Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Transformation of Plain Text with Two Ciphers

Rajani bala
SES, BPSMV
Khanpur kalan, Sonepat, India.

Swapnika Saxena
SES, BPSMV
Khanpur kalan, Sonepat, India.

Sonal beniwal
AP,BPSMV
khanpur kalan,sonepat, India.

Abstract: Information security has become a very critical aspect of modern computing systems. With the global acceptance of the Internet, virtually every computer in this world is connected to every other computer. Therefore, with the advent of the productivity and opportunity, it has also created risks for new users. Hence, cryptography is a tool by which the whole of the communication system can be made secure. Vigenere cipher and Ceaser Cipher when used alone proves out to be very vulnerable. This paper presents the combination of the two techniques. Combining Ceaser cipher and Vigenere cipher removes their basic weakness to give a cipher text which is hard to obtain.

Keywords: Ceaser cipher, cipher text, cryptography, plain text, Vigenere cipher.

I. INTRODUCTION

Cryptography- secret –writing- is the strongest tool for controlling against many kinds of security threats. The word cryptography means hidden writing, and it refers to the practice of using encryption to conceal text. In a communication system, the messages are exchanged between sender and receiver. To ensure the integrity and confidentiality of the messages they are encrypted using various ciphering techniques. The original message is plaintext, when encrypted gives cipher text. The encryption process is defined over the usage of key. When a single key is shared between the two entities of the communication, it is symmetric, otherwise, it is asymmetric. Traditional (recomputed) symmetric ciphers use substitution and/or transposition techniques substitution techniques map plaintext elements into cipher text elements. Transposition techniques systematically transpose the positions of plaintext elements.

(A) Ceaser Cipher

The ceaser cipher has an important place in history. It is the earliest known use of a substitution cipher, Julius Ceaser is said to have been the first to use this scheme, in which each letter is translated to the letter a fixed number of place after it in the alphabet. In Ceaser Cipher, each alphabet in a message is replaced by an alphabet three places down the line.

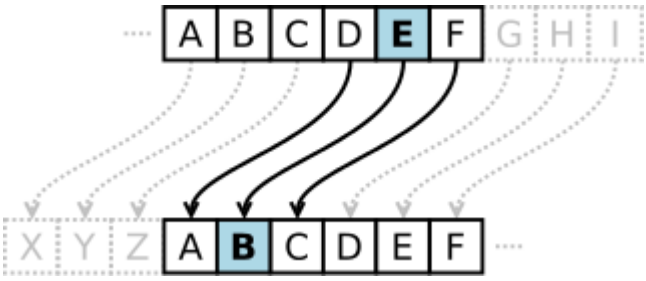

Figure 1: Ceaser Cipher

$$E_n(x) = (x-n) \bmod 26$$

$$D_n(x) = (x+n) \bmod 26$$

The main flaw in ceaser cipher is its simplicity. In a brute force attack, we have to try only 25 possible keys to generate the plaintext. Hence, it is not used in the real world scenario.

(B) Vignere Cipher

Vignere cipher is a special case of substitution techniques which uses a series of different Ceaser cipher. It is actually categorized as the polyalphabetic substitution. This was developed by Blaise de Vigenere in the 19th Century. He used a Vigenere tableau, also known as tabula recta, for enciphering and deciphering the texts.

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

A 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
B 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 A
C C 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
D 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

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

To obtain the cipher text from the table, one finds the intersection of row given by the corresponding keyword letter and the column given by the plaintext letter itself to pick out the cipher text letter.

(C) – Analysis of Ceaser Cipher and Vignere Cipher

Cryptanalysis is process of deducing or breaking the encryption and knowing the original meaning of the text, by an unauthorized person. The cryptanalysis of ceaser cipher is extremely easy. A brute-force attack can easily break the cipher text to obtain the plaintext. If it is known that a given cipher text is a ceaser cipher, then an interceptor has to try only 25 keys to decode the message. The attacker has to just know the shifts applied on the plaintext and the cipher text is decoded. Similarly in Vignere Cipher, if the attacker analyses the cipher text and calculates its statistical value then there are chances of guessing the keyword length (K). An analyst by looking at only cipher text would detect the repeated sequences at a displacement, equal to the keyword length (K). After having the brief analysis of both the techniques it has been observed that none of these techniques are secure. But on combining these two techniques we can generate a more sophisticated and secure enciphering technique.

II. Proposed Work

In this section we will present three different ways of encrypting the plaintext using both Vignere and Ceaser cipher. The key is kept common for both the techniques

Case 1- Applying ceaser cipher and vignere cipher on plaintext.

Encryption Algorithm:

Step 1- Consider a plaintext and convert it into encrypted message using ceaser cipher.
Step 2- choose a key for further encryption.
Steps 3- convert encrypted message into cipher text with the help of Vignere tableau and the key.
Step4- The cipher text is now ready for the transmission.

Decryption Algorithm:

Step 1- Consider the received cipher text and the key.
Step 2- Change the cipher text into the encrypted message with the Vignere tableau and the key.
Step 3- On receiving .he encrypted message, use ceaser cipher to change it into plaintext.
Step 4- the obtained plain text is the message sent by the sender.

Case 2- the key is encrypted using Ceaser cipher.

