International Journal of Allied Practice, Research and Review

Website: www.ijaprr.com (ISSN 2350-1294)

Enhancing Ceaser Cipher by Using Multiple Keys

Naillah Gul[1], Zulykha Ali Khan[2], Tamseel Majid Khan[3]
STUDENT, DEPARTMENT OF CSE,
SSM COLLEGE OF ENGINEERING. AND TECHNOLOGY,
PATTAN, BARAMULLA, JAMMU AND KASHMIR, INDIA

Abstract: In cryptography, a ceaser cipher also known as ceaser's cipher, the shift cipher, ceaser's code or ceaser shift is one of the simplest and most widely known encryption technique. It is a type of substitution cipher in which each letter in the plain-text is replaced by a letter some fixed number of positions down the alphabet [1]. In this paper, we present a way to enhance the security of ceaser cipher using multiple keys.

Keywords: ***Plain-text, cipher-text, redundancy, numbering, counters.***

I. INTRODUCTION

The modern world and the internet go hand in hand. The paperless approach cannot breathe without internet, be it e-mails, net banking, e-commerce or anything that uses internet for its working. With the excessive use of internet, there automatically arises the need of providing security to the data that is being exchanged. To do so, the sensitive data needs to be changed into a form that is not readable to the intruders. The art and science of creating non-readable data or cipher so that only intended person is able to read the data is known as cryptography [3]. In cryptography, encryption is the process of encoding a message or information in such a way that only authorized parties can access it [1]. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users. Decryption is the reverse of encryption [1].

Encryption can be done in two ways:

1. Substitution technique

2. Transposition technique [4].

In substitution technique, the letters of plain text are replaced by other letters or any number or by symbols. Example, ceaser-cipher, hill-cipher, mono-alphabetic cipher etc. [4].

In transposition technique, some sort of permutation is performed on plain text.eg rail fence method, columnar method etc. [4].

II. CAESAR CIPHER AND ITS CRYPTANALYSIS

Caesar cipher is one of the simplest types of substitution method. In this, letters of alphabets are replaced by letters three places further down the alphabet. But in general, this shift may be of any places. Using the Caesar cipher, the message “MISSIPPI ISLAND” is encrypted as “OKUVLRSK LUNCPF”. So, attacker is not able to read the message if he intercepts the message.

If, in case it is known that a given ciphertext is Caesar cipher, then brute force cryptanalysis is easily performed: Try all the 25 keys. There are some weak points about Caesar cipher which enables us to use brute force attack.

1. The encryption and decryption algorithm is known.

2. Only 25 keys are to try.

3. The language of the plaintext is known and easily recognizable [5].

III. CEASER CIPHER USING MULTIPLE KEYS [INTRODUCTION]

The idea behind ceaser cipher is to replace the letters of English alphabet by some other letter up down the sequence.

The thought behind “ceaser cipher using multiple keys” is to use two keys.

The question arises how we can use multiple keys in ceaser cipher

The answer to this question is based on the repetition of the same letters in the plain text.

In plain ceaser cipher we do not maintain the occurrence of the letters, but here we will be maintaining the occurrence of the letters by use of counters equal to the number of English alphabets i.e. 26.

We also have to look out for a way in order to communicate to the receiver about the repetition of some letter in the plain text. This can be done by numbering the letters in the plain text.
Two ways of doing this are:

1. NUMBERING ALL LETTERS:

Each letter which is encountered for the first time will be numbered as 0, and those letters which are encountered second time will be marked as 1. This process of marking the letters can be done to either cipher text only or to both plaintext and ciphertext.
Example:

M I S S I P P I I S L A N D
//Plain-text

$M_0\ I_0\ S_0\ S_1\ I_1\ P_0\ P_1\ I_0 \quad I_1\ S_0\ L_0\ A_0\ N_0\ D_0$
//Modified Plain-text

An issue arises i.e. what to number a letter if it occurs for third time.

When using two keys, counters can be reset to zero after they have been incremented to one. When first occurrence happens, counter value will be zero (0). For second occurrence counter value will be one (1). For third occurrence, counter will again be zero (0). That is the reason for the third occurrence of letter ‘I’ to have numbering as zero (0).

Key 1 = 2
Key 2 = 3
$M_0\ I_0\ S_0\ S_1\ I_1\ P_0\ P_1\ I_0 \quad I_1\ S_0\ L_0\ A_0\ N_0\ D_0$
//Modified Plain-text

$O_0\ K_0\ U_0\ V_1\ L_1\ R_0\ S_1\ K_0 \quad L_1\ U_0\ N_0\ C_0\ P_0\ F_0$ //Upper text with same numbering as of plain-text

Disadvantages of numbering all letters:

It will consume more bandwidth.

