Automatic Key Generation of Caesar Cipher

B. Bazith Mohammed[#1]

[#]*Co-ordinator ASK Solutions*

Abstract*— Cryptography has been through numerous phases of evolution. Early ciphers in cryptography were designed to allow encryption and decryption to take place by hand, while those which are developed and used today are only possible due to the high computational performance of modern machines [1]. Conceptually cryptographic technique divided into two categories substitution and transposition methods. Transposition Ciphers are a bit different to Substitution Ciphers. Whereas Substitution ciphers replace each letter with a different letter or symbol to produce the cipher text, in a Transposition cipher, the letters are just moved around. There are numerous number of algorithms are proposed in both techniques. But combination of these techniques rare in the cryptographic trends. So this paper is providing combination of caesar cipher and railfence cipher are proposed. Also the caesar cipher key generation new way to proposed using automatic key generation techniques. Our algorithm supports security for the data containing alphabets with case sensitive, numbers and special characters. The proposed method can be used to simply encode the message for preserving privacy. It is difficult to understand the cipher text..

Keywords*— Caesar Cipher, Cryptography, Symmetric Key, Network Security.

I. INTRODUCTION

The word cryptography comes from the Greek words Crypto and Graphy. Crypto means Secret and Graphy means Writing. Cryptography deals with creating documents that can be shared secretly over public communication channels. Cryptography is the study of creating and using encryption and decryption techniques. An encryption algorithm works with a key to transform the plaintext into cipher text. Decryption algorithm works in the reverse order and converts the cipher text into. Usually key is a number that is mixed with plaintext to yield cipher text. The process of converting plaintext into cipher text is called enciphering or encryption. The process of retaining the plaintext from the cipher text is called deciphering or decryption. In general cryptography is used to achieve authentication, confidentiality, integrity and non-repudiation to ensure reliability of data.

Cryptography is grouped into Symmetric Key and Asymmetric Key Cryptography [3]. In *Symmetric key cryptography*, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions. The *Asymmetric Key Cryptograph*y uses different keys for encryption and decryption. The encryption key is public so that anyone can encrypt a message. However, the decryption key is private, so that only the receiver is able to decrypt the message. It is common to set up "key-pairs" within a network so that each user has a public and private key. The public key is made available to everyone so that they can send messages, but the private key is only made available to the person it belongs to [4].

Two types of ciphers are used in Symmetric Key Cryptography. They are stream cipher and block cipher. Stream ciphers encrypt the bits of information one at a time - operate on 1 bit of data at a time. Stream ciphers are faster and smaller to implement than block ciphers, however, they have an important security gap. If the same key stream is used, certain types of attacks may cause the information to be revealed. Block cipher is a symmetric cipher which encrypts information by breaking it down into blocks and encrypting data in each block. A block cipher encrypts data in fixed sized blocks [6].

II. CAESAR CIPHER

The simplest possible substitution cipher is the *Caesar cipher*, reportedly used by Julius Caesar during the Gallic Wars. Each letter in the plaintext is replaced by a letter shifted a fixed number of places to the right. (Caesar normally used a shift of three places). We regard the alphabet as a cycle, so that the letter following Z is A. Thus, for example, the table below shows a right shift of 5 places.

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
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

The message “Send a hundred slaves as tribute to Rome” would be enciphered as XJSI F MZSIWJI XQFAJX FX YWNGZYJ YT WTRJ. The key is simply the number of places that the letters are shifted, and the cipher is decrypted by applying the shift in the opposite direction (five places back). Some practical details make the cipher harder to read. In particular, it would be sensible to ignore the distinction between capital and lower case letters, and also to ignore the spaces between words [2]. The Caesar cipher is not difficult to break. There are only 26 possible keys, and one can try them all.

XJSI F MZSIWJI XQFAJX FX YWNGZYJ YT WTRJ

KEY

In this case, the plaintext leaps out as occupying the fifth line. Encryption of a letter x by a shift n can be described mathematically

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

Decryption is performed similarly

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

In the above, the result is in the range 0…….25. If x+n (or) x-n are not in the range 0……25, we have to subtract or add 26.

2.1 Limitations

- It cannot use special character and numbers.
- Space between two words in the plaintext is not considered as one character.
- It is not case sensitive.
- All the 25 possible keys can be tried for the easy identification of the plaintext.

III. RAIL FENCE CIPHER

The railfence cipher is a very simple, easy to crack cipher. It is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the cipher text. The railfence cipher offers essentially no communication security, and it will be shown that it can be easily broken even by hand. Although weak on its own, it can be combined with other ciphers, such as a substitution cipher, the combination of which is more difficult to break than either cipher on it's own. Many websites claim that the rail-fence cipher is a simpler "write down the columns, read along the rows" cipher. This is equivalent to using an un-keyed columnar transposition cipher [7].

IV. PROPOSED METHOD

This algorithm can accept the Plaintext containing Alphabets (capital letters and small letters), Numbers and Special characters. So the user can easily encrypt combination of alphabets, numbers and characters efficiently.

