Volume 2, Issue 12, December 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security

Ajit Singh* CSE, SES, BPSMV India
Aarti Nandal CSE, SES, BPSMV India
Swati Malik CSE, SES, BPSMV India

Abstract*— In recent years there is drastic progress in Internet world. Sensitive information can be shared through internet but this information sharing is susceptible to certain attacks. Cryptography was introduced to solve this problem. Cryptography is art for achieving security by encoding the plain text message to cipher text. Substitution and transposition are techniques for encoding. When Caesar cipher substitution and Rail fence transposition techniques are used individually, cipher text obtained is easy to crack. This talk will present a perspective on combination of techniques substitution and transposition. Combining Caesar cipher with Rail fence technique can eliminate their fundamental weakness and produce a cipher text that is hard to crack.

***Keywords*— Cryptography, Cipher text, Substitution, Transposition, Caesar Cipher, Rain Fence.**

I. INTRODUCTION

The dramatic rise of internet has opened the possibilities that no one had imagined. We can connect to any person, any organization or any computer, no matters how far we are from them. Internet cannot be used only for browsing purpose. Sensitive information like banking transactions, credit card information and confidential data can be shared through internet. But still we are left with a difficult job of protecting network from variety of attacks. With the lots of efforts, network support staff came up with solution to our problem named "Cryptography". Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be read and understood without any difficulty is called plain text or clear text. The method of encoding Plain text in such a way as to hide its content is called encryption. Encrypting plain text results in unreadable gibberish called cipher text. You use Encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plain text is called decryption [1].

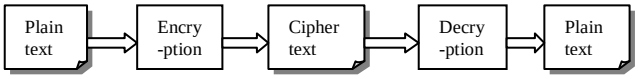


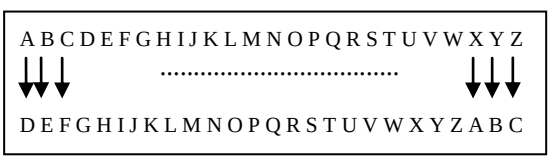
Fig.1 Encryption and Decryption

There are two primary ways in which plaintext can b codified to corresponding Cipher text: Substitution and Transposition. A Substitution technique is one in which the letters of Plain text are replaced by other letters or by numbers(Caesar Cipher , Hill Cipher, Monoalphabetic cipher etc).A Transposition technique is one in which the letters of the message are rearranged or permuted. (Rail Fence method, Columnar method etc.) [2].

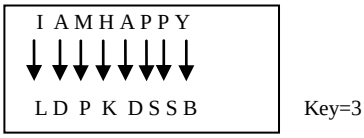
A. Caesar Cipher

When Julius Caesar sent messages to his generals, he didn't trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3" rule could decipher his messages [1].

$$C = E(k, p) = (p + k) \bmod 26 \quad (1)$$

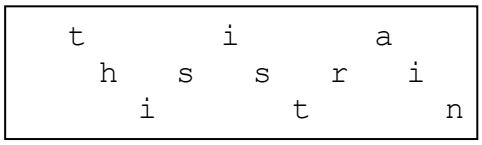


Example: "I AM HAPPY" is encoded to "L DP KDSSB".



B. Rail Fencing Technique

Rail fencing technique involves: Writing plain text message as a sequence of diagonal and reading it as a sequence of row to produce cipher text. For e.g. suppose we want to encrypt " This is train" so in a Rail Fence cipher, after removing the spaces from the original message, we would write the characters in the message in the following zig-zag pattern. The key for the Rail Fence cipher is just the number of rails [3]. To encrypt a piece of text, e.g.



Here the key or depth of the train is 3. To encrypt, we construct the cipher text by reading across the rows that result.
Cipher text: tia hssri itn
Cipher text: tia hssri itn.

C. Analysing Caesar Cipher and Rail Fence Technique

Cryptanalysis means breaking codes and ciphers. The decryption algorithm of Caesar cipher is simple.

$$P= D(C) = (C - k) \bmod 26 \quad (2)$$

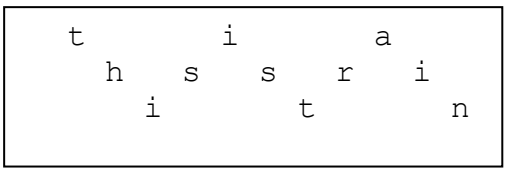
If it is known that given cipher text is a Caesar cipher, then a brute-force cryptanalysis can be easily performed. Simply by trying all possible 25 keys a cryptanalyst just has to find the shift that causes the cipher text frequencies to match up closely with the natural English frequencies and then decrypt the text using that shift. This method can be used to easily break Caesar ciphers by hand [2].

Similarly Rail Fence cipher is also a very weak cipher to Cryptanalyze. A code breaker simply has to try several depths until the correct one is found. It is very easy to find depth if you know some of the plain text. Letters break into rows according to certain fixed patterns based on the number of rows in the key [2]. For example, if there are two rows, then letters 1, 3, 5, … of the message are in row one and letters 2, 4, 6, ... are in row two [4].

1 3 5 7 9
2 4 6 8

Decrypting the message is easy if the row boundaries are known. Just write down the rows in order. From above example of rail fencing we can write cipher text as:
Tia
hssri
itn

After constructing the "rails" of the fence we get:



If no row boundaries are present, it is not difficult to reconstruct the fence [4].

After analysing both of these techniques we came to the conclusion that neither of the technique is much secure. But a combination of both of these techniques can provide much better security than the security they provide alone [5], [6].

II. PROPOSED WORK

In proposed work we will combine Caesar Cipher and Rail Fence techniques with stack method for making the communication more secure.

