Integration of Caesar Cipher with Redefence cipher For Enhancing Data Security

RandhirKumar[1]
[1]Saveetha university ,Chennai

Abstract— In present period, there is momentous progress in earth of internet. Much Sensitive data can be shared through internet but this information sharing is susceptible to precise attacks. Cryptography was gave to solve these kinds of protection issues. It is an art for accomplished protection by encoding the plain text memo to cipher text. Substitution cipher and transposition cipher are the acquainted methods utilized for encoding. After Caesar cipher substitution and Redefence cipher transposition techniques are utilized individually, it is easy to crack the information. This paper suggests a hybrid method by combining substitution and transposition techniques. Combining Caesar cipher alongside Redefence cipher method can remove their fundamental flaw and produce a cipher text that is hard to crack.

Key words: Cryptograph, Cipher text, Substitution, Transposition, Caesar Cipher, Redefence.

.

I. INTRODUCTION

In our date to date existence internet plays a vital act in every single and every single person's life. In this present globe it is manipulated by paperless workplaces, E-mail messages, transactions online and virtual departmental stores for this.

Intention there is a outstanding demand of interchanging of data through internet. To protect the information considering this kind of data there is a outstanding demand of security. Since, they are extra sensitive data [1]; it needs extra protection as allocating that information in internet. But yet we are left with a tough job of protecting network from collection of attacks. We change our data in a non-readable form at sender side and change that data in readable form again at receiver end. The fine art and science of crafting non readable data or cipher so that merely aimed person is merely able to read the data is shouted cryptography [2]. Encryption is the process converting plaintext into cipher text. Decryption is reverse encryption process. Plaintext is denoted as early message and cipher text denoted as encrypted message.

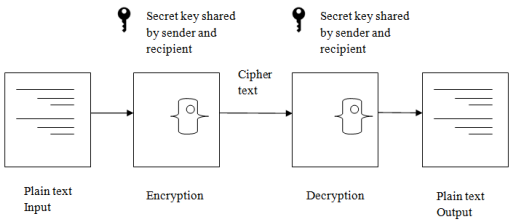

Fig.1: Process of encryption and Decryption

The rest of the paper is set out as follows. In serving 2, the comparative literature are studied, serving 3 think features about Caesar cipher and Redefence cipher, section 4 describes concerning counselled work, section 5 illuminate the example, serving 6 presents gains and in the end concluded up with the conclusion, the findings of the study.

II. . LITERATURE REVIEW

In the discover of the cryptography, the custom of substitution method is the simplest and extensively used. After one of the transposition methods is joined with substitution method, the allocating of information will come to be extra safeguard and reliable. Caesar cipher in substitution technique is joined alongside Rail Fence in transposition method [3]. But this is, difficult to apply as an easy Caesar cipher [3]. Protection of Caesar Cipher is enhanced alongside the Double Columnar Transposition method. It is convoluted to perform Double columnar transposition method alongside Caesar cipher.

A. Overview of Cryptography:

Many methods are utilized in protecting the secrecy of sensible information by changing them into unreadable (cipher text) form. Merely the use of a hidden key can change the cipher text back into human readable plain text. There are two main kinds of cryptography: Hidden key cryptography Area key cryptography The word key mentions to a numerical value utilized in an algorithm to alter information, making that information secure and visible merely to individuals. Secret key cryptography is additionally shouted as symmetric key cryptography. In this type, both the sender and the receiver understand the same hidden key. Area key cryptography, also shouted asymmetric encryption, uses a pair of keys for encryption and decryption. Encryption is the procedure of translating plain text into something that appears to meaningless cipher text Decryption is the procedure of converting cipher text back to plaintext. A cipher is an algorithm for performing encryption and decryption, a series of well described steps that can be followed as a procedure A substitution cipher is a method of encryption by that constituents of plaintext are substituted alongside cipher text according to a regular system; the "units" could be single letters (the most common), pairs of letters, triplets of messages, mixtures of the above, and so forth. The receiver deciphers the text by giving an inverse substitution. There are a number of different types of substitution cipher. If the cipher operates on solitary messages, it is termed a simple substitution cipher. One of the simple substitution ciphers is the Caesar cipher. A transposition cipher is a method of encryption by that the locations held by constituents of plain text that are commonly characters or clusters of acts are shifted according to a usual system.

