International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

A Review Paper on Cryptography and Plaintext Based Transposition Method

Priya Soni, Ritu Hedau

Department of IT, SSGMCE, Shegaon, Buldhana, India

ABSTRACT

From last few years, the public is becoming dependent on computers and networks , so they are also interested in the security of these same computers and networks. Encryption algorithm provides the necessary protection against the data intruders' attacks by converting information from its original form into an unreadable form. The majority of current web authentication is built on username/password. And the password replacement offers more security, but it is very much difficult to use and expensive to deploy. Security of data can be done by a technique called cryptography. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium ,which includes just about any network , particularly the Internet. At present, the range of cryptography applications have been expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against unauthorized access and to prevent the practice of spying. Cryptography is a developing technology, which is important for network security and computer security. Study on cryptography is still in its developing stages and a considerable research effort is still required for secured communication. This paper talks about the cryptographic algorithm and Transposition technique.

Keywords : Cryptography, Encryption, Decryption, Plaintext, Cipher Text, Public Key Cryptography, Symmetric Cryptography Network Security, Transposition Technique.

I. INTRODUCTION

Cryptography, a word with Greek origins, means "secret writing" is the science of devising methods that allow for information to be sent in a secure form in such a way that the only person able to retrieve this information is theintended recipient. The message to be sent through an unreliable medium is known as **plaintext**, which is encrypted before sending over the medium. The encrypted message is known as **cipher text**, which is received at the other end of the medium and decrypted to get back the original plaintext message. Hence a cryptosystem is a collection of algorithms and associated procedures for hiding and revealing information.

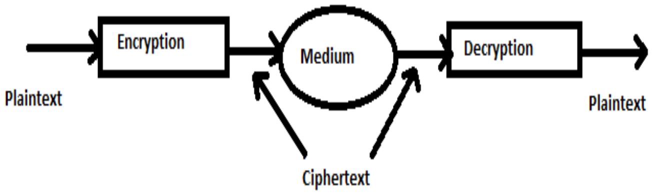


Figure 1. A Simple Cryptography Model

Cryptography algorithms can be divided into two broad categorizes - **Symmetric key cryptography** and **asymmetric key cryptography**

Asymmetric-Key Cryptography:

In symmetric key cryptography, same key is shared, i.e. the one key is used in both encryption and decryption, hence also known as single key or secret key encryption.Symmetrickey cryptography algorithms are simple requiring lesser execution time. As a consequence, these are commonly used for long messages. There are two types of symmetric keyencryption modes one as block ciphers and other as stream ciphers. Block ciphers operate on groups of bits called blocks and each block is processed multiple number of times. The key applied in each round is in a unique manner. A stream cipher operates on one bit at a time i.e. The data is divided as small as single bits and then the encryption is done. In symmetric key encryption the AES algorithm and the DES algorithm different factors are analyzed.

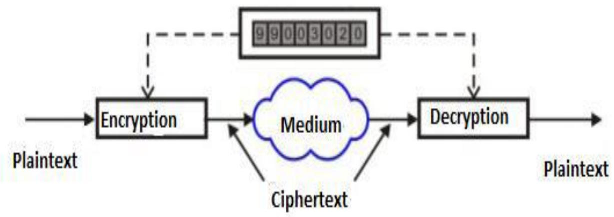


Figure 2. A Simple Symmetric Key Cryptography Model

Asymmetric-Key Cryptography:

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. In such type of cryptography user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

RSA and Merkle–Hellman knapsack cryptosystem is the most commonly used asymmetric key algorithm. The security of RSA relies on the difficulty of factoring large integers [7].

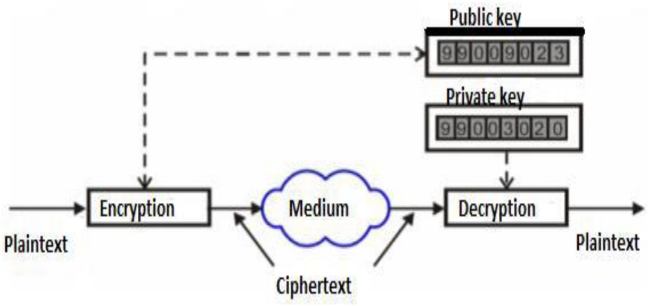


Figure 3. A Simple Asymmetric Key Cryptography Model

II. TRANSPOSITION TECHNIQUES

All the techniques examined so far involve the substitution of a ciphertext symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message "meet me after the toga party" with a rail fence of depth 2, we write the following
m e m a t r h t g p r y e t e f e t e o a a t

