IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Using Letters Frequency Analysis in Caesar Cipher with Double Columnar Transposition Technique

Gaurav Shrivastava[*1], Ravindra Sharma[2], Manorama Chouhan[3]

[*1,2,3]Assistant Professor, Department of Information Technology , Shri Vaishnav Institute of Technology & Science,Indore, Madhya Pradesh, India

gaurav2086@gmail.com

Abstract

In this paper we have some modification in Caesar Cipher Technique. We have proposed a method to enhancing the Caesar cipher for more efficient and secure. We use Relative Frequency of Letters in Alphabets. We arrange the sequence of letter according to the frequency in increasing ordered. And then we have made use of a Modified Caesar cipher technique with double Columnar Transposition Technique.

Keywords: Caesar Cipher, Double Columnar Transposition Technique, Frequency of Letters.

Introduction

Cryptography is the science which deals with all the means and methods for converting an intelligible message into an unintelligible or secret form and for reconverting the secret form into the intelligible message by a direct reversal of the steps used in the original process [1]. Even though encryption is very powerful among these two, the cryptanalysts are very intelligent and they were working day and night to break the ciphers. To make a stronger cipher it is recommended that to use: 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. In transposition technique, some sort of permutation is performed on plaintext. Example: rail fence method, columnar method etc. [2]

Cryptography Science

The word is derived from the Greek crypto's, meaning hidden. Cryptography is a science of devising methods that allow information to be sent in a secure from in such a way that the only person to able retrieve this information is the intended recipient. Encryption is based on algorithms that scramble information (Plaintext or Clear Text) into unreadable (Cipher Text) form. Decryption is the process of restoring the scrambled information to its original form. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. Cryptographic systems are used to provide privacy and authentication in computer and communication systems. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. [1]

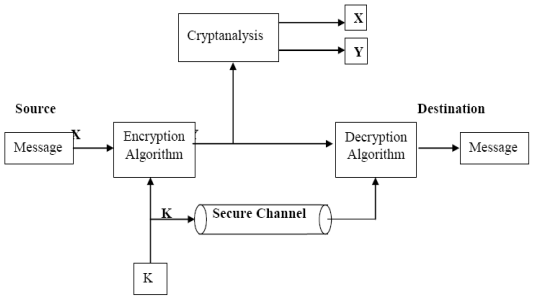


Fig: 1.1

All Cryptographic algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, and group of bits or letters) is mapped into another element and in transposition, the elements of the plaintext have simply been re-arranged in different order; their position with relation to each other have been changed.[1]

Classic Cryptography

The earliest forms of secret writing required little more than local pen and paper analogs, as most people could not read. More literacy, or literate opponents, required actual cryptography. The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message (e.g., 'hello world' becomes 'hello owrdl' in a trivially simple

rearrangement scheme), and substitution ciphers, which systematically replace letters or groups of letters with other letters or groups of letters (e.g., 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet).[6]

A. Substitution Technique

In cryptography, a substitution cipher is a method of encryption by which units of plaintext are replaced with cipher text according to a regular system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution.

There are a number of different types of substitution cipher available like Caesar Cipher, Mono-alphabetic Cipher, Homophonic Substitution Cipher, Polygram Substitution Cipher, Polyalphabetic Substitution Cipher, Playfair Cipher and Hill Cipher. [6]

B. Transposition Technique

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically a objective function is used on the characters' positions to encrypt and an inverse function to decrypt.

There are a number of different types of Transposition cipher available like Rail Fence Cipher, Simple Columnar Transposition, Vernam Cipher, Double transposition, Myszkowski Transposition, Disrupted Transposition. [6]

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 [4]. Using the Caesar cipher, the message “RETURN TO ROME” is encrypted as “UHWXUA WR URPH”. So attacker is not able to read the message if he intercepts the message.

If in case it is known that a given cipher text 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. [2]

Brief Description Of Our Proposal

In this algorithm which is used to encryption and decryption the data which provides more secure Caesar cipher than original Caesar cipher. We use Relative Frequency of Letters in Alphabets. We arrange the sequence of letter according to the frequency in increasing ordered.

