A New Cryptosystem for Ciphers using Transposition Techniques

U. Thirupalu
Research Scholar
Dept. of Computer Science
S V U CM&CS – Tirupati
India – 517502

Dr. E. Kesavulu Reddy FCSRC (USA)
Assistant Professor,
Dept. of Computer Science
S V U CM&CS - Tirupati
India – 517502

***Abstract*:- Data Encryption techniques is used to avoid the unauthorized access original content of a data in communication between two parties, but the data can be recovered only through using a key known as decryption process. The objective of the encryption is to secure or save data from unauthorized access in term of inspecting or adapting the data. Encryption can be implemented occurs by using some substitute technique, shifting technique, or mathematical operations. By adapting these techniques we can generate a different form of that data which can be difficult to understand by any person. The original data is referred to as the plaintext and the encrypted data as the cipher text. Several symmetric key base algorithms have been developed in the past year. We proposed a new technique diagonal transposition with 256 bits different key values and generation of wave as in the form of cipher with variable length matrix to reduce the time complexity of simple column transposition techniques.**

Keywords:- Substitution Cipher, Transposition Cipher, Encryption, Decryption, Diagonal transposition technique.

1. INTRODUCTION

Cryptography is the art of achieve security by encoding messages to make them non-readable [1]. It is a technique which allow human-being to encrypt the data in such a way that the decryption can be performed without the aid of sender. Cryptography not only protects the information but also provides authentication to the user. As the network technology has been greatly advanced, there is a need to send much information via the Internet. Data can be read and understood without any special measures are called plaintext. Cryptography plays an important role insecure communication over the network and it provides a best solution to offer the necessary protection against the data intruders. Cryptography is the science of securing data. Cryptography is way of implanting mathematics to encrypt and decrypt data. Cryptography provides you to store sensitive information or transmit it across the insecure networks so that cannot be read by anyone except the intend recipient.

Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis [2][3]. During communication, the sender performs the encryption with the help of a shared secret key and the receiver performs the decryption. Cryptographic algorithms are broadly classified as Symmetric key cryptography and Asymmetric key cryptography.

A. *Symmetric Cryptography*

In the symmetric key encryption, same key is used for both encryption and decryption process. Symmetric algorithms more advantageous with low consuming with more computing power and it works with high speed in encrypt them. The symmetric key encryption takes place in two modes either as the block ciphers or as the stream ciphers. The block cipher mode provides, whole data is divided into number of blocks. This is based on the block length and the key is provided for encryption. In the case of the stream ciphers the data is divided as small as single bits and randomized then the encryption takes place. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems [3]. In this paper we examine only called classical encryption techniques. There are two building blocks of all encryption techniques.

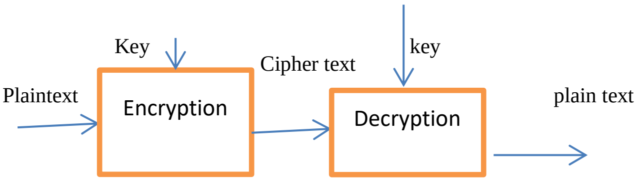


Figure 1. The encryption and decryption process of symmetric keys

B. *Asymmetric Key Encryption*

Asymmetric key algorithms use two keys, a public key (PBK) and a private key (PRK) for encryption and decryption as shown in Figure 2.. Each user have their own private key and public key. In this algorithm the sender (X) encrypt the plain text message (M) input into cipher text (C) by using the public key PBK of the receiver (Y), which is known to the parties involved in the transmission. At the receiver end the cipher text is converted back into the original plain text by applying the receiver’s private key (PRK) because the receiver’s private key and public key are related. So only the authorized person at the receiver end can decrypt the encrypted message. In public key algorithms key exchange is easier but encryption and decryption are complex and time consuming. Also public key algorithms are vulnerable against chosen plain text attack. The main examples of Public key algorithms are RSA, ECC and Diffie-Hellman key exchange algorithm.

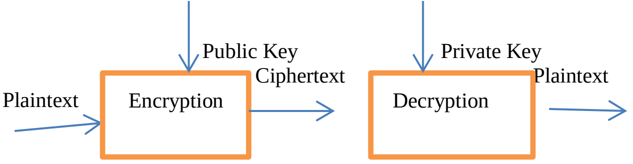


Figure 2. The encryption and decryption process of asymmetric keys.