The encrypted message is

MEMATRHTGPRYETEFETEOAAT

This sort of thing would be trivial to cryptanalyze. A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of the columns then becomes the key to the algorithm. For example,

Key: 4 3 1 2 5 6 7
Plaintext: a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z
Ciphertext:

TTNAAPTMTSUOAODWCOIXKNLYPETZ

1. Pure Cipher

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. For the type of columnar transposition just shown, cryptanalysis is fairly straightforward and involves laying out the ciphertext in a matrix and playing around with column positions. Diagram and trigram frequency tables can be useful.

The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is a more complex permutation that is not easily reconstructed. Thus, if the foregoing message is reencrypted using the same algorithm,

Key: 4 3 1 2 5 6 7
Input: t t n a a p t
m t s u o a o
d w c o i x kn l y p e t z

Output:

NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

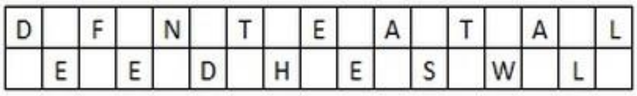
To visualize the result of this double transposition, designate the letters in the original plaintext message by the numbers designating their position. Thus, with 28 letters in the message, the original sequence of letters is

01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28
After the first transposition we have
03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28
which has a somewhat regular structure. But after the second transposition, we have
17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28
This is a much less structured permutation and is much more difficult to cryptanalyze.

2. Rail Fence Cipher

Rail Fence cipher is a form of transposition cipher, in which letters of the plaintext are written alternating between rows and the rows are then read sequentially to give the cipher. In a depth -two rail fence (two rows) the message "CRYPTOGRAPHY AND NETWORK SECURITY"

For example, the plaintext "defend the east wall" is written as shown below, with all spaces removed.



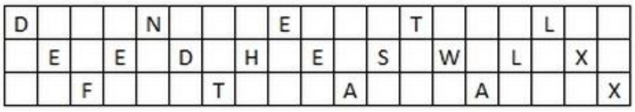
D		F		N		T		E		A		T		A		L
	E		E		D		H		E		S		W		L	

The simplest Rail Fence Cipher, where each letter is written in a zigzag pattern across the page.

The ciphertext is then read off by writing the top row first, followed by the bottom row, to get "DFNTEATALEEDHESWL".

Encryption

To encrypt a message using the Rail Fence Cipher, you have to write your message in zigzag lines across the page, and then read off each row. Firstly, you need to have a key, which for this cipher is the number of rows you are going to have. You then start writing the letters of the plaintext diagonally down to the right until you reach the number of rows specified by the key. You then bounce back up diagonally until you hit the first row again. This continues until the end of the plaintext.
For the plaintext we used above, "defend the east wall", with a key of 3, we get the encryption process shown below.



D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

The Rail Fence Cipher with a key of 3. Notice the nulls added at the end of the message to make it the right length.

Note that at the end of the message we have inserted two "X"s. These are called nulls, and act as placeholders. We do this to make the message fit neatly in to the grid (so that there are the same number of letters on the top row, as on the bottom row. Although not necessary, it makes the decryption process a lot easier if the message has this layout.

The ciphertext is read off row by row to get "DNETLEEDHESWLXFTAAX".

3. Columnar Transposition Cipher

The columnar transposition cipher is a fairly simple, easy to implement cipher. It is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the ciphertext.

Although weak on its own, it can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on it's own. The ADFGVX cipher uses a columnar transposition to greatly improve its security.

Example

The key for the columnar transposition cipher is a keyword e.g. GERMAN. The row length that is used is the same as the length of the keyword. To encrypt a piece of text, e.g.
defend the east wall of the castle
we write it out in a special way in a number of rows (the keyword here is GERMAN):
<u>G E R M A N</u>
d e f e n d

t h e e a s
t w a l l o
f t h e c a
s t l e x x

In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.

