protecting information by encrypting it, called Cipher Text and only those who have secret key can decipher or decrypt the cipher text into plain text. In other words, we can define cryptography as the concealing of a message by enciphering.

Types of Ciphers

A cipher is an algorithm for performing encryption and decryption. Ciphers are broadly classified into two categories:

1. Symmetric key ciphers:

In this type of cipher same key is used for both encryption and decryption. Both sender and receiver can use the same key means the secret key is shared between two persons. This type of cipher is also called as secret key ciphers. There are two broad categories of symmetric key ciphers one is Traditional ciphers and second is Modern ciphers.

- Traditional Ciphers*:* these types of ciphers are simple and character oriented ciphers, not much secure as that of modern ciphers. Traditional ciphers are classified into Substitution ciphers and Transposition ciphers.
  a) Substitution Ciphers*:* Replacement of symbols with another is performed in this type of cipher. This sub type of Symmetric key cipher has been classified further into:

Monoalphabetic Ciphers: There is a one to one relation between the symbols from the plaintext to the cipher text. Additive cipher or shift cipher is one of the simplest monoalphabetic cipher. Additive Ciphers are also sometimes referred as Caesar Cipher [1].

Polyalphabetic ciphers: There is a one to many relation between the symbols from the plaintext to the cipher text. Autokey cipher is one of the simple polyalphabetic cipher.

b) Transposition ciphers: Reordering of symbols is performed in this type of cipher. In other words, characters or symbols in the plaintext are rearranged so that the cipher text can be formed.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

- Modern ciphers*:* These types of ciphers are complex and bit-oriented ciphers, secure as compared to the traditional ciphers. The information to be encrypted Is not only just text, it can be numbers, graphics, audio and video as well. Data to be encrypted is first converted into stream of bits. A Modern cipher can be either a block cipher or a stream cipher [3].

2. Asymmetric key cipher**:**

In this type of cipher separate secret keys are used: one is private key and other is public key. Here in this type the secret key is not shared unlike in symmetric key ciphers.

Mathematical Representation

Consider an example of Caesar ciphers, it is one of the simplest type of substitution ciphers, in which simple shifting of letters from plaintext is done by some specific value down the alphabet. Consider the shifting key as 2 means we have to shift each letter of the plaintext by value 2 down the alphabet i.e. A will be replaced by 'C', 'B' will be replaced by 'D' and so on.

Consider the plaintext as: Bring The Book.

Shift key: 2

Then the encrypted information will be: 'DtkpiVjgDqqm'.

Therefore, the cipher text for the above given plaintext with shift key 2 is: DtkpiVjgDqqm.

The decrypted information will be obtained by simply subtracting the shift key value which is 2 in above example.

All the operations done in the monoalphabetic ciphers are modulo 26. Therefore, each letter can be translated to numeric values, for letter 'A' the translation to numeric value will be 0, similarly, for letter 'B' the translation to numeric value will be 1 and so on. For letter Z the translation to numeric value will be 25.

Let E(P) be the Caesar cipher encryption function, then mathematically E(P) can be represented as:

$$E(P) = (P + S) \bmod 26$$

Where S is the shift key for the letter P. P represents plain text letters.

Similarly, let D(C) be the Caesar the cipher decryption function, the mathematically:

$$D(C) = (C - S) \bmod 26$$

Where C represents the cipher text letters.

Caesar Ciphers and its limitations

Caesar cipher is one of the oldest and simplest strategy for encrypting information, named after Julius Caesar. It is a type of substitution cipher in which plain text is encrypted by simply shifting plaintext letters to certain number of places down the alphabet, the shifting is decided by key or secret key. It is also called shift cipher.

Limitations:

1. More prone to attacks like frequency analysis attack.
2. An encrypted message has only 26 possibilities, so an experienced cryptobreaker could decode the code easily by brute force attack.

II. PROPOSED ALGORITHM

The proposed algorithm will enhance not only security of Caesar Cipher but will also overcome above mentioned limitation to a great extent. The tasks of encryption and decryption go one after another so the proposed system comprises two algorithms one for encryption and other for decryption.

A. *Encryption Algorithm:*

1. Get plaintext as input.
2. Write the plaintext in a rectangular fashion, column by column, order of the text will be determined by key k1.
3. Read off the message row wise beginning from the first row. We get the first cipher text.
4. Reverse the cipher textobtained in step 3.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

5. Use key k2 to shift each character of the cipher text obtained in step 4.
6. The obtained cipher text in step 5 will be our final cipher text.

B. Decryption Algorithm:

1. Get final cipher text as input.
2. Use key k2 to reverse shift each character of the inputted cipher text.
3. Reverse the cipher text obtained in step 2.
4. Use key k1 and arrange the obtained cipher text from step 3 column wise to get the order.
5. Again use key k1 and arrange the obtained text from step 3 in the same order as of step 4.
6. Read off the message column wise.
7. The output of the step 6 will be actual decrypted cipher text.

III. EXAMPLE

A. Encryption:

1. Suppose the inputted plaintext is:

HELLOCRYPTOGRAPHY

2. Let the Key k1 be 3 4 1 2 5.

The plaintext will be arranged in rectangular fashion, column by column as

Key K1	Plaintext			
3	H	C	O	H
4	E	R	G	Y
1	L	Y	R	
2	L	P	A	
5	O	T	P	

3. Read off the text row wise.

HCOHERGYLYRLPAOTP

4. Reverse the obtained cipher text.

PTOAPLRYLYGREHOCH

5. Use key k2 = 2 (say) to shift each character of above text.

RVQCRNTANAITGJQEJ

6. The output of step 5 is the final cipher text

i.e. Cipher text = **RVQCRNTANAITGJQEJ**

B. Decryption:

1. The inputted cipher text is: **RVQCRNTANAITGJQEJ**
2. Use key k2 = 2 (as in encryption) to reverse shift the characters.

PTOAPLRYLYGREHOCH

3. Reverse the above cipher text.

HCOHERGYLYRLPAOTP

4. Use key k1 same as in encryption and arrange the character string column wise.

Key k1	cipher text			
3	H	R	R	T
4	C	G	L	P
1	O	Y	P	
2	H	L	A	
5	E	Y	O	

This implies that first two rows will contain four columns and remaining three rows will contain only three columns.

5. Arrange the obtained text from step 3 by using key k1 row wise, in the same order as in step 4.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

Key k1	cipher text			
3	H	C	O	H
4	E	R	G	Y
1	L	Y	R	
2	L	P	A	
5	O	T	P	

6.. Read off the message column wise, which is:

HELLOCRYPTOGRAPHY

7.. The output obtained from step 6 is original plain text.

IV. ADVANTAGES & DISADVANTAGES OF PROPOSED ALGORITHM

A. *Advantages of proposed algorithm:*

The proposed algorithm for Caesar ciphers has the following advantages over traditional Caesar ciphers.

1. Simple method of concealing the message with great security.
2. Less structured permutations are used.
3. Difficult to break the cipher text.
4. Brute force attacks are not possible.
5. Order determination problemof matrix for decryption as in [2] is overcomed.

B. *Disadvantages of proposed algorithm:*

1. Difficult to implement as compared to traditional Caesar ciphers.
2. Time complexity is increased because of finding the order of the text matrix.

REFERENCES

1. Data Communications and Networking 5E by Behrouz A. Forouzan.
2. Shahid Bashir Dar,'Enhancing The Security of Caeser Cipher Using Double Substitution Method', International Journal of Computer Science & Engineering Technology (IJCSET.), Vol. 5 No. 07 Jul 2014, pp. 772-774.
3. http://practicalcryptography.com/ciphers/caesar-cipher/.