Volume 2, Issue 7, July 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Plaintext Based Transposition Method

Prof. S. D. Padiya*
Sipna COET,
Amravati, India

Prof. D. N. Dakhane
Sipna COET,
Amravati, India

Abstract— Cryptography is the art and science of achieving security by encoding message to make them non-readable. There are many techniques to encrypt plaintext and convert it to the cipher text. There are two primary ways in which a plaintext message can be codified to obtain the corresponding cipher text : 1) Substitution and 2) Transposition. Earlier we developed few transposition techniques. In this paper we have to attempt to enhance those techniques and made them more advanced. One of the most important things is that all the old techniques such as rail fence and simple columns are key-based and the key is in, any sequence or in any order to encrypt the plaintext. The reverse transposition technique and Odd-Even transposition technique (The IUP journal of Computer sciences, Vol. V, No. 4, 2011) are in which key is depend on the plaintext so that sender or receiver can easily understand and easily decrypt the cipher text into plaintext but these techniques does not provides any limitation for the generation of key value, does not provide any idea above the digits, characters and special character. There is no provision to recapture blank spaces of the words of the plaintext.

Index Terms — Cryptography, Encryption, Decryption, Plaintext, Cipher text, Cryptanalyst, Attacks and Network Security.

I. INTRODUCTION

Cryptography is the art and science of achieving security by encoding message to make them non-readable. In cryptographic terms, Clear text or Plain text signifies a message that can be understood by the sender, the recipient, and also by anyone else who gets an access to that message (original message). Cipher text signifies a message that is codified using any suitable scheme (encrypted message).

The transmitter in secure system encrypts the original readable message (plaintext) to hide its meaning. This reversible mathematical process produces an encrypted output called cipher text. Cipher is an algorithm used to encrypt the message [2]. The encryption algorithm runs in reverse to capture the plaintext, known as Decryption. It takes the cipher text and the secret key and produces the original plaintext [4]. The Cryptanalyst is the science of breaking ciphers without knowing the key. It converts cipher text back to the plaintext without knowing key. It is possible by using number of attacks. The person who performs this hacking is known as cryptanalyst [2].

In this paper, the encryption algorithm is a block cipher which operates on blocks of data. Hence, for more secure encryption the block value must be change randomly. The value must be different for each message. The block size is depends on the key, which varies for each encryption.

In (The IUP Journal of Computer sciences, Vol. V, No. 4, 2011) by Satish Bansal and Rajesh Shrivastava, transposition technique algorithms 1) 'Reverse transposition cipher' and 2) 'Odd-even transposition technique' were introduced. These are simple in which key value is based on the number of words, lines or paragraphs. This used of the random key makes the process of cryptography more secure. These techniques have few disadvantages are as:

1) This technique does not provide any range for the generation of key. According to this method the key value may be any value greater than or equal to one. This generation of non-limiting key process is problematic. The value of key less than 5 (2, 3 or 4), perform the reverse operation of only 2, 3, or 4 characters respectively.
2) Any key value greater than 10, perform the reverse operation of words. This method does not provide effective generation of key.
3) The 'Reverse transposition cipher' performs the deletion of spaces between the words. But it does not provide any method to recapture of these spaces at decryption side.

Only rearrangement of key number of characters, it is very easy to perform cryptanalyst by using different attacks like Brute-force attack.

II. ALGORITHM

A) ENCRYPTION

1) First, we take a message (plain text) from user which we have to encrypt.
2) Find the value of P ie. number of character which present maximum number of time in the given plaintext.
3) Find the value of Q ie. number of characters which present minimum number of times in the given plaintext.
4) Calculate, N = P-Q;
5) if (N<9 && N>2)
   Perform K = N;

else

Perform K = N%9;

if (K=0 || K=1 || K=2)

Perform K = K+3

6) Replace all characters which present maximum number of times in the plaintext by the character which present minimum number of time.
7) Replace all characters which present minimum number of times in the plaintext by the character which present maximum number of time.
8) Form the group of 'K' characters including space, digits, characters and all special characters.
9) Reverse characters of each group.
10) Finally we get secure encrypted message (cipher text).

B) DECRYPTION

The encryption algorithm runs in reverse to capture the plaintext, known as Decryption. It takes the cipher text and the secret key which produces the original plaintext [4]. The generation of security key is totally based on the plaintext. It mainly depends on the number of characters which present maximum as well as minimum number of times in the given plaintext. In the encryption process algorithm only replace the characters which present maximum number of times by the characters which present minimum number of times and vice versa. There is no change in the value of P and Q ie. No change in the value of K.

