Zigzag Ciphers: A Novel Transposition Method

Mu. Annalakshmi
Assistant Professor (Guest)
Department of Computer Science
Govt. Arts College for Women, Pudukkottai

A. Padmapriya, Ph.D
Assistant Professor
Dept. of Computer Science & Engineering
Alagappa University, Karaikudi

ABSTRACT
The requirement of information security has undergone changes in the last several decades. Network security measures are needed to protect data during their transmission. Cryptography is probably the most important aspect of communications security and is becoming increasingly important as a basic building block for computer security. This paper sets out to develop a hybrid way of encryption of plain text by combining rail fence cipher and columnar transposition cipher. This approach provides more security to information when compared with simple columnar transposition.

Keywords
Cryptography, Encryption, Rail fence cipher, Columnar Transposition

1. INTRODUCTION

Cryptograph***y*** [2] is an algorithmic process of converting a plain text (or clear text) message to a cipher text (or cipher) message based on an algorithm that both the sender and receiver know, so that the cipher text message can be returned to its original, plain text form. In its cipher form, a message cannot be read by anyone but the intended receiver. The act of converting a plain text message to its cipher text form is called enciphering. Reversing that act (i.e., cipher text form to plain text message) is deciphering. Enciphering and deciphering are more commonly referred to as encryption and decryption, respectively.

Cryptography [1] has remained important over the centuries, used mainly for military and diplomatic communication. Recently, with the advent of the internet and electronic commerce, cryptography has become vital for the functioning of the global economy, and is something that is used by millions of people on a daily basis. Sensitive information such as bank records, credit card reports, passwords, or private communication, is (and should be) encrypted – modified in such a way that, hopefully, it is only understandable to people who should be allowed to access it, and undecipherable to others. Symmetric cryptography [3] is also called as conventional or traditional cryptography. Here the encryption and decryption keys are the same. The encryption algorithm run in reverse serves as the decryption algorithm. Asymmetric cryptography is also called as public-key cryptography and it uses different keys for encryption and decryption. The decryption algorithm and key are kept secret. Anyone can encrypt the information, but only the authorized receiver can decrypt it. The decryption algorithm is designed in such a way that it is not the inverse of the encryption algorithm.

While using symmetric key cryptographic algorithms we can reduce the number of keys. In case of asymmetric key cryptography if there are ***n*** users we have to remember ***n*** number of public keys for encryption [4]. This paper proposes a new simple but novel transposition cipher method for better security than the existing transposition algorithms.

The paper is organized as follows. Section 2 provides an overview of some of the existing transposition algorithms. Section 3 introduces the proposed zigzag cipher transposition method. Section 4 elaborates the implementation of the zigzag cipher and discusses the results. Section 5 concludes the paper with some observations and remarks.

2. BACKGROUND STUDY

A transposition cipher [5] is the rearrangement of the letters in the plain text according to some specific system and key. They do not change the letters in the plaintext or even cover up frequencies, but they can be built upon to make more secure methods of encryption. Mathematically, a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

2.1 Rail Fence Cipher

The Rail Fence cipher [6] is a form of transposition cipher that gets its name from the way in which it is encoded. In the rail fence cipher, the plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom. The message is then read off in rows. For example, using three "rails" and a message of 'WE ARE DISCOVERED. FLEE AT ONCE', the cipherer writes out:

W . . . E . . . C . . . R . . . L . . . T . . . .. E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .

Then reads off:

WECRL TEERD SOEEF EAOCA IVDEN

2.2 Route cipher

In a route cipher, the plaintext is first written out in a grid of given dimensions, and then read off in a pattern given in the key.

W R I O R F E O E
E E S V E L A N J
A D C E D E T C X

The key might specify "spiral inwards, clockwise, starting from the top right". That would give a cipher text of:

EJXCTEDECDAEWRIORFEONALEVSE

2.3 Columnar transposition

In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the word ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose the keyword used is ZEBRAS and the message is WE ARE DISCOVERED FLEE AT ONCE. In a regular columnar transposition, this is written into the grid as follows:

```
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E Q K J E U
```

Providing five nulls (QKJEU) at the end. The cipher text is then read off as:

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

In the irregular case, the columns are not completed by nulls:

```
6 3 2 4 1 5
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E
```

This results in the following cipher text:

EVLNA CDTES EAROF ODEEC WIREE

To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length, then write the message out in columns again, then re-order the columns by reforming the key word.

