The International Journal Of Engineering
And Science (IJES)
||Volume|| 2 ||Issue|| 1 ||Pages|| 314-338 ||2013||
ISSN: 2319 – 1813 ISBN: 2319 – 1805

Pattern In Splitting Sequence In Okike's Merged Irregular Transposition Cipher Technique In Securing Web Information

[1,]Okike Benjamin, [2,]Prof. E.G.D. Garba
[1,]*Department Of Computer Science, University Of Abuja, Nigeria*
[2,]*Department Of Mathematics and, Computer Science University Of Jos Nigeria*

----------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. In addition, new issues have surfaced that did not exist previously, e.g., the use of the Internet for business transactions, video conferencing, net meeting, etc. These issues have made it possible for information in transit more vulnerable to attack by unauthorized users. Transposition cipher addresses the above issues - it is at the foundation of all information security. Even if the information in transit is intercepted, with transposition cipher, the information would be meaningless to the interceptor. The researcher will in this work review Single Columnar Transposition Ciphers, Double Columnar Transposition Cipher and Irregular Transposition Cipher. Because of the problems associated with these ciphers, the researcher will deploy Merged Irregular Transposition Cipher to ensure that information is more secure than there are in the reviewed transposition ciphers presently in use. However, Merged Irregular Transposition Cipher will ensure that the original message is split into two or more parts, each of the part encrypted and finally combined to form the ciphertext message that would be sent. The number of parts that the original message would be split depends on the length of the message.

Keywords: *Merged Irregular transposition, Cipher, Web Information, Splitting Sequence*

Date of Submission: 07,January, 2013 Date of Publication: 30, January 2013

I. 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 researcher intends to deploy a Merged Irregular Transposition Cipher to encrypt information. This cipher will certainly offer a more secured information than the other forms of transposition ciphers that already exist since multiple irregular tables and multiple keywords are employed to secure the information. The researcher intends to develop a transposition model to be known as Merged Irregular Transposition Cipher. This cipher will differ considerably not only in terms of the simplicity of its algorithm, but also powerful in its application when compared to existing transposition ciphers. The intended transposition cipher will overcome the weaknesses of the previous transposition ciphers. This would be achieved by the application of multiple irregular tables and keywords to encrypt a message.

II. Literature Review

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

2.1 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. And, if a message might mention, or might not mention, someone with, say, a Q or an X in his name, then a transposition cipher will indeed give that away, although one could solve that by adding some garbage to the end of the message before encrypting it (Henk, 1999). Transposition cipher 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 (John, 2001). To illustrate how transposition cipher without the use of keyword works, the message below can be employed:

DID I HAVE A DREAM OR DID A DREAM HAVE ME – RUSH

To encipher the above message, the letters contained in the message are written out in a block matrix as shown in table 2.1(a) below:

D	I	D	I	H	A	V
E	A	D	R	E	A	M
O	R	D	I	D	A	D
R	E	A	M	H	A	V
E	M	E	R	U	S	H

Table 2.1(a): Block Matrix Containing a message written row-wise

The message is written in the block matrix row-wise. The enciphered message is formed by reading the block matrix column-wise as shown below:

DEORE IAREM DDDAE IRIMR HEDHU AAAAS VMDVH

Of course, that same message may be written in a different order. Table 2.1 (b) below shows the same message written in a spiral form:

D	I	D	I	H	A	V
A	D	R	E	A	M	E
D	R	U	S	H	H	A
I	E	M	E	V	A	D
D	R	O	M	A	E	R

Table 2.1 (b) Block Matrix Containing a message written spiral-wise

When written in a spiral-wise form, the ciphertext corresponding to the same message is shown below:

DADID IDRER DRUMO IESEM HAHVA AMHAE VEADR

Whichever method that is adopted, all that matters is that the sender and the receiver of such message must agree prior to its use, (Anderson, 2002). The grid can have as many columns as desired. Using the same example, table 2.1 (c) below shows block matrix with six columns.

