IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Enhancing Security of Caesar Cipher Using Divide and Conquer Approach

Pooja Singh[1], Pintu sen[2]

[1]*Computer Science, Columbia institute of Engineering & Technology, Raipur*

[2]*Computer Science, Columbia institute of Engineering & Technology ,Raipur*

ABSTRACT

Cryptography is an art and science of converting original message into non readable form. There are two techniques for converting data into no readable form: 1)Transposition technique 2)Substitution technique. Caesar cipher is an example of substitution method. As Caesar cipher has various limitations so this talk will present a perspective on combination of techniques substitution and transposition. In this paper I have focused on the well known classical techniques the aim was to induce some strength to these classical encryption for that purpose I blended classical encryption with the some more techniques. my proposed method showed that it is better in terms of providing more security to any given text message. In our experiments I took Caesar Ciphers as representatives of Classical Techniques. To make it more secure I have used some techniques like I have used divide and conquer approach after applying normal caesar cipher technique up to 4 rounds.

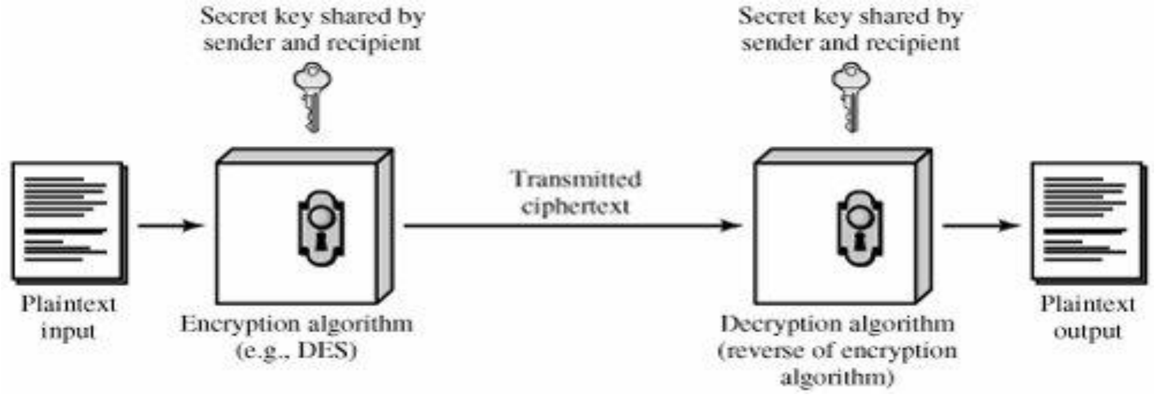
Keywords— substitution, transposition, cryptography, Caesar cipher, divide and conquer approach.

I. INTRODUCTION

In today's information age, it is impossible to imagine without internet. This modern era is dominated by paperless offices mail messages-cash transactions and virtual departmental stores. Due to this there is a great need of interchanging of data through internet. Various sensitive information like banking transactions, credit information, confidential data is transferred over internet. To protect this type of data there is a great need of security. We convert our data in a no readable form at sender side and convert that data in readable form again at receiver end. The art and science of creating no readable data or cipher so that only intended person is only able to read the data is called Cryptography [2]. Encryption is a process by which we convert our data in no readable form. Decryption is reverse of encryption process [3].Plaintext is the intended original message. Cipher text is the coded message. There are two techniques of encryption: Substitution Technique and Transposition Technique [4]. In substitution technique, the letters of plain text are replaced by other letters or any number or by symbols. Example Caesar cipher, hill cipher, monoalphabetic cipher etc[4].

In transposition technique, some sort of permutation is performed on plaintext.Example:rail fence method, columnar method etc[4].

Cryptology is not a new; it has existed for more than 2000 years5. Cryptography is an area within the field of cryptology. The name cryptology is a combination of the Greek cryptos (=hidden) and logos (=study, science). Therefore, the word cryptology literally implies the science of concealing6. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit7. An original message is known as the plaintext while the coded message is called the ciphertext. The process of converting from plaintext to ciphertext is known as enciphering or encryption; restoring the plaintext from the ciphertext is deciphering or decryption by using algorithm3.


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

II. BACKGROUND

In the field of cryptography there exist several techniques for encryption/decryption these techniques can be generally classified in to two major groups Conventional and Public key Cryptography, Conventional encryption is marked by its usage of single key for both the process of encryption and decryption whereas in public key cryptography separate keys are used. Further on conventional techniques are further broken in to Classical and Modern techniques. Ciphers are inter related a comprehensive hierarchal diagram can be seen below. Public key cryptography is also an option when it comes to encryption but it require excessive communication and processing resources [10]. In next sections we will discuss some of the conventional methodologies after which we will come to our proposed technique and finally we will compare our proposal with some standard conventional encryption models and display the results.