A. Encryption Algorithm

Phase 1: Encryption of Caesar cipher

Step 1: Generate the ASCII value of the each plaintext letter.
Step 2: Sum the ASCII value of all character.
Step 3: Mod the value of 256 because total number of key consider as ASCII value.
Step 4: Corresponding ASCII value is considered as a key.
Step 5: To apply the below given formula to generate cipher text.

K= (1^{st} char+2^{nd} char+…..n^{th}char)%256
E = ((P + K) % 256)
p – Plaintext, k – key.

Step 6: The cipher text value of the ceaser cipher to perform the Transposition.

Phase 2: Encryption of Rail Fence Cipher

Step 7: the cipher text value of the Substitution method as input of the Rail Fence Cipher
Step 8: Here we are consider as Key value 3.
Step 9: Perform Rail Fence Cipher to generate the final cipher text.

B. Decryption Algorithm

Phase 1: Decryption of Caesar cipher

Step 1: Perform Rail Fence Cipher decryption process using the key value of 3.
Step 2: To generate the cipher text of Substitution.

Phase 2: Decryption of Ceaser cipher

Step 3: Perform step3 value as input of the ceaser cipher method.
Step 4: Here the same encryption key used.
Step 5: To apply the below given formula:
D = ((p – k) % 256)
c – Cipher text, k – key
Step 6: Generate the ASCII character of the corresponding decimal value. This would be the original plaintext.

Example 1

Encryption

Phase 1: Encryption of Caesar cipher

Let, the plaintext is "welcome". Now according to the steps we will get the following:
Key Generation:
The ASCII value of the welcome is follows: 119, 101, 108, 99, 111, 109, 101
Key value = 119+ 101+ 108+ 99+111+ 109+ 101
= 748 Mod 256
= 236.

TABLE I

Plaintext	Key	Cipher Text (key + plaintext) %256	Cipher text
w	236	119+236 = 355 MOD 256 =99 ASCII value	c
e	236	101+236 = 337 MOD 256 =81 ASCII value	Q
l	236	108 +236 = 344 MOD 256 =88 ASCII value	X
c	236	99 +236 = 335 MOD 256 =79 ASCII value	O
o	236	111 +236 = 347 MOD 256 =91 ASCII value	[
m	236	109 +236 = 345 MOD 256 =89 ASCII value	Y
e	236	101+236 = 337 MOD 256 =81 ASCII value	Q

As per result of the ceaser cipher algorithm cipher text would be "**cQXO[YQ**".

Phase 2: Encryption of Rail Fence Cipher

The cipher text of the ceaser cipher as plaintext of Rail Fence Cipher
Perform railfence cipher
Plaintext - **cQXO[YQ**
Keyvalue - 3
cipher text - **c[QOYXQ**

Decryption

Phase 1: Decryption of Rail Fence Cipher

After encrypting "welcome" we have got "**c[QOYXQ**" as the cipher text. Now according to decryption algorithm let's try to get back the original text i.e. "welcome".

The cipher text **c[QOYXQ** to decrypt using Rail Fence Cipher and get **cQXO**[**YQ.**

Here, same key "3" is used in Rail Fence Cipher.

Phase 2: Decryption of Caesar cipher

The formula is applied to the ASCII value 54 of the cipher text character and key 5.

$$D = ((p – k) \% 256)$$

"**cQXO**[**YQ**" is the ASCII character of the decimal values applied "welcome" would be the original plaintext.

A. Advantage of Proposed Method

- The Algorithm is very simple in nature.
- The user can easily encrypt and decrypt the combination of alphabets, numbers and special characters efficiently.
- It considers the space between two words in plaintext as one character.
- It is case sensitive.
- To compare with the existing algorithms, it is very difficult to find the Plaintext from Cipher text.

V. Conclusion

Classical ciphers can be made effective and used for providing security by adding the properties possessed by the modern ciphers. The key generation plays a important role in designing the ciphers. It is concluded that the proposed method is a refinement of existing Caesar method overcoming the drawbacks of the method. Also the key generation new method for automatically generating in the caesar cipher is important role in our proposed method. The concept of key is introduced with Caesar cipher to generalize the encryption concept. This is further extended to complicate the age old basic method to a cumbersome method. In order to complicate cipher text.

References

[1] http://practicalcryptography.com/ciphers/

[2] William Stallings, "Cryptography and Network Security: Principles and Practice", 4th Edition, Prentice Hall, 2006.

[3] Hans Delfs and Helmut Knebl, "Introduction to Cryptography: Principles and Applications", Springer International Edition.

[4] Ayushi, "A Symmetric Key Cryptographic Algorithm". International Journal of Computer Applications (0975 – 8887), Volume.1, No.15.

[5] http://en.wikipedia.org/wiki

[6] Behrouz A. Forouzan, "Data Communications and Networking", 4th Edition, McGraw-Hills, 2006

[7] http://practicalcryptography.com/ciphers/rail-fence-cipher/