3. ZIGZAG TRANSPOSITION CIPHER METHOD

When rail fence cipher or columnar transposition is applied individually, it is easier to cryptanalyze. The proposed zigzag transposition combines rail fence cipher and columnar transposition to generate a cipher text which is more difficult to cryptanalyze. Zigzag transposition may be done in row wise or column wise manner.

Here the plain text is arranged in a matrix format.

If the zigzag transposition is done row wise, then the message is read in zigzag fashion based on the digits in the key. If the digit in the key is i, then message is read in the following order of matrix positions.

(i , 1) (i+1, 2) (i , 3) (i+1 , 4) (i , 5)

If the same transposition is done column wise, then the message is read as

(1, i) (2, i+1) (3 , i) (4 , i+1) (5 , i)

Since transposition comes under the category of symmetric ciphers, the same key is used for decryption. If the jth digit in the key is i , then the jth row of cipher text is arranged as (i , 1) (i+1, 2) (i , 3) (i+1 , 4) (i , 5).

3.1 Process of Encryption

Consider the following example.

Plaintext : ZIGZAGCOLUMNTRANSPOSITION

Key : 4 2 5 3 1

Arrange the plain text in matrix format.

	1	2	3	4	5
1	Z	I	G	Z	A
2	G	C	O	L	U
3	M	N	T	R	A
4	N	S	P	O	S
5	I	T	I	O	N

The first digit in the key is 4. In case of row zigzag transposition, characters in the matrix positions (4 , 1) (5 , 2) (4 , 3) (5 , 4) (4 , 5) are read. These characters (N T P O S) form the first row of cipher text matrix.

Plain Text Matrix Cipher Text Matrix

	1	2	3	4	5					
1	Z	I	G	Z	A	N	T	P	O	S
2	G	C	O	L	U					
3	M	N	T	R	A					
4	N	S	P	O	S					
5	I	T	I	O	N					

Similarly, the remaining digits in the key are also processed in the same order to get the cipher text matrix.

Plain Text Matrix Cipher Text Matrix

	1	2	3	4	5					
1	Z	I	G	Z	A	N	T	P	O	S
2	G	C	O	L	U	G	N	O	R	U
3	M	N	T	R	A					
4	N	S	P	O	S					
5	I	T	I	O	N					

When the digit in the key is 5, then the message is read in the order (5,1) (1 ,2) (5,3) (1,4) (5,5)

Plain Text Matrix Cipher Text Matrix

	1	2	3	4	5					
1	Z	**I**	G	**Z**	A	N	T	P	O	S
2	G	C	O	L	U	G	N	O	R	U
3	M	N	T	R	A	I	I	I	Z	N
4	N	S	P	O	S					
5	**I**	T	**I**	O	**N**					

Plain Text Matrix Cipher Text Matrix

	1	2	3	4	5					
1	Z	**I**	G	**Z**	A	N	T	P	O	S
2	G	C	O	L	U	G	N	O	R	U
3	M	N	T	R	A	I	I	I	Z	N
4	N	S	P	O	S	M	S	T	O	A
5	**I**	T	**I**	O	**N**					

Plain Text Matrix Cipher Text Matrix

	1	2	3	4	5					
1	Z	**I**	G	**Z**	A	N	T	P	O	S
2	G	C	O	L	U	G	N	O	R	U
3	M	N	T	R	A	I	I	I	Z	N
4	N	S	P	O	S	M	S	T	O	A
5	**I**	T	**I**	O	**N**	Z	C	G	L	A

The Cipher text generated is NTPOSGNORUIIIZNMSTOAZCGLA.

3.2 Process of Decryption

Since transposition comes under the category of symmetric ciphers, the same key 4 2 5 3 1 is used for decryption. Again the cipher text is arranged in matrix format.

Cipher Text Matrix

	1	2	3	4	5
1	N	T	P	O	S
2	G	N	O	R	U
3	I	I	I	Z	N
4	M	S	T	O	A
5	Z	C	G	L	A

The first digit in the key is 4. Now the first row in the cipher text matrix N T P O S are arranged in positions (4 , 1) (5 , 2) (4 , 3) (5 , 4) (4 , 5)

Cipher Text Matrix Decrypted Matrix

	1	2	3	4	5		1	2	3	4	5
1	N	T	P	O	S						
2	G	N	O	R	U						
3	I	I	I	Z	N						
4	M	S	T	O	A		N		P		S
5	Z	C	G	L	A			T		O	

The same process is repeated for the remaining digits of the key and the following matrix is generated.