II.TYPES OF ENCRYPTION TECHNIQUES

A. *Substitution Techniques*

This is one of the classical encryption technique which involve the substitution of a cipher text symbol for a plain text symbol [4].This method replaces the plain text bit patterns with cipher text bit patterns or plain text letters with other letters, numbers or symbols based on the key values. Examples of this method are Caesar cipher, Playfair cipher and Hill cipher.

B. *Transposition Techniques*

The process of mapping plain text letters to cipher text letters is achieved by performing some permutation on the original plain text letters [4]. This method can be made more secure by performing more than one transposition operation. Examples of transposition ciphers are Rail fence technique and columnar transposition.

III. STREAM CIPHERS

Stream ciphers perform encryption and decryption on stream of plain text and cipher text, usually one bit or byte at a time. Sometimes stream ciphers operate on one 32-bit word [5]. Stream ciphers are more suitable for real time applications such as multimedia. The examples of stream ciphers are A5 and RC4.

IV. BLOCK CIPHERS

Block ciphers perform encryption and decryption on blocks of plain text and cipher text, usually a block size of 64 bits. Sometimes block size is more than 64 bits [5]. Linear cryptanalysis is one of the widely used attacks on block ciphers. The examples of block ciphers are DES, AES and Blowfish.

A. *Mon Alphabetic Cipher*

This is one of the substitution techniques. This method map the plain text alphabet to cipher text alphabet, that is a single cipher alphabet is used per message [22]. Example of this method is DES.

B. *Polyalphabetic Cipher*

This method is also a substitution technique. This technique uses a set of related mono alphabetic substitution rules based on the key value and the key determines the rule chosen for a given transformation [12]. The examples of this method are Vigenere cipher and Vernam cipher.

V.RELATIVE WORK

A new approach to encrypt secret information based on the introducing concept of triangularization [6]. Since the encryption and decryption is done on a binary file by means of XOR operation it is effective on any type of data such as text or multimedia files. Modify the plain text to a cipher text using cryptography process [7].. Some Boolean algebraic operations are used. The cipher text is further suppressing the inside a cover media of image. Cryptanalysis and Steganalysis methods of recovering data at receiver side are also exposed. An algorithm is proposed for considering encryption as a critical security measure for protecting data privacy [8]. The entire process is achieved by considering binary data to cover all kinds of data in the field of Computer Science thus ensuring data security irrespective of what information is being transmitted. Focused primarily on the idea wherein the location of data is encrypted along with the data itself by means of a single Location Encryption Algorithm [9]. The security is further boosted using the Confirmation Code. Proposed a process of embedding to accomplish data hiding under the transformation (DWT and (IDWT) of cover image and to obtain privacy by using Huffman encoding [10].

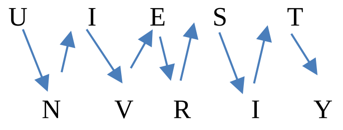
Introduced a technique where Caesar cipher and Rail Fence cipher technique are combined to eliminate their respective fundamental weaknesses, and produce a cipher text that is hard to crack [11]. When Caesar cipher substitution and Rail fence transposition techniques are used individually, cipher text obtained is easy to crack. This talk will present a perspective on combination of techniques substitution and transposition. Combining Caesar cipher with Rail fence technique can eliminate their fundamental weakness and produce a cipher text that is hard to crack.

VI. EXISTING SYSTEM

A. *Transposition techniques*

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 gets the cipher text. There are several techniques. They are:

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 gets the cipher like the following.



Plain text: UNIVERSITY

Cipher text: UIESTNVRIY

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,

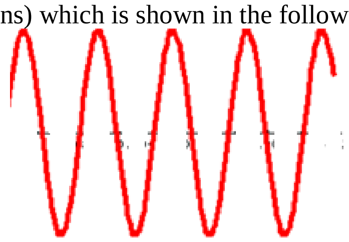
Key: 5 3 1 2 4
Palin text: C O M P U
T E R S C
I E N C E
Cipher text: MRNPSCOEEUCECTI

VII.PROPOSED WORK

We propose the Diagonal transposition technique for decrease the complexity of simple column transposition techniques. We arrange the plain text into diagonal position and assume the key. The matrix usually arranged as three levels of diagonal positions such as diagonal, upper triangular, lower triangular. These are arranging up to 65536 different characters at a time. The algorithm which is used to arrange the input string into diagonal is as follows.