III. CAESAR CIPHER AND REDEFENCE CIPHER

A. Caesar cipher:

When Julius Caesar dispatched messages to his generals, he didn't belief his messengers. So he substituted every single

A in his messages alongside a D, every single B alongside an E, and so on across the alphabet. Merely someone who understood the "shift by 3" law could decipher his memos [4]. But in general, this shift could be of each location [5]

C = E (k, p) = (p + k) mod 26 (1)

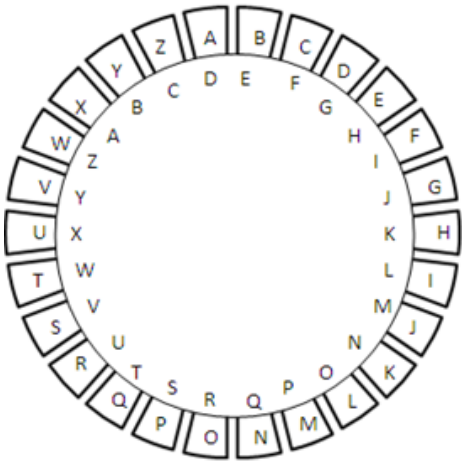

Fig. 2: Caesar cipher

If in case it is recognized that a given cipher text is Caesar cipher, next brute force cryptanalysis is facilely performed: Try all the 25 keys. There are a little weak points concerning Caesar cipher that enables us to use brute power attack [5]. Example: "LIFE IS BEAUTIFUL" is encoded to "OLIH LV EHDXWLIXO".

B. Redefence cipher:

Redefence is advance of Rail fence cipher, whereas in Rail fence method the plain text memo is coordinated in diagonal and reading it a sequence of line to produce cipher text. But in Redefence the plaintext could onset at each point in the cycle, is composed in zigzag, and is seized off by lines according to a key. The Key types are indicated in the solutions. The rail fence cipher could be made extra secure when a numerical key is utilized in addition to the early transposition [6].

Example:

Plain text: Trust You Can

2 beon3eivyua1lec

Cipher text: let been eivyua C. Analyzing Caesar Cipher and Redefence Cipher Cryptanalysis is destroying the codes and cipher. The algorithm use to decrypt Caesar cipher is simple. P=D(C) = (C – k) mod 26 (2) Brute-force cryptanalysis can be performed facilely, if recognized that given cipher text is a Caesar cipher. Just trying all probable 25 keys, a cryptanalysts can find the shift and decrypt the text using that shift. This method can be utilized to easily break Caesar ciphers by examination and error method. Likewise, Rail fence cipher is too a weak cipher to cryptanalyst. The code breaker can find correct one by trying depths. As it is frail, the Redefence cipher was introduced. It is hard to crack because messages break into rows according to precise hobble patterns based on the number of lines in the key. After the scrutiny of Caesar cipher and Redefence methods, allow us conclude that combination of both of these techniques can furnish far lot better security than the protection they provide alone.

IV. PROPOSED WORK

In the counselled work Caesar cipher and Redefence methods are combined alongside stack method for the secured communication.

A. Encryption Algorithm:

Step 1:• Input the Plain text and remove the spaces amid words.
Step 2:• Encrypt employing Caesar cipher.
Step 3:• Encrypt across Redefecne.
Step 4:• Locale the output in disparate stacks using PUSH and POP the values from every single stack.
Step 5:• Arose alongside Safeguarded Cipher text.