Encryption Algorithm:

Step1- Consider the plaintext which is to be transmitted and the key.
Step2- The key is now encrypted with the help of ceaser cipher.
Step 3- Now the encrypted key and the plaintext is converted into cipher text using Vignere tableau.
Step4- The cipher text obtained is ready for the transmission.

Decryption Algorithm:

Step 1- Receive the message sent by the sender.
Step 2- Convert the key into encrypted key using Ceaser cipher.

Step 3- make use of the encrypted key and the cipher text to convert it into plain text using Vignere tableau.
Step 4- The message sent by sender is now decoded.

Case 3- encrypting both plaintext and key using ceaser cipher.

Encryption Algorithm
Step 1- Consider the message which is to be encrypted.
Step2- Change the plaintext to cipher text and key to encrypted key using Ceaser cipher.
Step3- Now make use of the encrypted message and encrypted key to develop the cipher text using Vignere key.
Step4- The cipher text is now ready for transmission.

Decryption Algorithm:
Step 1- Receive the message sent by the sender.
Step 2-Change the key into encrypted key using Ceaser cipher.
Step 3-Take the message and the encrypted key to develop a plaintext using Vignere tableau.
Step 4-On reception of the plaintext, use ceaser cipher to convertthe plaintext back into the message.
Step 5-Now, The message has been received.

III Example

Message : this is my first paper
Key : accept

CASE1:

Encryption

Plain text	T	H	I	S	I	S	M	Y	F	I	R	S	T	P	A	P	E	R
Encrypt plain text	Q	E	F	P	F	P	J	V	C	F	O	P	Q	M	X	M	B	O
Key	A	C	C	E	P	T	A	C	C	E	P	T	A	C	C	E	P	T
Cipher text	Q	G	H	T	U	I	J	X	E	J	D	I	Q	O	Z	Q	Q	H

Decryption

Cipher text	Q	G	H	T	U	I	J	X	E	J	D	I	Q	O	Z	Q	Q	H
Key	A	C	C	E	P	T	A	C	C	E	P	T	A	C	C	E	P	T
Encrypt plain text	Q	E	F	P	F	P	J	V	C	F	O	P	Q	M	X	M	B	O
Plain text	T	H	I	S	I	S	M	Y	F	I	R	S	T	P	A	P	E	R

CASE2 :

Encryption

Plain text	T	H	I	S	I	S	M	Y	F	I	R	S	T	P	A	P	E	R
Key	A	C	C	E	P	T	A	C	C	E	P	T	A	C	C	E	P	T
Encrypt Key	X	Z	Z	B	M	Q	X	Z	Z	B	M	Q	X	Z	Z	B	M	Q
Cipher text	Q	G	K	T	X	I	J	X	E	M	D	I	Q	O	Z	Q	Q	H

Decryption

Cipher text	Q	G	K	T	X	I	J	X	E	M	D	I	Q	O	Z	Q	Q	H
Encrypt Key	X	Z	Z	B	M	Q	X	Z	Z	B	M	Q	X	Z	Z	B	M	Q
Key	A	C	C	E	P	T	A	C	C	E	P	T	A	C	C	E	P	T
Plain text	T	H	I	S	I	S	M	Y	F	I	R	S	T	P	A	P	E	R

CASE3 :

Encryption

Plain text	T	H	I	S	I	S	M	Y	F	I	R	S	T	P	A	P	E	R
Encrypt plain text	Q	E	F	P	F	P	J	V	C	F	O	P	Q	M	X	M	B	O
Key	A	C	C	E	P	T	A	C	C	E	P	T	A	C	C	E	P	T

Encrypt Key	X	Z	Z	B	M	Q	X	Z	Z	B	M	Q	X	Z	Z	B	M	Q
Cipher text	N	D	E	O	R	F	G	U	B	G	A	F	N	L	W	N	N	E

Decryption

Cipher text	N	D	E	O	R	F	G	U	B	G	A	F	N	L	W	N	N	E
Encrypt Key	X	Z	Z	B	M	Q	X	Z	Z	B	M	Q	X	Z	Z	B	M	Q
Key	A	C	C	E	P	T	A	C	C	E	P	T	A	C	C	E	P	T
Encrypt plain text	Q	E	F	P	F	P	J	V	C	F	O	P	Q	M	X	M	B	O
Plain text	T	H	I	S	I	S	M	Y	F	I	R	S	T	P	A	P	E	R

IV Advantages

These variations of Ceaser cipher along with Vignere Cipher leads to various advantages. These are:

1. Cryptanalysis is difficult.
2. The relation between the plaintext and the key as well as the relation between the key and the cipher text is made as complex as possible.
3. Brute-force attack is a complete failure.
4. Removes the weaknesses of both Ceaser cipher and Vignere tableau.

V- Conclusion

Ceaser cipher is the oldest and simplest known substitution technique. Because of its simple structure, it is very vulnerable to cryptanalytic attacks. Also, the Vignere cipher is also not secure. It is because the key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied. But when these two (Ceaser cipher and Vignere cipher) are used together, they remove each other's weaknesses. Hence we present an improved version of both Ceaser cipher and Vignere cipher, which is more sound and secure cryptographic technique

.

Acknowledgement

We would like to express our sincere gratitude to Mrs. Sonal Beniwal for her continuous encouragement and guidance over the paper.

Refrences

[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/vignerecipher.html
[4] practicalcryptography.com/ciphers/rail-fence-cipher/