III. CLASSICAL ENCRYPTION

Several encryption algorithms are available and used in information security [6, 7, 8] There are several algorithms that can be categorized as classical but out of many in this section we will be shedding some light on 3 such techniques:

i) Caesar Cipher:
ii) Vigenere Cipher
iii) Playfair Cipher

Caesar Cipher:

It is a classical substitution cipher, and one of the simplest example of substitution cipher [9], which replaces the letter of alphabet with a letter that is 3 paces ahead of it [1], for example “ZULU” will be converted in to “CXOX” as one can see that such a IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010 281 cipher may be difficult to break if you are trying to solve it on paper and have no clue of the key, but it has no standing these days in the age of computers and technology and through brute force attack it can be easily broken because in the end there are only 25 possible options of key available.

Vigenere Cipher:

This cipher when compared with Caesar gives some level of security with the introduction of a keyword; this key word is repeated to cover the length of the plain text that is to be encrypted example is Shown below:

KEY: f a u z a n f a u z a n

P.T: c r y p t o g r a p h y

Cipher: H R S O T B L R U O H L

As we can see from above example that "fauzan" is our keyword and plain text is "cryptography" which was encrypted in to "HRSOTBLRUOHL" this was done using Vigenere table which contains alphabets in form of rows and columns left most column indicates keywords and top most row indicates plaintext and at the junction of two alphabetic letters resides our replacement and after individually transforming every letter we get an encrypted message.

Playfair Cipher:

Another example of classical cipher is Playfair cipher that has a square of matrix of 5X5 alphabetic letters arranged in an appropriate manner [2]. We can select a key and place it in the matrix the remaining letters of English alphabet are then one by one placed in the matrix of Playfair cipher, the plain text is broken in to pairs and if a pair has same alphabet then they are separated by introducing a filler letter like 'x', other wise if the pair are different alphabetic letters and reside in the same row of matrix then each letter is replaced by the letter ahead of it. If the pair of letters are in same column of matrix then each letter is replaced by the letter below it, and when the pair of letters are neither in same column nor in same row then are they replaced by the letter in their row that resides at the intersection of paired letters. Reverse method is applied to yield the result.

IV. PURPOSE

The purpose of this document is to present different methods that enhances the security of substitution cipher. In this paper I have focused on the well known classical techniques the aim was to induce some strength to these classical encryption for that purpose I blended classical encryption with the some more techniques. my proposed method showed that it is better in terms of providing more security to any given text message. In our experiments I took Caesar Ciphers as representatives of Classical Techniques. To make it more secure I have used some techniques like I have used divide and conquer approach.

V. SIMPLE CAESAR CIPHER TECHNIQUE:

The earliest known use of a substitution cipher, and the simplest was by Julius Caesar. The Caesar involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Plaintext: meet me after the toga party.

Ciphertext: PHHW PH DIWHU WKH WRJD SDUWB.

Note that the alphabet is wrapped around, so that the letter following Z is A. we can define the transformation by listing all possibilities as follow:

Plaintext: a b c d e f g h I j k l m n o p q r s t u v w x z.

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

Let us assign a numerical equivalent to each other.

Plaintext: a b c d e f g h I j k l m n o p q r s t u v w x y z.

Ciphertext: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25.

VI.PROBLEM OBSERVED IN THIS TECHNIQUE

Aftet study about this simple technique we observed that, sending message which has been encrypted by this technique can be easily hacked if the hacker wanted to hack it because in this method we only skip to the letters of first three digits and add them in last but if we add some extra in this it will be proved best technique for encrypting to the message.

VII. SOLUTION

We saw in Caesar cipher technique we simply eliminate to the first three digits of alphabet of the abcd…. And add them in last. But it is easily accessable so for securing them after doing previous process we apply divide and conquer approach in it.

Encryption Algorithm:

Step 1: Apply the previous Caesar cipher technique.

Step 2: Now reverse it from the last.

Step 3: Now combine this reverse letters in group of two-two letter and shuffle it.

Step 4 : Now combine this shuffle letters in group of three-three letters and shuffle it again.

Step 5: After completing from step 4 compare this shuffled letters with the original letters i.e, abcd.. and send it safely.

(Note: After completing step 4 do not shuffle more otherwise it will give the wrong result.)

Example Demo:

Input: a b c d e f g h I j k l m n o p q r s t u v w x y z.

Step1: d e f g h I j k l m n o p q r s t u v w x y z a b c.

Step2: c b a z y x w v u t s r q p o n m l k j I h g f e d.

Step3: cb az yx wv ut sr qp on ml kj ih gf ed.
Bc za xy vw tu rs pq no lm jk hi fg de

Step4: bcz axy vwt urs pqn olm jkh ifg de.
Zcb yxa twv sru nqp mlo hkj gfi de.

Comparison: zcb yxa twv sru nqp mlo hkj gfi de.
Abc def ghi jkl mno pqr stu vwx yz.

Example1:

Plaintext: I love my country.