D	I	D	I	H	A
V	E	A	D	R	E
A	M	O	R	D	I
D	A	D	R	E	A
M	H	A	V	E	M
E	Q	R	U	S	H

Table 2.1 (c) : Block Matrix Containing a message written row-wise with 6 columns

From table 2.1 (c) above, it is noticed that there is one empty space, which is filled with a 'Q' - the position to be filled can be decided by the implementer. The ciphertext message is shown as below grouping the letters into six and read column-wise.

DVADME IEMAHQ DAODAR IDRRVU HRDEES AEIAMH

Sometimes when a frequency analysis is carried out, it is often found that each letter occurs with about the same frequency as would be expected in natural English text (or whichever language under study). This is a broad hint that the text is not enciphered using a substitution cipher, but rather by an anagram or transposition cipher, also known as an anagram cipher. In such a cipher the letters of the message are not replaced by substitutes, but rather jumbled using some rule which allows them to be untangled again
to decipher the message. To illustrate how transposition cipher can be enciphered using a keyword "BAD" the plaintext below is employed:

The Quick Brown Fox Jumps Over The Lazy Dog

The first step will be to write out the keyword at the head of a table with three columns, then enter the plaintext in the boxes below as shown in table 2.1 (d) below.

B	A	D
T	H	E
Q	U	I
C	K	B
R	O	W
N	F	O
X	J	U
M	P	S
O	V	E
R	T	H
E	L	A
Z	Y	D
O	G	X

Table 2.1 (d) Plaintext information written under a keyword BAD
Note that the last, empty, box is padded with an X.

Next, the columns are rearranged so that the letters in the keyword are now in alphabetic order as shown in table 2.1 (e) below:

A	B	D
H	T	E
U	Q	I
K	C	B
O	R	W
F	N	O
J	X	U
P	M	S
V	O	E
T	R	H
L	E	A
Y	Z	D
G	O	X

Table 2.1 (e) Plaintext information written under a keyword BAD rearranged as ABD
The rearrangement will produce a ciphertext shown below:

HTEUQIKCBORWFNOJXUPMSVOETRHLEAYZDGOX

Sometimes if the keyword contains repeated letters, then the repeated letters are deleted as it would in a substitution cipher before constructing the grid. Hence if the keyword was TOFFEE, then a grid of 4 columns would be employed with header TOFE and then would be rearranged so that its header would appear as EFOT to encipher the message. To decipher such cipher may be carried out despite the fact that the length of the keyword seems quite crucial. A cryptanalyst should be able to guess this from the length of the ciphertext, which will be a multiple of it. So if the keyword EFOT is applied to encipher the same information that was illustrated with the keyword BAD, then the ciphertext would have a length of 36 which has factors 2,3,4,6,9 and so on. Hence the cryptanalyst could try laying out the text in grids of width 2,3,4,6,9 respectively (a

keyword of length 12 or more is unlikely) and examining the rows. Of course a grid with 2 columns would leave the cryptanalyst just switching alternate letters so the cryptanalyst probably may not need to lay it out that way to check it. Having checked and dismissed the idea of a keyword of length 2, the first grid that may be tried looks like the grid shown in table 2.4 above. Having got to this point the best hope for a quick solution is to find a crib. If there is a word the cryptanalyst thinks ought to appear in the plaintext then the cryptanalyst could try looking for anagrams of that word. This is made difficult by the fact that in splitting the text into blocks (blocks of three in the example), If the crib word does not take up an entire block then even the characters from the crib that do appear will be jumbled with other nearby characters, so there may be a need for a reasonably long crib. On the other hand if it is too long only part of the word will appear in that block so only the anagrams of parts of the crib is sought. In the example, if it is known for some reason, that the text was likely to contain the word "jumps" the cryptanalyst could look for anagrams of "jum", "ump", "mps. Looking carefully the anagram PMS in the text may be observed and a guess that the first and second columns have been transposed may be made while the third has remained fixed. Checking this would have cracked the cipher. Things are harder with longer keywords but the principle remains the same. Things get tougher if the plaintext is not in our own language, since it is harder to say what makes sense. Of course even in this case it may be that part of the message is in a known language and the rest in an unknown language. In this case it might be possible to crack the ciphertext corresponding to the known language of the cryptanalyst, and apply the knowledge that gives an idea about the cipher to write down a decrypt of the entire message, even when the text is unfamiliar, Graham(2004). In English language, the letters q and u occur together so if they are separated either the language is not English or they should be brought back together by undoing the anagram.

