IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Design and Develop an Effective Cryptographic System using Diagonal Transposition, Substitution and Oscillation Techniques

[1]U. Thirupalu,
Associate Professor,

[2]Dr. P. Chandra Kanth,
Assistant Professor,

[1,2]Dept. of Computer Science,
Audisankara College of Engineering and Technology,
Andhra Pradesh, India.

Abstract *- In this paper, we given the overview about cryptography and the techniques, which are used for converting a readable text into non readable text. This feature makes data more secure. To increase security of massages which are sent over the internet, we use such type of technique and study of this is called cryptography. This paper proposes to generate cipher text with the help of various techniques like transpositions, substitute and oscillation technique.*

Keywords – Cryptography, Substitution Technique, Transposition Technique, Oscillation Technique, Plaintext, Ciphertext.

I. Introduction

Cryptography is the art and science of encoding messages from readable format to non-readable format. In terms of data and telecommunications, cryptography plays an important role when we communicate over any untrusted medium like internet. While communicating over the network some specific security requirements are need such:

Authentication: It proves the identity of the person to whom we are communication or we can say that it provides the host to host authentication overt the internet.

Confidentiality: It ensures that no one can read the message other than sender.

Integrity: it assumes that message has not altered in any way from the original during arrival from sender to receiver.

Non-repudiation: It is a mechanism which proves that sender really sent this message.

So we can now say that cryptography not only protects data from theft but it can also be used for authentication of user. In all cases, initial data in plain text and data after encryption is known as cipher text which in turn converted back to plain text for reading the plain text.

II. Cryptography

Cryptography is the art and science of achieving security by converting readable message into non readable format.

Cryptography is the technique of converting non readable form without knowing how they were converted from readable to non-readable from.

Cryptology is the combination of cryptography and cryptanalysis.

In early days, the cryptographic operations are done manually i.e. if we have to make any message secure, then we have to perform all task manually it takes lot of time but now computer perform these cryptographic functions and it is more secure and perform very fast than humans.

Basic terms used in network security are:

Plain text:

Any language which is supported to communicate the humans is usually called Plaintext. Generally, a message in plain text is understood by everybody if they know that language. For instance, when we don't want to hide anything from the persons available near us we use plain text to exchange information. Suppose that I say '*Hi'* to my friend and anybody who is listening to our conversation they can easily come to know that I am greeting my friend because I am not talking something important. If someone know that language that I am using they can get the message without problem.

We also use plain text during electronic communication. For example, suppose someone is sending an email to his friend and message in the mail is not that much important then he can use plain text in English language or in any other language.

Cipher text:

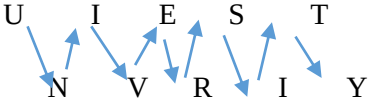
It is a scramble text, which is not understandable by the others. It is also a text which is converted the format of message into non-readable format using any scheme available to us.

III. Techniques

Substitution technique*:* It is the technique which replaces the alphabet of plain text with any other alphabet that is we substitute the character of plain text with other character. There are several schemes for the substitute techniques like Caesar cipher, Playfair cipher, One-time pad etc.

Transposition technique: In the cryptography system, a transposition cipher is a method of encryption by changing the position of plain text into different position. In this technique, the character or group of characters are shifted into different positions. That is the order of units is changed mathematically and get the cipher text. There are several techniques. They are:

i) *Rail fence technique:* It is the technique which rotates the position of plain text into cipher text. For example the message UNIVERSITY is positioned and get the cipher like the following.



Plain text: UNIVERSITY

Cipher text: UIESTNVRIY

ii) *Columnar transposition technique*: In this technique, we 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 column then becomes the key to the algorithm. For example,

Key: 5 3 1 2 4

Palin text: C O M P U

T E R S C

I E N C E

Ciphertext: MRNPSCOEEUCECTI

IV. Oscillation

Oscillation is the repetitive variation, typically in time of some measure about a central value or between two or more different states.

It is the motion of an Object that regularly repents itself, back and forth, over the same path.

Characteristic of Oscillation: It as the following characteristics.

- Oscillation motion is about some (energy = 0) equilibrium position.
- Oscillation motion is periodic, with a definite period or cycle time.

The steps which are satisfy the above are as follow.

- Cycle – One complete Oscillation.
- Frequency (f) – Number of cycle or oscillation completed per second.
  UNITS = 1/s or Hertz (Hz)
- Period (t) – The time for one cycle.
- Amplitude (A) – The maximum displacement from equilibrium.

The diagrammatic representation of oscillation is as follows.

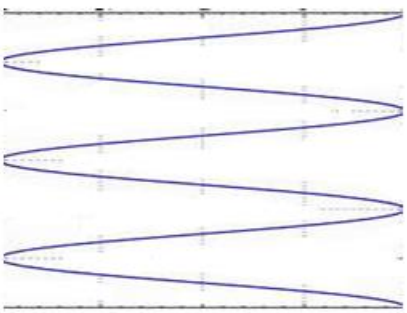


Figure 1: Oscillation model

V. Proposed Work

Diagonal transposition technique is used to arrange the elements into diagonal positions. The *substitution* technique is used to arrange the plaintext letters with other letters. There are several substitution techniques, here we use **Caesar Cipher** in different manner. Generally, the Caesar Cipher involves to replace each letter of the alphabet with the letter standing at a number (usually key k=3) places further down the alphabet. Most of the application use the key size as standard, in our paper the key size is different, which is related to the key letter positions. These key value are used for both row and column position of the block to generate different text as cipher text than the previous techniques. This technique rearranges the plaintext at different letters rather than standard position of text. The following example shows the process of *diagonal transpositions* and *substitution* technique.

