Improved Caesar Cipher Algorithm Using Multistage Encryption

[1]Greetta Pinheiro, [2]Shruti Saraf
[1,2]SCOPE, VIT University, Vellore, Tamil Nadu, India

Abstract
Cryptographic algorithms play an important role in the security domain. In this system, in order to increase the security of the Caesar cipher, some basic mathematical calculations are performed on the cipher text in order to make it strong. The proposed new system is case sensitive. The encryption and decryption of the plain text is done by making use of the face values and positional values of the corresponding characters as the key. The multistage encryption is imposed on the plain text which indeed improves the security of the plain text and secures it from brute force attack, pattern matching and frequency analysis to an extent. Further discuss the need of the additional methodology to the existing scenario.

Keywords
Cryptography, Caesar Cipher, Brute Force Attack, Pattern Matching, Frequency Analysis, Encryption and Decryption, Key

I. Introduction

Now a day when internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. One essential aspect for secure communication is that of cryptography.

Cryptography is mainly used in transmitting the text which is sometimes called as the plaintext or the clear text from one end to the other. It includes techniques such as merging the words with some images, transforming in microdot form etc. to securely transmit the text.

But in today's computer centric world, cryptography is mainly dealing with the scrambling of the plaintext into a form which is not meaningful and does not reveal any information that is being transmitted called cipher text and then later converting it back to the plaintext. The process of converting plaintext to cipher text is called encryption and then converting the cipher text back to the plaintext is known as decryption. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Cryptography is about constructing and analyzing protocols that block adversaries. Various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography [10].

Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography also include ATM cards, computer passwords, and electronic commerce [9].

Cryptographic algorithms make use of Caesar cipher which is also known as a shift cipher, is one among the widely used cipher text mechanisms [8]. It is a substitution cipher where each character in the original message (called the plaintext) is replaced with a letter that is some number of positions down in the alphabet [2-3].

Among all the other cipher techniques, Caesar cipher is the easiest to break. Since the shift has to be a number between 1 and 25, one can simply try each possibility and see which one results in a piece of readable text. If it happens to be known a piece of the cipher text, then it is easy for a person to guess the key and hence the plaintext.

In shot Caesar ciphers is vulnerable to brute force attack, pattern matching and frequency analysis. Multiple encryptions and decryptions on the same cipher text provide no additional security.

To increase the security of the Caesar cipher, some basic mathematical calculations are performed on the cipher text in order to make it strong. The encryption and decryption of the plain text is done by making use of the face values and positional values of the corresponding characters as the key [1].

The multistage encryption is imposed on the plain text which indeed improves the security of the plain text and secures it from brute force attack, pattern matching and frequency analysis to an extent [4].

II. Overview of the Proposed System

The main focus of this system is to increase the security of the basic Caesar cipher in terms of pattern matching, frequency analysis and brute force attack. In order to achieve this, the proposed system is capable of handling case sensitive plaintext. Since the classical Caesar cipher is not case sensitive and hence for one particular shift for a plaintext the corresponding cipher text is always the same. Whereas in this system, if one toggles with the upper or the lower case letters in one plaintext, the corresponding cipher text will be different hence covering a wide range of plaintext cases.

In the encryption side, we have used 3 stages of encryption. The first stage of encryption is based on the basic Caesar cipher algorithm with shift + 1 as the substitution [8]. We are using face values and position values in our further computation where face values are the values assigned to a particular character say, A-1, B-2.…Z-26, a-27, b-28.…z-52. These face values are fixed for the corresponding letter [1].

The position values are assigned based on the position of the corresponding letter in the plain text. In the second stage, we assign face values and position values to each individual letters of the stage 1 encrypted text. The sum of the obtained face values is also been calculated.

The stage 2 encrypted text is obtained by subtracting the face values from the sum which was calculated earlier. The third stage encryption is done by subtracting the positional values from the stage 2 encrypted text to obtain the final cipher text which is sent to the receiver along with the sum of the face values as the key.

The decryption also includes 3 stages. In the first stage, the position values are added to the obtained cipher text. In the second stage, the above obtained stage 1 decrypted text is subtracted from the key as received from the sender.

The result will be the face values of the corresponding letters which is the stage 2 decryption. These face values are converted back to its corresponding fixed character. The third stage decryption uses the basic Caesar cipher algorithm with shift -1 as a substitution technique. Hence the plain text is obtained.

III. Design of the proposed system

A. The Encryption Algorithm:-

1. Transform the plain text using basic Caesar cipher algorithm.
2. Use the cipher text obtained from step (1) and do the following:
- Assign Face values and position values to each individual letters in the cipher text.
- Sum up the individual face values of all the letters in the cipher text.
- Subtract the individual face value of each letter of the cipher text from the above obtained sum.
- Now, subtract the position values of each of the corresponding letters of the cipher text obtained from step (2c).
3. The obtained cipher text is sent to the receiver along with the sum of face values.