The encryption algorithm as it is may use for the decryption.

II. EXAMPLE

A) ENCRYPTION

1) Suppose plaintext is :

To accomplish great things, we must not only act,
but also dream.

2) In above plaintext the character 't' present maximum number (7) times,
P = 7;

3) In above plaintext the character 'p' present minimum number (1) time,
Q = 1;

4) Calculate :
N = P- Q;
N = 7 – 1 = 6;

5) If (N<9 && N>2)
(6<9 && 6>2)
(T && T) = T
a. Perform K = N;
K = 6;

6) Replace all characters 't' by 'p' and all characters 'p' by 't'.

To accomplish great things, we must not only act, but also dream.

po accomtlish greap phings, we musp nop only acp, bup also dream.

7) K=6, form the group of '6' characters including space, digits, characters and all special characters.

po_acc omtlis h_grea p_phin gs,_we _musp_ nop_on ly_acp ,_bup_ also_d ream.

8) Reverse characters of each group.

cca_op siltmo aerg_h nihp_p ew_,sg _psum_ no_pon pca_yl _pub_, d_osla .maer

9) Finally we get secure encrypted message

cca opsiltmoaerg hnihp pew ,sg psum no ponpca yl pub ,d osla.maer

B) DECRYPTION

1) Take cipher text :

cca opsiltmoaerg hnihp pew ,sg psum no ponpca yl pub ,d osla.maer

2) In above plaintext the character 'p' present maximum number (7) times,
P = 7;

3) In above plaintext the character 't' present minimum number (1) time,
Q = 1;

4) Calculate :
N = P- Q;
N = 7 – 1 = 6;

5) If (N<9 && N>2)
(6<9 && 6>2)
(T && T) = T
a. Perform K = N;
K = 6;

6) Replace all characters 'p' by 't' and all characters 't' by 'p'.

cca_op siltmo aerg_h nihp_p ew_,sg _psum_ no_pon pca_yl _pub_, d_osla .maer

7) K=6, form the group of '6' characters including space, digits, characters and all special characters.

cca_ot silpmo aerg_h niht_t ew_,sg _tsum_ no_ton tca_yl tub_,d _osla. maer

8) Reverse characters of each group.

to_acc omplis h_grea t_thin gs,_we _must_ not_on ly_act ,_but_ also_d ream.

9) Finally we get decrypted original information.

to accomplish great things, we must not only act, but also dream.

IV. APPLICATION

This 'Plain text based transposition method' contains few advantages over the old transposition methods.

1) It provides limiting range (3-to-9) for the generation of key. ie. It not allowed the key value 0, 1, or 2 and any value greater than 9.
2) Since, key value must not be less than 3, does not allows the reverse operation for 2 or 3 characters.
3) Since, key value must not be greater than 9, does not allows the reverse characters operation of words.
4) The mod (%) operation provides limiting range.
5) It performs the encryption of letters, digits, characters and all special characters.
6) The Brute-force attack is not possible, it have large probability value.
7) The resultant cipher text is a combination of letters (26), digits (10), characters and special characters (32). Due to this, attacks must attempt (26+10+32)! number of changes. It is very hard to achieve practically.
8) The replacement of random (not fixed) characters of the plain text, makes more complex encryption.
9) It is very easy for decryption, Using same algorithm of encryption, user can find original message (plaintext).
10) Due to the replacement of characters by another characters, the meaning of words changes, attacker never find the meaningful words.
11) Key value is based on the plaintext, no need to transmit key from sender to receiver.

V. DISADVANTAGES

1) Complex method for implementation.
2) Complex due to used of digits, characters and special characters.

VI. CONCLUSION

Transposition is often combined with other techniques. With the power of computers, substitution and transposition encryption can be easily performed. The combination of these two classic techniques provides a more secure and strong cipher. The key is like a password for cipher text which is so strong that no one can break it.

Transposition method only provides the rearrangement of characters of the plaintext. The attacker may attacks on the cipher text to known plaintext. Above described method contain transposition as well as substitution method which makes secure and strong cipher text.

REFERENCES

[1] "*Transposition method for cryptography*" by Satish Bansal and Rajesh Shrivastava in 'The IUP Journal of Computer Sciences, Vol. V, No. 4, 2011'.
[2] Atul Kahate (2009), *Cryptography and Network Security*, 2nd edition, McGraw-Hill.
[3] Stallings W (1999), *Cryptography and Network Security*, 2nd edition, Prentice Hall.
[4] William Stallings (2003), *Cryptography and Network Security*, 3rd edition, Pearson Education.