Cipher Text Matrix Decrypted Matrix

	1	2	3	4	5	1	2	3	4	5
1	N	T	P	O	S	Z	I	G	Z	A
2	G	N	O	R	U	G	C	O	L	U
3	I	I	I	Z	N	M	N	T	R	A
4	M	S	T	O	A	N	S	P	O	S
5	Z	C	G	L	A	I	T	I	O	N

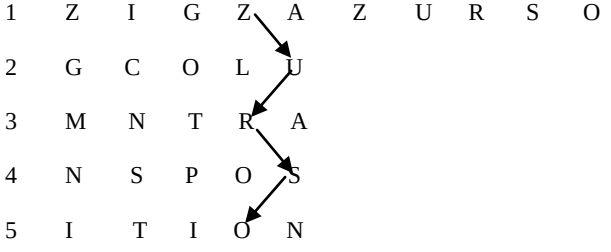
Now the decrypted text produced is ZIGZAGCOLUMNTRANSPOSITION.

The same example can be processed with column zigzag transposition.

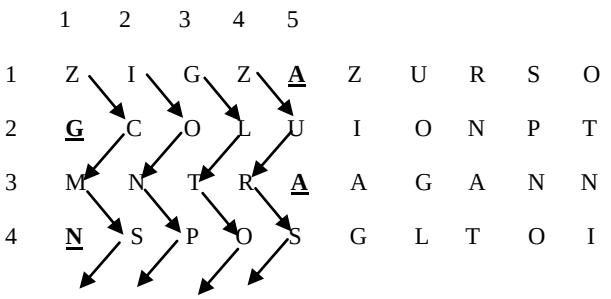
Plain Text Matrix

	1	2	3	4	5
1	Z	I	G	Z	A
2	G	C	O	L	U
3	M	N	T	R	A
4	N	S	P	O	S
5	I	T	I	O	N

Plain Text Matrix Cipher Text Matrix



Plain Text Matrix Cipher Text Matrix



5 I T I O **N** Z C M S I

The cipher text generated is ZURSOIONPTAGANNGLTOIZCMSI. The decryption is done with the same key as follows.

Cipher Text Matrix

	1	2	3	4	5
1	Z	U	R	S	O
2	I	O	N	P	T
3	A	G	A	N	N
4	G	L	T	O	I
5	Z	C	M	S	I

The first digit in the key is 4. Now the first row in the cipher text matrix Z U R S O are arranged in positions (1 , 4) (2 , 5) (3 , 4) (4 , 5) (5 , 4)

Cipher Text Matrix Decrypted Matrix

	1	2	3	4	5	1	2	3	4	5
1	Z	U	R	S	N				Z	
2	I	O	N	P	T					U
3	A	G	A	N	N				R	
4	G	L	T	O	I					S
5	Z	C	M	S	I				O	

The number of digits in the key for zigzag transposition depends on the number of rows, in case of row wise transposition and on the number of columns, in case of column wise zigzag transposition.

The same approach can be applied more than once to produce cipher text with more security.

4. EXPERIMENTAL STUDY

The proposed zigzag method offers better security because of the complexity of transposition being employed. The proposed method is implemented using vb.net. Since the block is formed as a 7 x 7 matrix, the proposed method uses a 7 digit key value for the implementation. The proposed symmetric key transposition algorithm overcomes the drawback of remembering n number of public keys in asymmetric key cryptographic algorithm. The sample output screen is shown below.

