American Journal of Computation, Communication and Control
2015; 2(2): 7-11
Published online March 20, 2015 (http://www.aascit.org/journal/ajccc)
ISSN: 2375-3943

Keywords
Information Security,
Message Splitting,
Pattern,
Sequence

Received: January 4, 2015
Revised: March 6, 2015
Accepted: March 7, 2015

Pattern in Splitting Sequence in Okike's Merged Irregular Transposition Cipher for Encrypting Cyberspace Messages

Okike Benjamin[1], Garba EJD[2]

[1]Department of Computer, Science, University of Ghana, Legon, Accra
[2]Department of Mathematical Sciences, University of Jos, Jos, Nigeria

Email address
okikeb@yahoo.com (O. Benjamin)

Citation
Okike Benjamin, Garba EJD. Pattern in Splitting Sequence in Okike's Merged Irregular Transposition Cipher for Encrypting Cyberspace Messages. *American Journal of Computation, Communication and Control*. Vol. 2, No. 2, 2015, pp. 7-11.

Abstract
The protection of sensitive information against unauthorized access or fraudulent changes has been of prime concern throughout the centuries. Modern communication techniques using computers connected through networks make all data even more vulnerable to these threats. The researchers in this work propose a new encryption technique to be known as Okike's Merged Irregular Transposition Cipher. In this proposed encryption technique, a message to be encrypted will first of all be split into multiple parts depending on the length of the message. After the split, different keywords are chosen to encrypt different parts of the message. After encrypting all parts of the message, the positions of the encrypted message could be swapped to other positions thereby making it very difficult to decrypt by any unauthorized user. The researchers intend to show the pattern of splitting sequence as the message deployed is split from 2 through 10. The result show that as the number of splits, S increase from 2 through 10, the number of swap positions, Z increase by factorial of S (S = Z!). The swapping of the positions of the encrypted message would further increase the complexity with which an adversary may take the decrypt such a message.

1. Introduction

In clear terms, a "transposition" is the simple changing of positions of two symbols within a message. A sequence of such exchanges can form any possible mathematical "permutation" of the original message. In other words, it is the simple re-arrangement of the existing data symbols [1]. The techniques employed to this end have become increasingly mathematical in nature. Although Transposition Cipher may take many forms, this research concentrates on three main areas: First, the Single Columnar Transposition, the Double Columnar Transposition Ciphers and the Irregular Transposition Cipher cryptosystems. The Irregular Transposition cipher makes it possible to protect information in a more reliable form than both the Single Columnar and the Double Columnar Transposition Ciphers. Its security is based on the arrangement of the information in an irregular table rather than a block. In this research work, the researchers intend to propose a Merged Irregular Transposition Cipher to encrypt information. This cipher will certainly offer more secured information than the other forms of transposition ciphers that already exist since multiple irregular tables and multiple keywords are employed to encrypt the information.

In the past several decades cryptography has become an indispensable tool for

constructing secure electronic banking systems, Internet-based commerce, and secure mobile telephony [2].

2. Literature Review

This section will review some existing literatures in relation to information security. The researchers have chosen to review the works on transposition ciphers during the course of this work.

Most real-world encryption is based on block, which transform fixed-sized inputs into fixed-sized outputs. In a block cipher the message is broken into blocks, each of which is then encrypted (ie like a substitution on very big characters - 64-bits or more) [3].

A. Transposition Cipher

After looking at ciphers like the Substitution Cipher, which can replace the letters of one's message by completely different letters, a cipher that cannot change any letters at all seems weak. However, this is not the case with transposition cipher. There is no doubt that the letters in the message are not replaced by some other letters, but the reordering of the ciphertext makes transposition cipher a very strong and powerful cipher technique. Transposition ciphers can be secure in themselves, and as well, transposition methods are useful to know, since they can sometimes be mixed with substitution methods for a more secure cipher.

The approach adopted here is very straight forward. The plaintext is written (without spaces) in a grid containing a certain number of columns. The cipher is read off in columns [4].

B. Single Columnar Transposition Cipher

One of the easiest ways to achieve transposition cipher is by the use of a Single Columnar Transposition Cipher. To use it, one may need a keyword or phrase, whose letters are numbered according to their presence in the English alphabet.

