American Journal of Computation, Communication and Control
2014; 1(4): 61-65
Published online October 10, 2014 (http://www.aascit.org/journal/ajccc)

AASCIT American Association for Science and Technology

Keywords
Transposition Cipher,
Merged Irregular Cipher,
Encryption,
Complexity Level

Received: September 27, 2014
Revised: October 07, 2014
Accepted: October 08, 2014

Determination of complexity level in Okike's merged irregular transposition cipher

Okike Benjamin, Garba E. J. D.

Department of Computer Science, University of Ghana, Legon and University of Jos, Nigeria

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

Citation
Okike Benjamin, Garba E. J. D.. Determination of Complexity Level in Okike's Merged Irregular Transposition Cipher. *American Journal of Computation, Communication and Control*. Vol. 1, No. 4, 2014, pp. 61-65.

Abstract
Today, it has been observed that security of information along the superhighway is often compromised by those who are not authorized to have access to such information. In other to ensure the security of information along the superhighway, such information should be encrypted by some means to conceal the real meaning of the information. There are many encryption techniques out there in the market. However, some of these encryption techniques are often decrypted by adversaries with ease. The researchers have decided to develop a new encryption technique that may be more difficult to decrypt. This may be achieved by splitting the message to be encrypted into parts and encrypting each part separately and swapping the positions before transmitting the message along the superhighway. The method is termed Okike's Merged Irregular Transposition Cipher. Also, the research would determine the complexity level in respect to the number of splits of the message.

1. Introduction

Specifically, a "transposition" is the simple exchange in position of two symbols within a message or ordered array or vector. A sequence of such exchanges can form any possible mathematical "permutation" of the message. In other words, it is the simple re-arrangement of the existing data symbols, Terry (2001). 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 and the Double Columnar Transposition Ciphers are discussed. These systems have extremely fast implementations, but may or may not involve the use of keywords. Second, the researcher presents an Irregular Transposition Cipher cryptosystems, which 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 deploy a Merged Irregular Transposition Cipher to encrypt information. This cipher will certainly offer more secured information than the other forms of transposition ciphers that are already in existence since multiple irregular tables and multiple keywords are employed to secure the information.

2. 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 alphabet. In the Single Columnar Transposition Cipher, the letters of the plaintext are copied down by reading them off column-wise in the order stated by the enumeration of the keyword, Harry (2004).

3. Double Columnar Transposition Cipher

Double Columnar Transposition Cipher uses the actual letters of the message to be enciphered, simple letter-equivalents being substituted for figures and punctuation before enciphering begun. The order of the letters is then changed in a complex manner, according to a definite plan, by the encipherer and restored in due course, using the same plan, to its original form by the decipherer (Rutter, 2012).

4. Irregular Transposition Cipher

Geometrical Transposition Cipher becomes less crude when the order in which the columns or rows are taken off is not fixed. Normally, keywords are employed to specify the removal order, Luigi (2000). 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

5. Okike's Merged Irregular Transposition Cipher

The researchers having reviewed the Single Columnar Transposition Cipher, the Double Columnar Transposition Cipher and the Irregular Transposition Cipher, otherwise known as Geometrical Transposition Cipher, now proposes Okike's Merged Irregular 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 is split into multiple parts and each part encrypted separately. At the end, the encrypted parts will be combined together for the ciphertext information to be sent over the Internet to recipient(s). The positions of the splits may be swapped to improve on the security of the encrypted information.

According to Okike (2012), unlike the Irregular Transposition Cipher already in existence, Okike's 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. Analysis will be carried on the behavior of each of the part in relation to the overall behavior of the cipher.

5.1. Structure of Okike's Merged Irregular Cipher

The structure of the table is depicted in table 5.1 below:

Table 5.1. *Keyword written against Column*

Col	1	2	3	4	----------		m
K/W	k	e	y	w	o	r	d
O/V	3	2	7	6	4	5	1
Row							
1							
2							
3							
:							
:							
:							
n							

From the table above, there are n rows and m columns. In table 5.1, the keyword is written against the columns. There would not be much difference if the keyword is 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 in 2004:

Attention: police boss – hoodlums plan mayhem on anambra residents.

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

i. Choose keywords to use. The number of keywords at a given point in time should depend on the length of the message.
ii. Split the original message into multiple equal or nearly equal parts.
iii. Encrypt each part of the split message using any of the keywords.
iv. 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.

5.2. 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. Message Characters, C is the individual characters in a message.
vi. Available spaces, A refers to the number of spaces in a table that may contain any message character, C.
vii. Empty character, X is used to fill up empty spaces when all the message characters, C have been entered and yet the ordinal value corresponding to the row has not yet been reached.
viii. Empty Space, B is the number of space(s) in the table that either contains no message characters, C or empty character, X
ix. Non-empty space, Q is the number of space(s) that either contains a message character, C or empty character, X in a table.
x. 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 Okike's 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"

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."

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 will produce the ciphertext below:

LNMNEDX HRX ANMNX AX MOASEX YBTX PEAARIS. X

which will produce the combined ciphertext below:

N:OS L TOE-L TICOSL POX OX ATIBSD ENHM LNMNEDX HRX 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 could take the first position thereby increasing the complexity of the encryption algorithm.