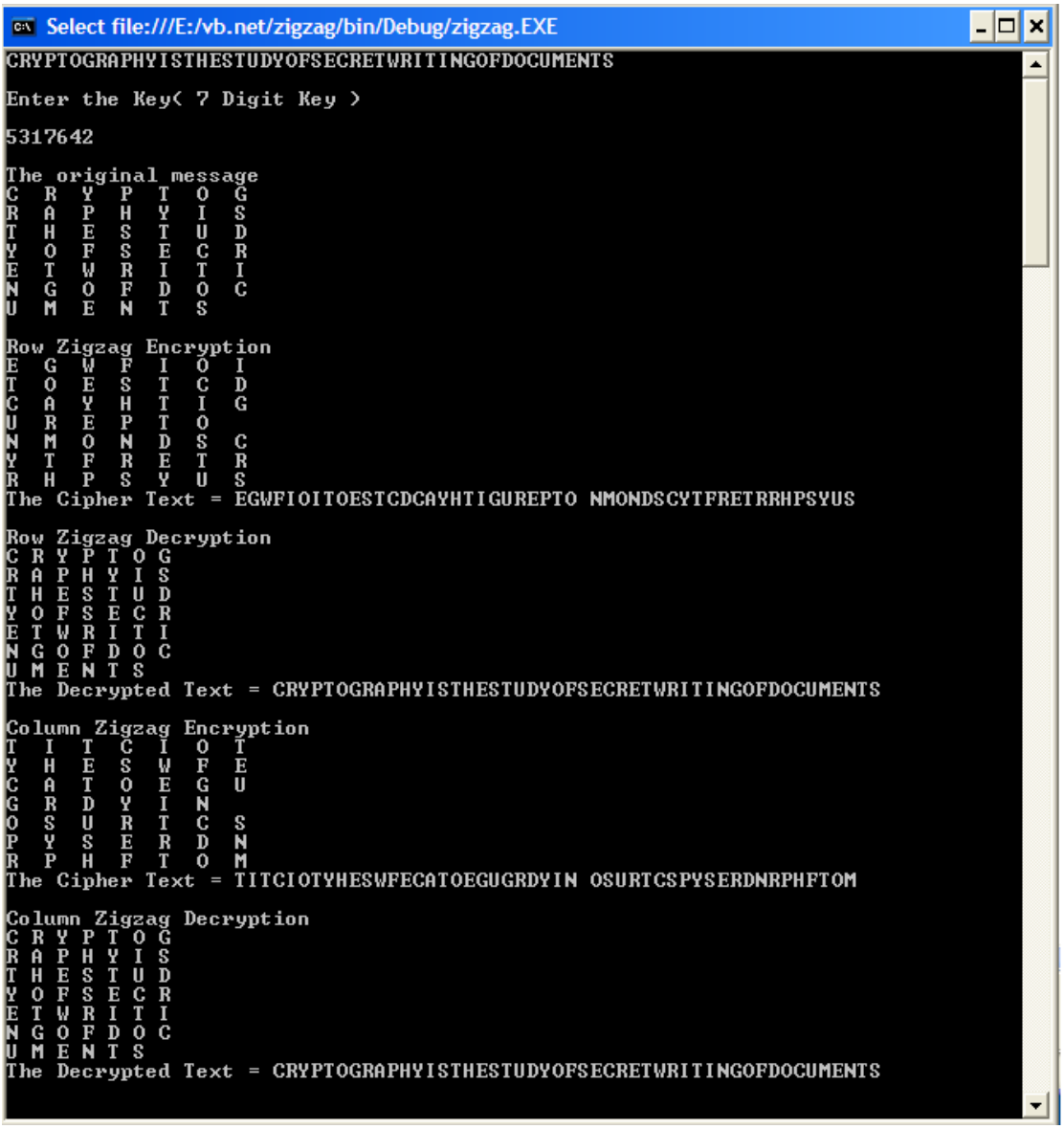


Fig 1: Encryption and Decryption process

5. CONCLUSION

The zigzag transposition approach can be applied more than once to produce cipher text with more security. Transposition can also be combined with other techniques such as substitution to generate ciphers which are more difficult to crack. If future this can be further extended for multi level encryption to offer improved security.

6. REFERENCES

[1] Atul Kahate, "Cryptography and Network Security", Tata Mc-Graw Hill, 2003.

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

[3] Quist-Aphetsi Kester, "A Hybrid Cryptosystem based on Vigenere Cipher an Columnar Transposition Cipher" , International Journal of Advanced Technology and Engineering Research (2250-3536), Volume 3, Issue 1, Jan 2013.

[4] S.D. Padiya, D.N.Dakhane, "Plaintext Based Transposition Method", International Journal of Advanced Research and Software Engineering (2277 128X), Volume 2, Issue 7, July 2012.

[5] "Transposition method for cryptography" by Satish Bansal and Rajesh Shrivastava, The IUP Journal of Computer Sciences, Vol. V, No. 4, 2011.

[6] Rail Fence Cipher, Route Cipher, Columnar Transposition Cipher retrieved from http://en.wikipedia.org/Transposition