A. Algorithm

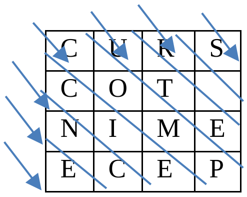
a) Write the plain text message in a diagonal form of variable length size (where as transposition technique or AES techniques use fixed length size of matrix).
b) Generate the key (any key usually any ASCII key). Read the message column by column in random order of columns by using the key positions with the help of wave technique (i.e. first column reads from top to bottom, second column
a) Reads from bottom to top like that it reads all columns) which is shown in the following diagram.



b) The message obtained by doing so is the cipher text.
c) Finally, we get plain text thru the cipher.

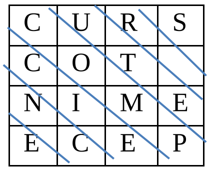
For example

Plain text: COMPUTER SCIENCE. The plain text “computer science” is arranged into diagonal position. Generally, these are diagonal, upper triangular, and lower triangular format. This kid of specification is as follows.



C	U	R	S
C	O	T	
N	I	M	E
E	C	E	P

Then write and generate the key for the above positions and generate the cipher text like the following.



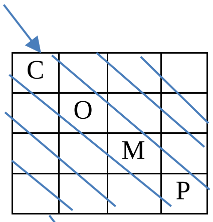
3	1	4	2
C	U	R	S
C	O	T	
N	I	M	E
E	C	E	P

Cipher text: UOICS EPCCNEREE
The Code which is used to *encrypt* the data is as follows:

```
Diagonal_Trans(int a[][], String s, int c)
{
  for(i=0;i<c;i++)
  {
           a[i][i]=s.charAt(k++);
   }
  for(i=1;i<c;i++)
  {
           for(j=i;j<c;j++)
           {
               a[j-i][j]=s.charAt(k++);
           }
   }
  for(i=1;i<c;i++)
  {
           for(j=i;j<c;j++)
           {
               a[j][j-i]=s.charAt(k++);
           }
   }
}
```

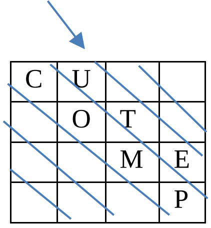
While executing the above code, the matrix is constructed as mentioned above is shown like the following step of procedures.

Step1:



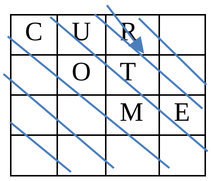
C			
	O		
		M	
			P

Step 2:



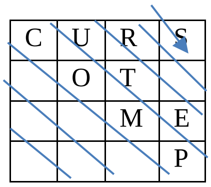
C	U		
	O	T	
		M	E
			P

Step 3:



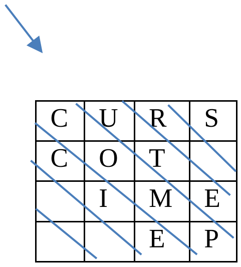
C	U	R	
	O	T	
		M	E

Step 4:



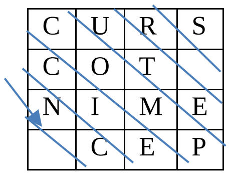
C	U	R	S
	O	T	
		M	E
			P

Step 5:



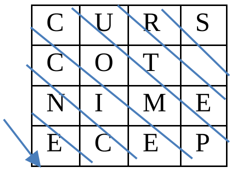
C	U	R	S
C	O	T	
	I	M	E
		E	P

Step 6:



C	U	R	S
C	O	T	
N	I	M	E
	C	E	P

Step 7:

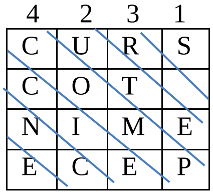


C	U	R	S
C	O	T	
N	I	M	E
E	C	E	P

Then read and generate the key by executing the following code:

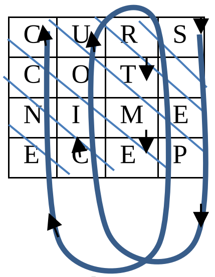
```
Read_Key()
{
  Key=readLine();
}
```

For example, if we read key like *time*, it converts and assumes the numeric column values for the matrix (according to ASCII values) like the following.



4	2	3	1
C	U	R	S
C	O	T	
N	I	M	E
E	C	E	P

Then implement the ware generation technique like the following to get the cipher text.



C	U	R	S
C	O	T	
N	I	M	E
E	C	E	P

The given code processes the cipher text using wave generation techniques.

```
Cipher_Text(String ct, ke[])
{
          int p=0;
          k=0;l=1;
          int x=0;
          while(l<=c)
          {
            for(i=0;i<c;i++)
            {
                    if(l==ke[i])
                    {
                      p=i;
                      l++;
                      break;
                    }
            }
            if(x==0)
            {       x=1;
                    for(i=0;i<c;i++)
                    {
                              ct+=a[i][p];
          }
            }
            else
            {
                    x=0;
                    for(i=c-1;i>=0;i--)
                    {
                              ct+=a[i][p];
          }
            }
          }
```

After execution of the above code, it generates and stores the cipher text in the variable ‘ct’. The cipher text for the above diagonal transposition technique is as follows.