Ciphertext: v upgx nd bpjqkod.

Decryption algorithm:

To encrypt a text proposed algorithm requires Text and encryption key. The encryption key is an integer value and it determines alphabet to be used for substitution. It is based on modulo twenty six arithmetic to ensure that integer value wraps round in case encryption key supplied is more than twenty six. Decryption follows reverse operations per Formed during the process of encryption. It requires decryption key, and encrypted text. The decryption key should be complement to the encryption key so that reverse character substitution can be achieved

Difference between simple Caesar cipher and including divide and conquer approach Caesar cipher substitution technique:-

Simple Caesar cipher	**Caesar cipher including divide and conquer approacl**
It is simple compare than the Caesar cipher includi divide and conquer approach.	It is little complex compare than the simple Caes cipher technique.
It is less secure compare than the Caesar ciph including divide and conquer approach.	It is more secure compare than the simple Caes cipher technique.
It is easy to hack.	It is not easy to hack.

VIII. IMPORTANCE:

Security is one of the important aspects in computing. In data transfer,security must be considered as one of the method implemented to ensure secure data transfer. Data transfer is transferring information from a location or host to another host, or server. To have a secure data transfer, this can be applied, and one of them is encryption of data, prepare it to be transferred in encrypted way and decrypted when the data want to be used.

As the importance and the value of exchanged data over the Internet or other media types are increasing, the search for the best solution to offer the necessary protection against the data thieves' attacks along with providing these services under timely manner is one of the most active subjects in the security related communities

IX. CONCLUSION:

This paper can be concluded that the ciphertext produced by this method can be read properly, thus of certain parties would not be suspicious of messages that have been encrypted. Besides the resulting ciphertext can be read, also imply. But not all the results of the rotation (root) imply. For the user, this method can choose the ciphertext that can be read and simply as needed. This method has the key (key) which lies on the line turnaround results (root) that can be used by the user as needed. Because the results of this modification are a single substitution, then the method is also easily solved by cryptanalyst along the ciphertext results not suspicious by cryptanalyst or of certain parties.

X. FUTURE WORK

In this paper we have shown that Caesar cipher being one of the simplest and widely used encryption techniques can be fortified beyond what common Caesar cipher algorithm can achieve. Many methods are used for Security purpose based on Caesar cipher algorithms. In our future work we can use various types of keys in one method also we can add more algorithms to enhance the security.

XI. REFERENCES:

[1]. Somdip Dey,Joyshree Nath and Ashoke Nath, "An Advanced Combined Symmetric Key Cryptographic Method using Bit Manipulation, Bit Reversal, Modified Caesar Cipher (SD-REE), DJSA method, TTJSA method: SJA-I Algorithm", International Journal of Computer Applications (IJCA). Vol. 46, No. 20. Pp. 46-53, May, 2012.

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

[3]. Hamdan.O.Alanazi, B.B.Zaidan and A.A.Zaidan, "New Comparative Study Between DES, 3DES and AES within Nine Factors", JOURNAL OF COMPUTING. Vol.2 , Issue 3. Pp.152-157, MARCH, 2010.

[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]. "CRYPTOGRAPHY", https://en//.wikipedia.org/wiki/cryptography.

[6]. Ochoche Abraham, Ganiyu O. Shefiu, "AN IMPROVED CAESAR CIPHER (ICC) ALGORITHM", International Journal Of Engineering Science & Advanced Technology (IJESAT). Vol. 2, Issue -5. pp .1198 – 1202, October 2012.

[7]. Jason Crampton, "Time-Storage Trade-Offs for Cryptographically-Enforced Access Control", Lecture Notes in Computer Science, Springer, 2011, Vol. 6879/2011, pp. 245-261.

[8]. Jiannong Cao, Lin Liao, Guojun Wang, "Scalable key management for Secure Multicast Communication in the Mobile Environment" Pervasive and Mobile Computing Vol. 2, pp.187–203, 2006.

[9]. Jawahar Thakur, Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering,Vol. 1, Issue 2, pp. 6-12, 2011.

[10]. "ENCRYPTION",http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryption_perf/index.htm.

[11]. VinodSaroha, SumanMor and AnuragDagar, "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.

[12]. Stalling, William.”Cryptography and Network Security: Principles and Practice”. 5th ed, Prentice Hall, 2006.

[13]. “Classical-Encryption Techniques”, mrajacse.files.wordpress.com/chapter-2.

[14]. Sinkov A., “Elementary “Cryptanalysis-A mathematical Approach”, Mathematical Association of America, 1966.

[15]. Somdip Dey ,”SD-AREE: A New Modified Caesar Cipher Cryptographic Method Alongwith Bit-Manipulation to Exclude Repetition from a Message to be Encrypted”, Department of Computer Science, St. Xavier’s College, Kolkata, West Bengal, India.

[16]. “Caesar.doc”,www.ti89.com/cryptotut/text/.