Usually when employing a transposition cipher, one adds dummy letters to ensure that all the spaces in the table formed are filled up. It is important to do this before transposing the letters; otherwise the receiver may not calculate the columns that do not have a full number of letters if the last row is not complete. In some cases the last row is always made complete by adding dummy letters, but that reduces the security of the cipher and is not recommended since that may render the cipher quite easy to break [5].

C. Double Columnar Transposition Cipher

Double Columnar transposition ciphers are very similar to Single Columnar Transposition ciphers but are more complex in their design and are harder to decipher. It is similar to single columnar transposition, but the process is repeated twice. One either uses the same keyword both times or, preferably, a different one on the second occasion.

Double columnar transposition is substantially safer against cryptanalysis than single columnar transposition. To decipher any information encrypted using the above method, one needs to know how many letters are in the keyword and what order to arrange the columns for rewriting the enciphered letters into the matrix. To make it even harder, one may want to try other patterns of enciphering information using the Double Columnar Transposition Cipher with a keyword [6]. It may be possible to use the spiral, go right to left from bottom corner to the upper left corner or even zig zag up and down through different columns or rows.

Despite the fact that the Double Columnar Transposition Cipher is safer in securing information than the Single Columnar Transposition Cipher, it is also weak in the sense that the number of letters in a given row is almost constant apart from the last row, it then means that cryptanalysts can explore this weakness in order to decipher information encrypted using this method.

D. Irregular Transposition Cipher

As a result of the weakness observed in the previous transposition methods already reviewed in which the text being transposed is split into nearly regular divisions of almost equal length, even the Double Columnar transposition can be broken without recourse to multiple anagramming. In its simplest form, anagramming is a word, phrase, or sentence formed from another by rearranging its letters. The applications of several messages of the same length, enciphered using the same key, to recover the transposition by matching together columns of letters that form reasonable letter pairs.

Indeed, all a cryptanalyst needs to do is write the ciphertext information into different size grids - eventually the plaintext will emerge. To combat this weakness, one can employ Irregular Transposition Cipher, otherwise known as Geometrical Transposition Cipher. A geometrical transposition cipher is one which employs the use of keyword as was seen in both the Single Columnar and Double Columnar Transposition Ciphers. But unlike in the case of the Single Columnar or the Double Columnar Transposition Ciphers in which both have almost a fixed number of letters in a row or column, the Geometrical Transposition Cipher becomes less crude when the order in which the columns or rows are taken off is not fixed. Normally, a keyword is employed to specify the removal order [4]. Also, unlike the Single Columnar Transposition and the Double Columnar Transposition ciphers considered earlier, both of which have almost fixed number of letters in the rows except in some cases the last row, the Irregular Columnar Transposition Cipher has varied number of letters in its columns or rows. The number of letters in a given row or column is determined by the column or row number and the corresponding ordinal value.

3. Okike's Merged Irregular Transposition Cipher

The researchers have in this work reviewed the Single Columnar Transposition Cipher, the Double Columnar Transposition Cipher and the Irregular Transposition Cipher, otherwise known as Geometrical Transposition Cipher.

Despite the fact that the Irregular type of transposition cipher offers a better security than all other transposition ciphers considered earlier, there may be an improvement in the security if the message to be encrypted is split into multiple parts and encrypted separately. At the end, the encrypted parts will be combined together for the ciphertext information to be sent across through the Internet. The positions of the splits may be swapped to improve on the security of the encrypted information.

To improve on the Irregular Transposition Cipher, the researchers intend to develop a new type of cipher to be known as Okike's Merged Irregular Transposition Cipher. Unlike the Irregular Transposition Cipher already in existence, the Merged Irregular Transposition Cipher will utilize multiple tables and keywords to encrypt information. The first step toward the application of this model will be to divide the entire message into multiple equal or nearly equal parts. The number of parts may be determined by the length of the message to be encrypted. In this research work, the message to be encrypted will only be divided into ten parts for the sake of illustration and analysis carried on the behavior of each of the part in relation to the overall behavior of the cipher.