S= 3

ATTENTION: POLICE BOS 19
S - HOODLUMS PLAN MAYHE 19
M ON ANAMBRA RESIDENTS. 20

Using the keyword FORSEE, the first part of the message "ATTENTION: POLICE BOS"

Col	1	2	3	4	5	6
K/W	F	O	R	S	E	E
O/V	3	4	5	6	1	2
Row						
1	A	T	T	E	N	
2	T	I	O	N	:	P
3	O					
4	L	I				
5	C	E	B			
6	O	S	X	X		

This will yield the ciphertext below:

N: P ATOLCO TIIES TOBX ENX

Using the keyword VISION to encrypt the second part of the message "S - HOODLUMS PLAN MAYHE"

Col	1	2	3	4	5	6
K/W	V	I	S	I	O	N
O/V	6	1	5	2	4	3
Row						
1	S	–				
2	H	O	O	D		
3	L	U	M	S	P	L
4	A	N	M	A	Y	
5	H	E	X			

This will produce the ciphertext message below:

-OUNE DSA L PY OMMX SHLAH .

The keyword TONGUE when applied to encrypt the third part of the message "M ON ANAMBRA RESIDENTS."

Col	1	2	3	4	5	6
K/W	T	O	N	G	U	E
O/V	5	4	3	2	6	1
Row						
1	M	O	N	A	N	A
2	M	B	R	A		
3	R	E	S			
4	I	D				
5	E					
6	N	T	S	.	X	X

This produces the ciphertext message shown below:

AX AA NRSS OBEDT MMRIEN NX

which will produce the combined ciphertext below:

N: P ATOLCO TIIES TOBX ENX-OUNE
DSA L PY OMMX SHLAH . AX AA
NRSS OBEDT MMRIEN NX

Splitting the message further into 4 through 10 and choosing appropriate keywords resulted in table 5.2 below

Table 5. 2 contains the values of the variables defined earlier from the illustration and the application of Okike's Merged Irregular Transposition Cipher.

Table 5.2. *Okike's Merged Transposition Cipher Defined values of variables*

No. Of Splits (S)	Table Available Spaces No. (A)	Table Fill Characters No. (X)	Table Empty Characters No. (Q)	Table Non-empty Spaces No. (B)	Average No. of Characters per split (L)	Possible Swap Positions per Split (Z)
2	112	9	45	67	29	2
3	102	5	39	63	19.33333	6
4	100	2	40	60	14.5	24
5	120	16	46	74	11.6	120
6	92	1	33	59	9.666667	720
7	100	11	31	69	8.285714	5040
8	96	13	25	71	7.25	40320
9	97	7	32	65	6.444444	362880
10	78	1	19	59	5.8	3628800

From table 5.2 above, the researchers intend to determine the level of complexity with respect to the number of split, S. This can be achieved by extracting from table 5.2 above the No. of Split, S and the Possible Swap Position per Split, Z. This is represented in table 5.3 below:

Table 5.3. *S and Z Relationship*

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

From table 5.3 above, it would be observed that as the number of splits, 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.

5.3. Complexity Level

At this point, it would be good to establish the level of complexity with respect to the number of splits, S of a message. This can be shown by making reference to table 5.2 above. In that table, the variables of interest required in other to show the level of complexity of message with respect to the number of splits, S are the swap positions, Z and the Splits number, S. Table 5.3 above shows the two variables of interest, S and Z. Diagrammatically, table 5.3 above is depicted in figure 5.3:

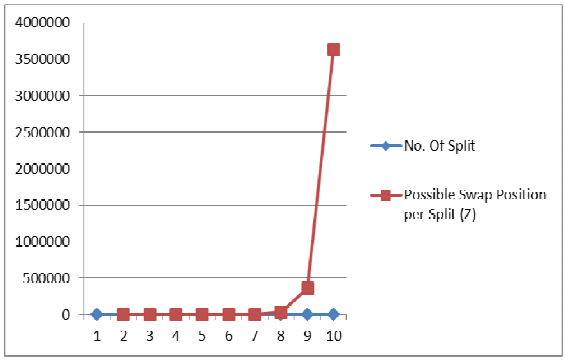

Fig 5.3. *S and Z Relationship*

From fig. 5.3 above, it was observed that when the splits No, S increases from 2,through 7, there is negligible increase in the swap position, Z. But when the splits No., S = 8, then there is a noticeable increase in swap positions, Z which occurred at about 40320.

6. Conclusion

It could be observed that the first noticeable increment in the possible swap positions, Z is seen when the split number, S increased from 8 to 9. Before that point, as the splits number, S increases, also, the number of swap positions, Z also increases. Similarly, the proposed encryption techniques may be applied in various areas of cyber security.

References

[1] Harry B. (2004), "Single Columnar Transposition", http://www.cipher.maths.soton.ac.uk

[2] Luigi S. (2000), "Geometrical Transposition", http://www.ridex.co.uk/cryptology/

[3] Okike B. (2012), Some New Encryption Techniques Using Firewalls and Random Generators, LAP Lambert Academic Publishing, Berlin – Germany, https://www.lap-publishing.com/

[4] Rutter S. (2012), Double Transposition Cipher, http://stuartrutter.com/2012

[5] Terry R. (2001), "Dynamic Transposition Revisited", http://www.ciphersbyritter.com