B. Decryption Algorithm:-

1. Do the following on the received cipher text:
- Add the position values of each corresponding letter to the cipher text as received from the sender.
- Subtract each corresponding values obtained from step (1a) from the sum received along with the cipher text to get the face value.
- Transform the obtained face values to its corresponding alphabets.
2. Apply the basic Caesar cipher decryption to obtain the plain text.

IV. Implementation

The steps involved in the implementation of the proposed system is as follows –

A. Encryption –

The plain text chosen for the encryption is CrYPtOgrAPhy

Initial step is to make use of the basic Caesar cipher to convert the given plaintext into its corresponding stage 1 cipher text having displacement +1. (Refer fig. 1)

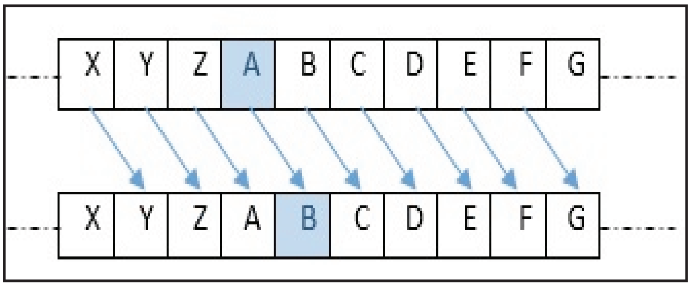
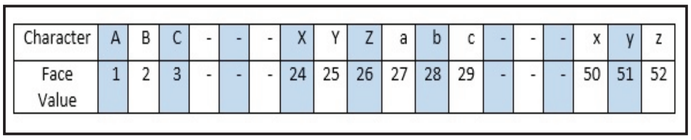


Fig. 1: The Classical Caesar Cipher With Shift +1

The position values are assigned corresponding to each letter of the plain text.

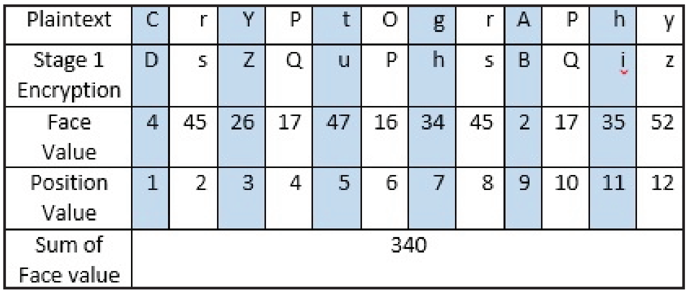
The face values are assigned to each letter of the stage 1 cipher text (Refer fig. 2)



Character	A	B	C	-	-	-	X	Y	Z	a	b	c	-	-	-	x	y	z
Face Value	1	2	3	-	-	-	24	25	26	27	28	29	-	-	-	50	51	52

Fig. 2: Face Values of Each Letter

Find the sum of face values (Refer fig. 3)

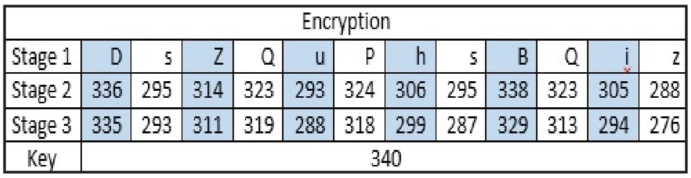


Plaintext	C	r	Y	P	t	O	g	r	A	P	h	y
Stage 1 Encryption	D	s	Z	Q	u	P	h	s	B	Q	i	z
Face Value	4	45	26	17	47	16	34	45	2	17	35	52
Position Value	1	2	3	4	5	6	7	8	9	10	11	12
Sum of Face value	340											

Fig. 3: Plaintext Having Face Values, Position Values and Sum of the Face Values

Subtract each face value from the sum to get the stage 2 cipher text.

Again subtract the position values from the stage 2 cipher text to get the final stage 3 cipher text (Refer fig. 4).



Encryption												
Stage 1	D	s	Z	Q	u	P	h	s	B	Q	i	z
Stage 2	336	295	314	323	293	324	306	295	338	323	305	288
Stage 3	335	293	311	319	288	318	299	287	329	313	294	276
Key	340											

Fig. 4: Results of Different Stages of Encryption

The cipher text obtained from stage 3 encryption is sent to the receiver along with the sum as the key.

B. Decryption –

Take up the cipher text and the key from the sender.

Add the position values of each corresponding letter to the cipher text as received from the sender to get stage 1 decryption.

The above obtained stage 1 decrypted text is subtracted from the key as received from the sender to get the face values which forms the stage 2 decrypted text.

Transform the obtained face values to its corresponding letters (Refer fig. 2)

Now, apply the basic Caesar cipher algorithm with substitution as -1 (Refer fig. 5). Thus the plain text is obtained (Refer fig. 6).