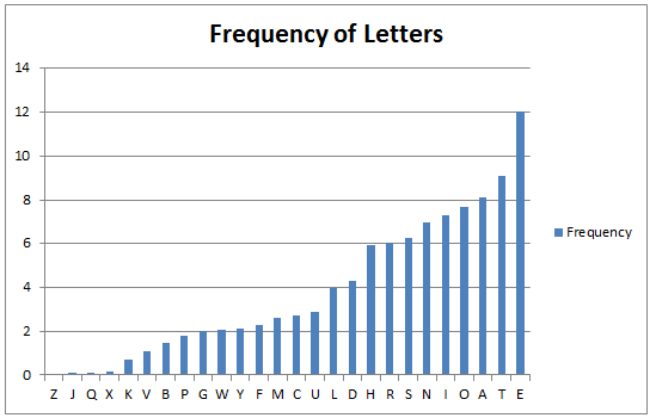


Fig: 1.1 [3]

Letter	Z	J	Q	X	K	V	B	P	G	W	Y	F	M	C	U	L	D	H	R	S	N	I	O	A	T	E
Frequency	0.07	0.1	0.11	0.17	0.69	1.11	1.49	1.82	2.03	2.09	2.11	2.3	2.61	2.71	2.88	3.98	4.32	5.92	6.02	6.28	6.95	7.31	7.68	8.12	9.1	12

Table: 1.1

According to frequency of letters our proposed Caesar Cipher

Z	J	Q	X	K	V	B	P	G	W	Y	F	M	C	U	L	D	H	R	S	N	I	O	A	T	E
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	26

Table: 1.2

After perform encryption of Caesar Cipher then we apply double Columnar Transposition Technique and then find the Cipher text. Encryption and Decryption process are detailed in below:

A. Encryption

1) First, we take a message or plain text from user which has to encrypt.
2) Decide the key (K1) (places) with the help of which characters are to be shifted.
3) After Encrypt by Key (K1) Produced Cipher Text as a Input to double Columnar Transposition Technique.
4) Now write this encrypted message or Cipher Text in rectangle way, row by row. The number of rows depends on amount of data.
5) The order of column becomes the key (K2) to this algorithm, which is decided by sender and also known to receiver.

6) Read off the message column by column and we can permute the order of column.
7) After Encrypted Messages by key (K2) is again apply double Columnar Transposition Technique with Key [K3] which is also decided by sender and also known to receiver.
8) It's written in rectangle form again, row by row as above told.
9) After placing data in rectangle form then it is read off column by column, we get our Output.
10) Finally we get the Final cipher text (encrypted message).

B. Decryption

1) The algorithm which runs in reverse order to get the original data is known as decryption.
2) It takes the cipher text, key (K1, K2 and K3).The number of rows is also known to receiver.
3) Arrange the cipher in rectangle form: column by column using Key (K3) and number of rows.
4) Read the message row by row.
5) Repeat the step 2 and 3 with key (K2) and produce Output.
6) Now Produced Output decrypt with key (K1).
7) Finally we get our original data (plain text).

Example

A. Encryption

1) Suppose the original message is "WE ARE DISCOVERED FLEE AT ONCE".
2) Suppose the K1 is 4.
3) Decrypt the data by 4 places:

Plain Text	K	V	B	P	G	W	Y	F	M	C	U	L	D	H	R	S	N	I	O	A	T	E	Z	J	Q	X
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Cipher Text	Z	J	Q	X	K	V	B	P	G	W	Y	F	M	C	U	L	D	H	R	S	N	I	O	A	T	E

Table: 1.3

Plain Text	W	E	A	R	E	D	I	S	C	O	V	E	R	E	D	F	L	E	E	A	T	O	N	C	E
Cipher Text	V	I	S	U	I	M	H	L	W	R	J	I	U	I	M	P	F	I	I	S	N	R	D	W	I

Table: 1.4

4) Cipher Text is
"VISUIMHLWRJIUIMPFIISNRDWI"
5) Then we apply double Columnar Transposition Technique.
6) Suppose the K2 is ZEBRAS

1	2	3	4	5	6

Table: 1.5 (Color Coding)

Z	E	B	R	A	S

7) These are number of column and also specify their order. It can be anything according to the sender.