A. Structure of Merged Irregular Cipher

The structure of the table is depicted in table 1 below:

Table 1. *Keyword Written Against Column*

COL	**1**	**2**	**3**	**----------m**			
K/W	K	E	Y	W	O	R	D
O/V							
ROW							
1							
2							
3							
-							
-							
-							
n							

From the table above, there are n rows and m columns. In table 1, the keyword is written against the columns. There would not be much difference if the keywords are written against the rows

To illustrate how Okike's Merged Irregular Transposition Cipher works, assuming the information below originates from Anambra State Government House, Awka few days before the political impasse that engulfed the state took place:

ATTENTION: POLICE BOSS – HOODLUMS PLAN MAYHEM ON ANAMBRA RESIDENTS

To encipher the above information using the Merged Irregular Transposition Cipher, the following steps are involved:

1. Choose keywords to use, The number of keywords should depend on the length of the message.
2. Split the original message into multiple equal or nearly equal parts.
3. Encrypt each part of the split message using any of the keyword.
4. Combine the multiple encrypted messages into a single message.

Before encrypting the above message, there may be a need to define the variables to be used.

A. Definition of Variables

i. Column, m is the number of columns contained in a table (matrix).
ii. Row, n is the number of rows in a table.
iii. Length of message, L is the total number of characters in the message to be encrypted for each split number, S.
iv. Message Split number, S is the number of parts the entire message is split into.
v. Swap Number, Z is the total number of positions that an encrypted message can be exchanged for each split, S.

At this point, an example may be used to illustrate how the Merged Irregular Transposition Cipher may be applied. The entire message, L to be encrypted may be split into a given number of parts, S, where S >=2.

$$S=2$$

Using UNIVERSE as a keyword and encrypting the first part of the message "ATTENTION: POLICE BOSS – HOODLUMS" is shown in table 2 below:

Table 2. *Using Universe as a Keyword and Encrypting the First Part of the Message*

COL	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
K/W	U	N	I	V	E	R	S	E
O/V	7	4	3	8	1	5	6	2
ROW								
1	A	T	T	E	N			
2	T	I	O	N	:	P	O	L
3	I	C	E					
4	B	O						
5	S	S	–	H	O	O		
6	D	L	U	M	S	X	X	

This will produce the ciphertext below:

N:OS L TOE-L TICOSL POX OX ATIBSD ENHM

Using SCIENCES as a keyword and encrypting the second part of the message" PLAN MAYHEM ON ANAMBRA RESIDENTS." Is shown in table 3 below:

Table 3. *Using Sciences as a Keyword and Encrypting the Second Part of the Message*

COL	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
K/W	S	C	I	E	N	C	E	S
O/V	7	1	5	3	6	2	4	8
ROW								
1	P	L						
2	A	N	M	A	Y	H		
3	E	M	O	N				
4	A	N	A	M	B	R	A	
5	R	E	S					
6	I	D	E	N	T			
7	S							
8	.	X	X	X	X	X	X	X

This in turn will produce the ciphertext below:

LNMNEDXHRX ANMNX AX MOASEX YBTX PEAARIS. X

Combining the two different ciphertexts for the first and the second messages shows the ciphertext below:

N:OS L TOE-L TICOSL POX OX ATIBSD ENHM LNMNEDXHRX ANMNX AX MOASEX YBTX PEAARIS. X

At this point, the positions of the ciphertext information may be swapped, Since S=2, the first could take the second position and the second take the first position thereby increasing the complexity of the encryption algorithm.

Using appropriate keywords and splitting the same message into 3, 4, ……., 10 produced the values of S and Z presented in table 4 below:

Table 4. *Values of S and Z for S=1, 2, ……,10*

No. of Split(S)	Possible Swap Position per Split (Z)
2	2
3	6
4	24
5	120
6	720
7	5040
8	40320
9	362880
10	3628800

From table 4 above, it would be observed that as the number of spit, S increases, the number of swap positions, Z also increases, thereby increasing the level of complexity that may be required for a cryptanalyst to decrypt a given message.

Graphically, figure 1 below shows the relationship between S and Z as S increases from 2 through 10.