B. Decryption Algorithm:

Step 1:• Insert cipher text acts into stack, word by word.
Step 2: • POP early character from each stack and locale them one after another.
Step 3: • Tolerate till stacks become empty.
Step 4: • Reverse of Caesar cipher.
Step 5: • Finally, arose alongside plain text.

V. V. EXAMPLE

A. Encryption:

Step 1: Presume early memo is
"BELIEVE YOURSELF".
After removing the space between words, the plain text will be "BELIEVEYOURSELF"
Step 1: Suppose early memo is "BELIEVE YOUSELF". After removing the space between words, the plain text will be "BE LIEVE YOURSELF"
Step 2: Requesting Caesar cipher with key 6 in, C=E (6, P) = (P+6) mod 26 The encrypted memo will be "HKROKBKEUAXYKRL".
Step 3: employing Redefence encrypt the above encrypted message Cipher text afterward Redefence: HRKKUXKL KOBEAYR

L
K
X
U
K
K
R
H

(Word 1)

R
Y
A
E
B
O
K

(Word 2)

Fig. 3: Encryption

Step 4: Filling above two cipher text words in disparate stacks by using PUSH method.
Step 5: Finally, the cipher text applying stack on redefence method. Later POP out the values from every single stack the result will be: LKXUKKRH RYAEBOK

B. Decryption:

Step 1: Insert cipher text acts in to stacks word by word.

Step 2: POP the early character from stacks and locale them one after another. Later the early POP operation output will be HK. Again the alike procedure is performed we become HKRO

Step 3: Tolerate till stack become empty. Output afterward the stack gets empty: HKROKBKEUAXYKRL
Step 4: Last pace is reverse of Caesar cipher. Key utilized is 6. By using decryption formula P = D (k, C) = (C-6) mod 26
Step 5: Later decryption the plain text will be BELIEVEYOURSELF

VI. ADVANTAGES

This Caesar cipher that is safeguarded by "Redefence Technique" has various advantages above easy cipher.

- extra tough to crypt analyze the encrypted message.
- Final consequence cannot be easily reconstructed.
- Brute power attack is not possible here.
- It overcomes all the limitations of Caesar cipher.

VII. CONCLUSION

In order to attain the secure transformation of sensible data, the combination of Caesar cipher and Redefence method alongside the stack implementation is gave in the proposed work. Substitution methods only replace the message alongside each supplementary message and Transposition method merely changes position of characters. Caesar cipher is simplest kind of cipher and most widely used Substitution method. Where redefence is one of the methods in the Transposition method. Redefence provide more safeguard than the Rail fence and most effective than Double Columnar Transposition method. And Transposition method is generally joined alongside other techniques. The combination of two classical methods provides extra secure and oust cipher. The final cipher text is very intricate to break. The above depicted method is the combination of both the Transposition and Substitution method which provides for extra safeguard cipher for transformation.

REFERENCES

[1] Anupama Mishra, "Enhancing Security of Caesar Cipher Using Different "Methods",International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308, Volume: 02 Issue: 09 | Sep-2013
[2] Vinod Saroha, Suman Mor, and Anurag Dagar , " Enhancing Security of Caesar Cipher by Double Columnar Transposition Method", International Journal of Advanced Research in Computer Science and Software Engineering 1 (8), August- 2012, pp. 1-6.
[3] Ajit Singh, Aarti Nandal, Swati Malik, "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security", International Journal of Advanced Research in Computer science and Software Engineering 2 (12), December - 2012, pp. 78-82
[4] Atul Kahate (2009), "Cryptography and Network Security", 2nd edition, McGraw-Hill.
[5] Stallings W (1999), "Cryptography and Network Security", 2nd edition, Prentice Hall.
[6] William Stallings (2003), "Cryptography and Network Security", 3drd edition, Pearson Education.
[7] http://www.xarg.org/tools/caesarcipher/
[8] http://www.ti89.com/cryptotut/transposition.htm