A. Encryption Algorithm

Step1: Take the plain text as input and remove the spaces between words.

Step2: Encrypt by using Caesar cipher i.e. shifting the alphabets of Plain text by k alphabets by using (1).

Step3: Write down the above encrypted message as sequence of diagonals and then read off as sequence of rows. (Rail fencing Technique).

Step4: After this, for adding complexity put these two different words in different stacks by using PUSH

methods. Fill Entries of stacks for both rows. Now, POP the values from each stack.

Step5: Finally the cipher text after applying Stack on Rail fence method is obtained.

After implementing the above specified encryption technique, cipher text is sent to the intended recipient.

B. Decryption Algorithm

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

Step 2: POP first character from word 1 and first character from word 2 position them one after another i.e. at first position, character from first word and character from second word at second position.

Step 3: Continue in the same manner until stacks become empty.

Step 4: This step is reverse of Caesar cipher. Plain text is obtained by using (2).

III. EXAMPLE

A. Encryption

Step 1: Suppose original message is SWEET HOMES. After removing the spaces between words plain text will be: SWEETHOMES

Step 2: If the key used is 4 then by applying Caesar cipher the encrypted message will be WAIIX LSQIW i.e.

$$C = E(4, p) = (p + 4) \bmod 26 = \text{WAIIX LSQIW}$$

Step 3: Writing down output of Step 2 it as a sequence of diagonals and then read off as sequence of rows. (Rail fencing technique)

W I X S I
A I L Q W

Cipher Text after Rail Fencing:

W IXSI AILQW
(Word 1) (Word 2)

Step 4: After this, putting these two different words in different stacks by using PUSH method. Fill Entries of stacks for both rows.

Word 1	Word 2
I	W
S	Q
X	L
I	I
W	A

Fig.2 Stacks after PUSH operation

After POP method the values from each stack result will be: ISXIW WQLIA.

Finally the cipher text after applying Stack on Rail fence method: ISXIW WQLIA

B. Decryption

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

W
I
X
S

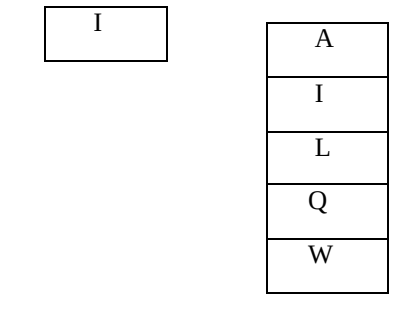


Fig.3 Stacks after pushing the cipher text

Step 2: POP first character from word 1 and first character from word 2 position them one after another.
After first pop operation output will be WA. Then performing the same operation again we get WAII.

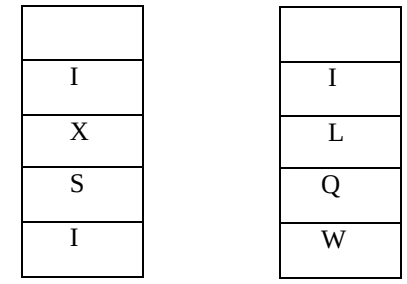


Fig.4 Stacks after first POP

Output after first POP: WA

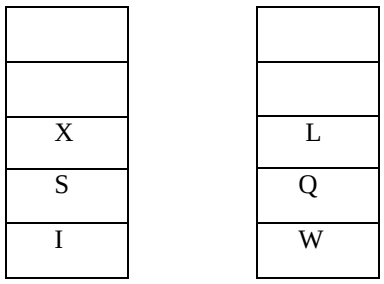


Fig.5 Stacks after second POP

Output after second POP: WAII

Step 3: Continue in the same manner until stacks become empty.
Output after stacks become empty: WAIIXLSQIW
Step 4: Last step is reverse of Caesar cipher. Key used is 4. By using decryption formula

$$P = D(k, C) = (C - 4) \bmod 26$$

The plain text is generated after performing the decryption in this manner.
Plain text: SWEETHOMES

IV. APPLICATION

This Caesar cipher which is secured by "Rail Fencing Technique" has various advantages over simple Caesar cipher.

- It is more difficult to cryptanalyze.
- The result cannot be easily reconstructed.
- Brute force attack cannot crack the cipher code.
- Overcome all the limitations of Caesar cipher.

.

V. DISADVANTAGE

- Difficult to implement as simple Caesar cipher.

VI. CONCLUSION

Caesar cipher is the simplest substitution method. It is also the weakest cipher. It's only advantage lies in the fact that it is not complex and can be understood easily. This advantage leads to the problem of easy detection. For overcoming this problem Caesar cipher is combined with transposition techniques. Transposition technique used here is rail fencing. For adding further complexity stacks are used which makes the detection of both the techniques (Caesar cipher and rail fencing) difficult. The above proposed method is a combination of transposition and substitution hence it will provide better security for text. However, the used algorithms can be improved to get better results.

ACKNOWLEDGMENT

We would like to give our sincere gratitude to our guide Ms. Ajit Singh who encouraged and guided us throughout this paper.

.

REFERENCES

[1] Atul Kahate (2009), *Cryptography and Network Security*, second edition, McGraw-Hill.
[2] William Stalling "*Network Security Essentials(Applications and Standards)*",Pearson Education,2004
[3] http://www.cs.trincoll.edu/~crypto/historical/railfence.html
[4] practicalcryptography.com/ciphers/rail-fence-cipher/
[5] Vinod Saroha1, Suman Mor2, and Anurag Dagar3," 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.
[6] Gurdev Singh, Jimmy Singla and Shivdev Singh, "Message Encryption and Decryption" VSRD-IJCSIT, Vol. 2 (7), 2012, 668- 671.