2. NUMBEERING ONLY REPEATED LETTERS

M I S S I P I I S L A N D //Plain-text
M I S S_1 I_1 P P_1 I I_1 S L A N D
//Modified Plain-text

When number it encountered for first time, it is not numbered. When second time number is encountered, it is numbered by one (1). When third occurrence of a number arrives, counter resets to zero (0) and hence each letter is not numbered.

If we observe the plain-text (modified) only 4 letters have been marked. In case of previous one, all 14 letters have been numbered.
Advantages of numbering only repeated letters:

Only repeated letters will be marked, hence consuming lesser bandwidth.

IV. ENCRYPTION ALGORITHM

1) First, we take a message or plain text from users which have to encrypt. Example: MISSIPPI ISLAND

2) Decide the key1 (places) with the help of which characters are to be shifted. Example: Key1=2, Key2=3.

3) Numbering the plaintext as per the numbering scheme described already. Example:

M_0 I_0 S_0 S_1 I_1 P_0 P_1 I_0 I_1 S_0 L_0 A_0 N_0 D_0

4) Encrypting the plaintext (modified plaintext). Letters which are not numbered are to be replaced using using key1 and letters which are marked are to be replaced using key2.

M I S S_1 I_1 P P_1 I
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
O K U V_1 L_1 R S_1 K

I_1 S L A N D
↓ ↓ ↓ ↓ ↓ ↓
L_1 U N C P F

Thus, the ciphertext is

O K U V_1 L_1 R S_1 K L_1 U N C P F.

V. DECRYPTION ALGORITHM

The algorithm which runs in reverse order to get the original data is known as decryption.

1) It takes the cipher text, key1 and key2. Example:
O K U V_1 L_1 R S_1 K L_1 U N C P F
//Ciphertext

Key1=2.
Key2=3.

2) Decrypting the ciphertext. Letters where no number is marked are replaced by using key1 and marked letters are replaced by using key2.

O K U V_1 L_1 R S_1 K
↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
M I S S_1 I_1 P P_1 I

$$\begin{tikzcd}
L_1 \arrow[d] & U \arrow[d] & N \arrow[d] & C \arrow[d] & P \arrow[d] & F \arrow[d] \\
I_1 & S & L & A & N & D
\end{tikzcd}$$

2) Thus, the original message:
MISSIPPI ISLAND

VI. ADVANTAGE

1. Easy to use as compared to other techniques that make excessive use of permutations.

2. Frequency of repeated letters in the ciphertext has been masked and as such intruder will find it difficult to perform frequency analysis of the cipher text (to arrive at plaintext) to determine the key. When number of keys increase no two same letters in the ciphertext will correspond to the same letter in the plaintext.

VII. DISADVANTAGE

1. Require more bandwidth as compared to plaintext ciphertext.

2. As the no of keys increases, the requirement for bandwidth also increases.

3. It requires additional space on sending side to implement counters.

VIII. CONCLUSION

1. The above thought is written with respect to using two keys and using a single bit to mark (either zero (0) or one (1)) to mark the repetition of a letter.

2. If we use 2 bits to mark letters, then we can have 4 keys.

3. For n bit marking, we can have 2^n keys.

IX. ACKNOWLEDGEMENT

Authors would like to give sincere gratitude especially to Dr. Fahad Rasool Dar and Ms. Sahila Shah for their guidance and support to pursue this work.

X. REFERENCES

[1]Wikipedia https://en.wikipedia.org/wiki/Ceaser_cipher.

[2]Wikipedia https://en.wikipedia.org/wiki/Encryption.

[3] Atul Kahate (2009), *Cryptography and Network Security*, 2nd edition, McGraw-Hill.

[4] William Stallings (2003), *Cryptography and Network Security*, 3rd edition, Pearson Education.

[5] Research Paper, *Enhancing Security Of Ceaser Cipher By Double Columnar Transposition Method.*

XI. BIOGRAPHY

Dr.Fahad Rasool holds a post doctorate in computer science. Research Interest of Dr. Fahad Rasool Dar are Artificial intelligence, Data science, network security. Ms. Sahila Shah holds B.tech degree in computer science. Her areas of interest include: Robotics, data mining.