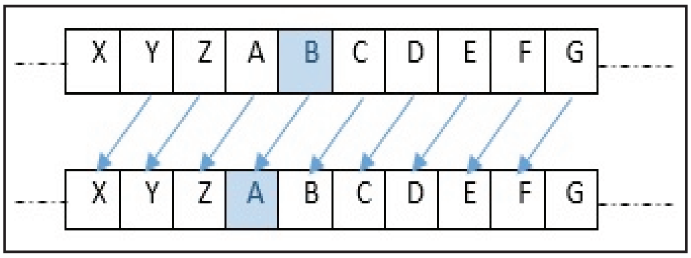
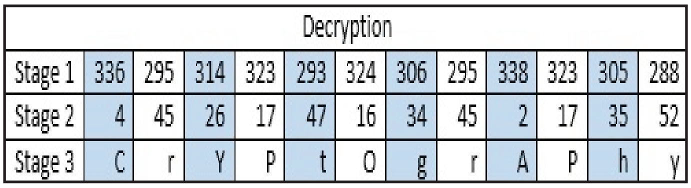


Fig. 5: Basic Caesar Cipher With Shift -1



Decryption												
Stage 1	336	295	314	323	293	324	306	295	338	323	305	288
Stage 2	4	45	26	17	47	16	34	45	2	17	35	52
Stage 3	C	r	Y	P	t	O	g	r	A	P	h	y

Fig. 6: Results of Different Stages of Decryption

V. Results and discussion

Caesar cipher is prone to brute force attack, frequency analysis and pattern matching. In order to overcome these problems occurring in the cipher text some modifications is been added with multi stage encryption technique.

The frequency analysis and pattern matching is done by observing the frequency of each occurrence of the letters in the cipher text. If the repetitions of the characters happen, it will be easy for the intruder to guess the plain text and crack it.

In this system as the plain text is been converted into numbers, and then upon carrying out some computations on the obtained numbers, the chances of getting the same number for the corresponding letter is very rare. In addition to this the system is case sensitive and so a wide range of plain text combinations can be covered. All these features provide security to the data transmitted using the insecure channel connecting the sender and receiver.

VI. Conclusion and Future Enhancement

The proposed system provides more security and it is capable of protecting the data from brute force attack by using additional stages of encryption. The cipher text generated after the different stages of encryption is in the form of numbers along with a key which is also a number. The chances of guessing the plaintext from those numbers is difficult and so frequency analysis and pattern matching is not possible to an extent.

We can also make the displacement dynamic instead of fixing it as ±1. Allowing the spaces between the words can also be added as a future enhancement. Using the various data structures in C, like linked list, stack, queue, tree graph etc, the modified Caesar cipher algorithm can be combined with any one the above mentioned data structures so that the cipher code is harder to crack. In this way an extra measure can be taken to send the private message safely from the sender to the receiver.

VII. Acknowledgement

The authors are pleased to thank Mrs. G Anuradha on her valuable comments, which improved the research clarity and conciseness. We also thank our friends for their support throughout our research.

References

[1] Sonali Kulkarni,"Cryptographic algorithm using data structure using c concepts for better security", International Conference on Pervasive Computing (ICPC), 2015.

[2] Willian Stallings,"Cryptography and Network", Prentice Hall of India.

[3] B.A.Forouzan,"Cryptography & Network Security", Tata-McGraw Hill Book Company

[4] S G Srikantaswamy, Dr. H D Phaneendra,"Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption", International Journal on Cryptography and Information Security (IJCIS). Vol. 2, No. 4. pp. 39-49, December 2012.

[5] Akanksha Mathur,"A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", International Journal on Computer Science and Engineering (IJCSE). Vol. 4, No. 09. pp. 1650-1657, September 2012.

[6] Vinod Saroha, Suman Mor, Anurag Dagar,"Enhancing Security of Caesar Cipher by Double Columnar Transposition Method", International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 2, Issue 10. pp. 86-88, October 2012.

[7] Gaurav Sharma, Ajay Kakkar,"Cryptography Algorithms and approaches used for data security", International Journal of Scientific & Engineering Research, Vol. 3, Issue 6, 2012.

[8] [Online] Available: http://www.cs.trincoll.edu/~crypto/historical/caesar.html. Last visited on 15-09-2015

[9] Ayushi,"A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (0975 - 8887), Vol. 1, No. 15, 2010.

[10] Shyam Nandan Kumar,"Review on Network Security and Cryptography", International Transaction of Electrical and Computer Engineers System, Vol. 3, No. 1, pp. 1-11, 2015.

Greetta Pinheiro received her B.Tech degree in Computer Science and Engineering from CUSAT University, Cochin. She has working experience in IT industry for 2 years. Currently she is pursuing her M. Tech in Computer Science from VIT University, Vellore. Her areas of interests include Cryptography, Cyber Security, Operating Systems and Computer Networks.

Shruti Saraf received her B.Tech degree in Computer Science and Engineering from Mody Institute of Technology, Lakshmangarh, Rajasthan, in 2012. In order to gain the corporate work experience, she joined one of the leading Multi National Company, Infosys Technologies in the year 2012 as a Systems Engineer for the consecutive two years. To increase her knowledge as software personnel, she is currently pursuing her Masters in Computer Science from Vellore Institute of Technology, Vellore, and would be receiving her M.Tech degree in the year 2017. Her research interest includes parallel and multicore programming, security by use of cryptography and various optimization techniques that can be employed for computation. At present, she is engaged in providing security in cloud applications.