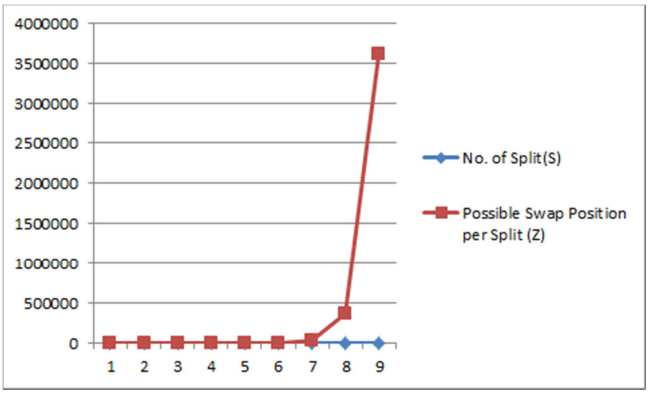

Fig. 1. *S and Z relationship S=2 through 10*

B. Pattern in Splitting Sequence

According to [7], the pattern in splitting sequence can be examined in terms of number of swap positions, Z as the number of split, S increases from 2. The first time the message to be encrypted is split into two parts (i.e. S=2), there are two possible swap positions, Z. The first encrypted message may either be placed at the first or second position before sending the encrypted message to the recipient. Below is shown ways in which the encrypted message can be positioned before sending it out for S=2,3 and 4 to establish a splitting sequence pattern. This is shown in figure 2 below:

From figure 2, it could be observed that the number of swap positions, Z of message is equal to the factorial of number of splits, S of that same message. Mathematically, it can be shown that:

$$Z = S!$$

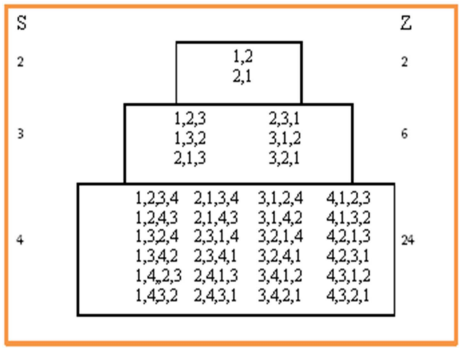

Fig. 2. *Values of S = 2, 3 and 4 and their possible swap positions*

From figure 1 above, it could be observed that the number of swap positions, Z of message is equal to the factorial of number of splits, S of that same message. Mathematically, it can be shown that:

$$Z = S!$$

4. Strengths of Okike's Merged Irregular Transposition and Dynamic Transposition Ciphers

If the same message that was deployed to illustrate how Okike;s Merged Irregular Transposition Cipher work is applied using the Dynamic Transposition Cipher, also known as the Irregular Transposition Cipher, it would take a cryptanalyst S! more efforts/time to decrypt the message, where S is the number of splits of the message.

5. Conclusion

In conclusion, it was observed that Okike's Merged Irregular Transposition Cipher will offer more secured information when compared to the Irregular Transposition Cipher used as a base. It is good to note that among most of existing transposition ciphers, the Irregular Transposition cipher is the most difficult transposition cipher that may be broken by cryptanalyst before now. As the split number, S increases, then the security level of complexity also increases since the positions of information encrypted may be swapped with one another before sending the message across

References

[1] R. Terry, "Dynamic Transposition Revisited", 2001. Retrieved from http://www.ciphersbyritter.com

[2] M. Green, "Practical Cryptographic Systems", 2010, Retrieved from http://spar.isi.jhu.edu/

[3] W. Stallings, "Modern Private Key Ciphers", 1996, Retrieved from http://williamstallings.com

[4] S. John, "Method of Transposition", 2001, Retrieved from<http://home.ecn.ab.ca/~/savard/

[5] N. Randy, "Classical Cryptography". 1996, Retrieved from http://www.und.nodak.edu/crypto/

[6] A. Torbjorn, "Double Columnar Transposition", 1998, Retrieved from http://www.cvni.net/radio/nsnl/>

[7] B. Okike, "Some New Encryption Techniques Using Firewalls and Random Number Generators" Being Ph. D. Thesis Defence Presented at ATBU, Bauchi, Nigeria, 2005.