A E G M N R
n e d e d f
a h t e s e
l w t l o a
c t f e a h
x t s e x l

The ciphertext is read off along the columns:
nalcxehwttdttfseeleedsoaxfeahl

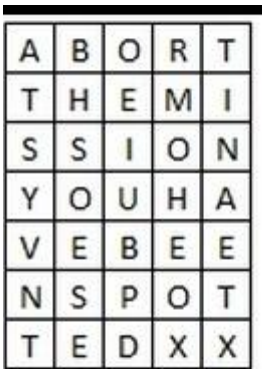
4.Route transposition Cipher

The Route Cipher is a transposition cipher where the key is which route to follow when reading the ciphertext from the block created with the plaintext. The plaintext is written in a grid, and then read off following the route chosen

Encryption

First we write the plaintext in a block of reasonable size for the plaintext. Part of your key is the size of this grid, so you need to decide on either a number of columns or number of rows in the grid before starting. Once the plaintext is written out in the grid, you use the Route assigned. This could be spiralling inwards from the top right corner in a clockwise direction, or zigzagging up and down.

As an example, lets encrypt the plaintext "abort the mission, you have been spotted". First we need to decide on the number of columns we are going to use, lets say 5.



A	B	O	R	T
T	H	E	M	I
S	S	I	O	N
Y	O	U	H	A
V	E	B	E	E
N	S	P	O	T
T	E	D	X	X

The plaintext written in a grid with 5 columns. Notice how we have used nulls at the end of the message to make a nice rectangle.
We then choose which route we want to use to encrypt the message.

With a route of reading down the columns we get the ciphertext: "ATSYV NTBHS OESEO EIUBP DRMOH EOXTI NAETX".

With a route of spiralling inwards counter-clockwise from the bottom right we get: "XTEAN ITROB ATSYV NTEDX OEHOM EHSOE SPBUI".

Decryption

To decrypt a message received that has been encoded with the Route Cipher, we need to know the route used and the width or height of the grid. We then start by constructing a blank grid of the right size, and then place the ciphertext letters in the grid following the route specified

III. 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)
6) Perform First, we take a message (plain text) from user which we have to encrypt.

7) Find the value of P ie. number of character which present maximum number of time in the given plaintext.
8) Find the value of Q ie. number of characters which present minimum number of times in the given plaintext.
9) Calculate, N = P-Q;
10) if (N<9 && N>2)
    Perform
        else

            Perform K = N%9;

    if (K=0 || K=1 || K=2) Perform K = K+3
        a. Perform K = N; K =6;

11) Replace all characters which present maximum number of times in the plaintext by the character which present minimum number of time.
12) Replace all characters which present minimum number of times in the plaintext by the character which present maximum number of time.
6) Form the group of „K‟ characters including space, digits, characters and all special characters.
7) Reverse characters of each group.

Finally we get secure encrypted message (cipher text).

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.

EXAMPLE

- ENCRYPTION
  - Suppose plaintext is :

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

1. In above plaintext the character „t‟ present maximum number (7) times,
   P = 7;
2. In above plaintext the character „p‟ present minimum number (1) time,
   Q = 1;
3. Calculate :
   N = P- Q;
   N = 7 – 1 = 6;
   If (N<9 && N>2) (6<9 && 6>2) (T && T) = T
4. 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.

5. 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.

6. Reverse characters of each group.

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

7. 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.

DISADVANTAGES

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

V. CONCLUSION

In this paper, encryption algorithms “Transposition cipher” are described. It is used to achieve the mains of security aim like confidentiality, integrity, authentication, non-repudiation. In order to achieve these goals, Several algorithms have been developed. The algorithm for encryption can be selected based on the type of data being communicated and type of channel through which data is being communicated.

VI. REFERENCES

[1]. Plaintext Based Transposition Method by Prof. S. D. Padiya* Prof. D. N. Dakhane Sipna COET, Sipna COET, Amravati, India Amravati, India in International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 7, July 2012 ISSN: 2277 128X

[2]. "Color Cryptography using Substitution method" by Manali Naik, Pushpanjali Tungare, Pooja Kamble, Shirish Sabnis in International Research Journal of Engineering and Technology (IRJET) Vol. V, No. 3, 2016‟.

[3]. "Cryptography: The Sciene of Secure Communication" by Jangala. Sasi Kiran M.Anusha, A.Vijaykumar, M.Kavya in IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.4, April 2016

[4]. "A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms" by Nivedita Bisht, Sapna Singh in International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 3, March 2015

[5]. William Stallings (2005), Cryptography and Netwotk security principles and practices, 4th edition.