1	6	2	3	5	4
V	I	S	U	I	M
H	L	W	R	J	I
U	I	M	P	F	I
I	S	N	R	D	W
I					

8) Read column by column according to the order

V	H	U	I	I	S	W	M	N	U	R	P	R	M	I	I	W	I	J	F	D	I	L	I	S

9) And then we apply double Columnar Transposition Technique.

10) Suppose the K2 is STRIPE

S	T	R	I	P	E

3	5	2	4	1	6
V	H	U	I	I	S
W	M	N	U	R	P
R	M	I	I	W	I
J	F	D	I	L	I
S					

10) Read column by column according to the order and

I	R	W	L	U	N	I	D	V	W	R	J	S	I	U	I	I	H	M	M	F	S	P	I	I

11) Finally we get our secure output "IRWLUNIDVWRJSIUIIHMMFSPII"

B. Decryption

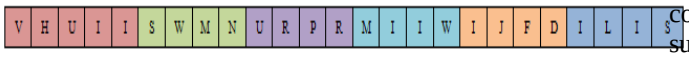
1) Arrange the cipher in rectangle form: column by column, receiver knows the key and number of rows.

I	R	W	L	U	N	I	D	V	W	R	J	S	I	U	I	I	H	M	M	F	S	P	I	I

Key (K3): STRIPE (352416)

3	5	2	4	1	6
V	H	U	I	I	S
W	M	N	U	R	P
R	M	I	I	W	I
J	F	D	I	L	I
S					

2) Read row by row:



3) Again arrange the output in rectangle form column by column:

Key (K2): ZEBRAS (162354)

1	6	2	3	5	4
V	I	S	U	I	M
H	L	W	R	J	I
U	I	M	P	F	I
I	S	N	R	D	W
I					

4) Read row wise,the data is
Plaintext: **"**VISUIMHLWRJIUIMPFIISNRDWI"
5) Using key (K1) with Table Number 1.4, which is 4,
decrypt the above cipher and we get

"WE ARE DISCOVERED FLEE AT ONCE".
6) This is original message which is sent by sender.

Advantage of Proposed Playfair Technique

- We can Encrypt & Decrypt any type of plain text (Alphabetical, Numerical & Special Symbols)
- Identification of individual diagrams is difficult.
- Frequency analysis difficult.
- In this double transposition method is applied which provide much less structured permutation.
- It is more difficult to cryptanalyze.
- The result is not easily reconstructed.
- Brute force attack is not possible.
- Overcome all the limitations of Caesar cipher. [2]

Conclusion

In this paper some modifications of Caesar cipher because it's very simple and easily cracked by Brute Force Attacks. We have to change sequence of letters according to the Frequency of letters. Its more difficult than previous Caesar cipher method. And then we apply double Columnar Transposition Technique to create more complexity. The combination of these two classic techniques provides more secure and strong cipher. The final cipher text is so strong that is very difficult to break. Substitution method only replaces the letter with any other letter and transposition method only change position of characters. The above described method is the combination of both the transposition and substitution method which provides much more secure cipher.

References

[1] Gaurav Shrivastava, Manoj Dhawan & Manoj Chouhanan, Enhance Security Of Playfair Cipher Substitution Using A Simple Columnar Transposition Technique With Multiple Rounds (SCTTMR, International Journal Of Research In Commerce, It & Management) Volume No. 2 (2012), Issue No. 8 (August) ISSN 2231-5756
[2] Mr. Vinod Saroha, Suman Mor, Anurag Dagar, Enhancing Security Of Caesar Cipher By Double Columnar Transposition, International Journal Of Advanced Research In Computer Science And Software Engineering Method Volume 2, Issue 10, October 2012 ISSN: 2277 128X
[3] http://www.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html
[4] http://en.wikipedia.org/wiki/Transposition_cipher
[5] http://en.wikipedia.org/wiki/Cryptography
[6] Atul Kahate, Cryptography and Network Security, Second Edition, the McGraw-Hill Companies.
[7] William Stallings, Cryptography and Network Security, Prentice Hall of India Private Limited, New Delhi.