Plaintext: ABCDEFGHIJKLMNOP

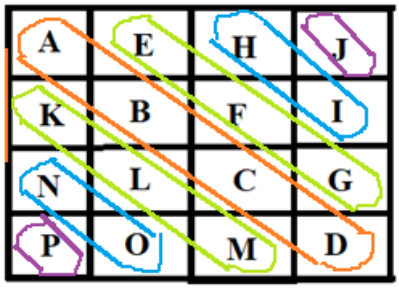


Figure 2: Block of Diagonal elements

Then implement the substitution technique using the key field 'CDBA'. The related numeric values of the key filed is 3421. Then the key values are used as column and row positions for implement the substitution technique to get different cipher text like the following.

	3	4	2	1
3	G	L	M	N
4	R	J	L	N
2	S	R	G	J
1	T	T	P	F

Figure 3: Block of Diagonal Cipher elements

The Java code which related to generate the transpositions and generate cipher text like the above is as follows.

```
void process(char in[][],char out[][],int ke[],int c)
{
// array in[][] represent input matrix
// array out[] represent output cipher text
// array ke[] have key values
// c is size of the diagonal matrix
        int i,j,t,g=0;
        for(i=0;i<c;i++)
        {
          for(j=0;j<c;j++)
          {
            t=((int)in[i][j]);
            if(t>64 && t <= 90)
            {
              if(t+ke[i]+ke[j]>90)
                t=((t+ke[i]+ke[j])-90)+64;
              else
                t=t+ke[i]+ke[j];
            }
            else if(t>96 && t <= 122)
            {
              if(t+ke[i]+ke[j]>122)
                  t=((t+ke[i]+ke[j])-122)+96;
              else
                  t=t+ke[i]+ke[j];
              }
              g=t;
              out[i][j]=(char)g;
          }
        }
}
```

Figure 4: Java Code to generate cipher text

Then implements the *Oscillation* technique to get the cipher text in a confused manner like the following.

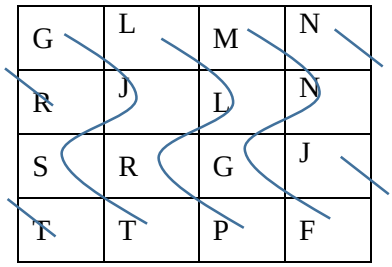


Figure 5: Implementation of Oscillation technique

Cipher text: NRJTMNGFGJSTLLRP

Here, the last column elements of the matrix oscillated with the next row element of the first column vice versa. The cipher text elements are arranged by getting them from column number positions because of oscillation technique is used.

This kind of cipher is very difficult to get plain text because of same letter (example the letter 'G' is generated for A and C, the letter 'J' is generated for B and G, letter 'L' is generated for E and F. Most of the time it generates duplicates that is depending upon the key which is given by us as key. So that this kind of cipher text is not easy to break by the cryptanalysts.

The Java program which is used to implement the above oscillation techniques to get a diffused text as a cipher text.

```
void oscillate (char in[][],char out[],int ke[],int c)
{
// array in[][] represent input matrix
// array out[] represent output cipher text
// array ke[] have key values
// c is size of the diagonal magtrix
int p=0,i,t;
int l=1,k=0;
while(l<=c)
{
  for(i=0;i<c;i++)
  {
        if(l==ke[i])
        {
          p=i;
          l++;
          break;
        }
  }//process of Oscillation
  for(i=0;i<c;i++)
  {
        t=p;
        if(i%2==0)
              out[k]=in[i][t];
        else
              if(t==c-1)
                    out[k]=in[i][0];
              else
                    out[k]=in[i][++t];
         k++;
   }
 }
}
```

Figure 6: Java code to implement Oscillation technique

VI. Conclusion

In this paper, we use the technique usually called as *diagonal transpositions*. Thru this technique, the matrix is automatically constructed for a maximum 65536 characters at a time and generate the key as an ASCII (usually thru the ASCII keyboards, its feature may support even Unicode) character positions for getting the cipher text. It also supports the space between the words. Here, we strongly believe that it would be a very interesting and fruitful area for future works.

VII. References

[1] Cryptography and Network Security principles and practice 5th Edition- William Stallings.

[2] IJARCSSE-"Study of Cryptography and its Techniques"-Ajit Singh, Madhu pahai, Annu malik, Volume 3, Issue 6, June 2013.

[3] http://www.google.com

[4] Robbi Rahim et al. "Data Security with International Data Encryption Algorithm".

[5] Isnar Sumartono et al. "An Overview of the RC4 Algorothm", IOSR Journal of Computer Engineering (IOSR-JCCE) e-ISSN : 2278,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. IV (Nov-Dec. 2016), PP 76-73, www.iosrjournals.org

.[6] Gowtham Tumati et al. "A New Encryption Algorithm Using Symmetric Key Cryptography", International Journal of Engineering & Technology,7 (2.32) (2018) 436-438.

[7] Isnar Sumartono and Andysah Putera Utama Siahaan, "Encryption of DES Algorithm in Information Security", International Journal for Innovative Research in Multidisciplinary Field, ISSN: 2455-0620 Valume – 4 , Issue – 10, Oct – 2018.

[8] http://en.wikipedia.org/wiki/Cryptography

[9] http://searchsecurity.techtarget.com/definition/private-key

[10] http://www.techopedia.com/definition/1773/decryption