Cipher text: S   EPCIOURTMEENCC

From the above cipher text, we get the plain text. For getting the plaintext, we use the same techniques that are wave technique and diagonal transpositions. The following code is used to get the plaintext form the above cipher text.

```
// -----Deciphering process--------------

k=0;
          l=1;x=0;
          while(l<=c)
          {
            for(i=0;i<c;i++)
            {
                    if(l==ke[i])
                    {
                      p=i;
                      l++;
                      break;
                    }
            }
```

```
  if(x==0)
  {       x=1;
          for(i=0;i<c;i++)
          {
                   b[i][p]=ct.charAt(k++);
}
  }
  else
  {
          x=0;
          for(i=c-1;i>=0;i--)
          {
                   b[i][p]=ct.charAt(k++);
}
  }
}
for(i=1;i<c;i++)
{
          for(j=i;j<c;j++)
          System.out.print(b[j][j-i]);
}
```

VIII.CONCLUSION

The proposed technique diagonal transpositions automatically construct the matrix with maximum 65536 characters at a time and generate the key as an ASCII code and to change the positions for generating the cipher text. It is also supports the space between the words but this feature is not designed in symmetric key systems.

AUTHOR'S PROFILE

1. U. Thirupalu

I am joining as a part-time research scholar in the department of computer science, Sri Venkateswara University College of CM&CS, Tirupati. I am pursuing PhD under the guidance of Dr.E.Kesavulu Reddy, Assistant Professor, in the department of Computer Science, S v U CM&CS, Tirupati.

2. Dr. E. Kesavulu Reddy

I am working as an Assistant Professor in the department of Computer Science, S V University College of CM&CS, Tirupati. I was recently received fellow of Computer Science Research Council from Global Journals, USA and also received Dr.Sarveypalli Radhakrishna life time Achievement Nation Award in 2018. My research interest is in the areas of Elliptic Curve Cryptography Network Security, Data mining and, Neural Networks,

REFERENCES

[1] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 1, No. 15, 2010.

[2] Sanket A. Ubhad, Prof. Nilesh Chaubey, Prof. Shyam P. DubeyASCII Based Cryptography Using Matrix Operation, Palindrome Range, Unique id International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 8, August 2015.

[3] Mohammad Shahnawaz Nasir, Prakash Kuppuswamy "Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm" International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 1, Issue 8, October 2013.

[4] Van Tilborg, HenkC. A.;Jajodia, Sushil, eds. Encyclopedia of Cryptography and Security. Springer.ISBN 978-1-4419-5905-8., p. 455, 2011.

[5] Anupam Mondal, Joy Samadder, Ivy Mondal, Neha Majumder, SudiptaSahana, Asymmetric Key based Secure Data Transfer Technique", International Conference on Computing, Communication and Sensor Network (CCSN) 2012.

[6] SudiptaSahana, Abhipsa Kundu, "Diagonal Block Steganography Based Enhanced Auxiliary Key Crypting for Secure Data Transfer", International Journal of Advanced Research in Computer Engineering & Technology(IJARCET) Volume 3 Issue 10, October 2014.

[7] MonalisaDey, Dhirendra Prasad Yadav, Sanik Kumar Mahata, Anupam Mondal, SudiptaSahana, "An Improved Approach of Cryptography using Triangulation andMSB Iteration Technique" Special Issue of International Journal of Computer Applications (0975 – 8887) International Conference on Computing, Communication and Sensor Network (CCSN) 2012.

[8] Soupayan Dutta, Soumya KantaDey, SudiptaSahana, "Implementation of Location Encryption Algorithm for Data Flow in Database Systems Ensuring Enhanced Security Management", International Journal of Innovations in Engineering and Technology(IJIET),Volume 6, Issue 4 April 2016, ISSN:2319-1058.

[9] A. Nag, S. Biswas, D. Sarkar, P. P.Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding," International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6),pp. 497-610,2011.

[10] Ajit Singh, Aarti Nandal, swati Malik, "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012, ISSN: 2277 128X.

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

[12] M. J. B.Robshaw, "Block Ciphers", Technical Report, RSA Laboratories, Number TR –601, July 1994.