2.1.1 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. To see how the Single Columnar Transposition works, the keyword "OZYMANDIAS" is used to illustrate and is numbered in the following way:

O Z Y M A N D I A S
7 10 9 5 1 6 3 4 2 8

That is, the first occurrence of the letter A is numbered 1, the second 2. There are no B:s or C:s so the next letter to be numbered are the D followed by I, and so on. Next the plaintext is written in rows under the numbered keyword, one letter under each letter of the keyword. Assuming the message to be encrypted is as shown below:

Company Has Reached Primary Goal.

Using a Single Columnar Transposition Cipher, table 2.1.1(a) below shows that:

O	Z	Y	M	A	N	D	I	A	S
7	10	9	5	1	6	3	4	2	8
C	O	M	P	A	N	Y	H	A	S
R	E	A	C	H	E	D	P	R	I
M	A	R	Y	G	O	A	L		

Table 2.1.1(a): Single Columnar Transposition Cipher with OZYMANDIAS as keyword

Now 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). The result is the finished cryptogram, which - of course – may be put into groups of five letters, like this:

AHG AR YDA HPL PCY NEO CRM SI MAR OEA

To decrypt a received message enciphered by this method, one must first calculate the number of letters present in the cryptogram. This is done to see how many letters that were originally in the last row. As can be seen above, the two last columns - the ones numbered 2 and 8 - only contains two letters and this is important. Now the cryptogram above contains 28 letters and as a legitimate user of the crypto system, one knows that the keyword is ten letters wide. Therefore the last row must consist of eight letters only, the two final positions being empty. Keeping that in mind - or better still, marking the two final position of row three in some way to indicate that they should not be used - one numbers the keyword letters (just as when encrypting) and then start by writing the first three letters of the cryptogram under keyword letter number one, as shown in table 2.1.1(b) below:

O	Z	Y	M	A	N	D	I	A	S
7	10	9	5	1	6	3	4	2	8
.	.	.	.	A	.	.	.	.	.
.	.	.	.	H	.	.	.	.	.
.	.	.	.	G	.	.	*	*	

Table 2.1.1(b): First three letters of the Cryptogram

Next comes column number two. Since the last position in column two is marked by a star and should not be used, one only writes the next two letters, instead of three. Continue in the same way by writing the next three letters under keyword letter number three, and so on up to keyword letter eight, it will look like as shown in table 2.1.1(c) below:

O	Z	Y	M	A	N	D	I	A	S
7	10	9	5	1	6	3	4	2	8
C	.	.	P	A	N	Y	H	A	.
R	.	.	C	H	E	D	P	R	.
M	.	.	Y	G	O	A	L	*	*

Table 2.1.1(c): 8th keyword letters of the Cryptogram

Now column eight follows, and there are only two letters which should be written as stated above (the position marked by a star being left empty). This leaves six letters of the cryptogram, and these - of course - are written in column nine and ten, and then the message can be read in the normal way, row by row. Usually when employing a transposition cipher like the above, one adds dummy letters to make the final group five letters long if it is not already full. 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 (Randy, 1996).

2.1.2 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. To illustrate the use of a Double Columnar Transposition Cipher using the keywords Agamemnon and Mycenae. The message to be encrypted reads:

SEND ARMOURED CAR TO HEADQUARTERS

Using keyword Agamemnon, table 2.1.2(a) below shows how the message can be encrypted with Double Columnar Transposition Cipher technique.

A	G	A	M	E	M	N	O	N
1	4	2	5	3	6	7	9	8
S	E	N	D	A	R	M	O	U
R	E	D	C	A	R	T	O	H
E	A	D	Q	U	A	R	T	E
R	S	J						

Table 2.1.2(a): Double Columnar Transposition Cipher with keyword Agamemnon

(Note dummy letter j is added at the end to make the total number of letters a multiple of five).
This first encryption when read column-wise gives:

SRER NDDJ AAU EEAS DCQ RRA MTR UHE OOT.

These ciphertext letters are written under the second keyword, as it is shown in table 2.1.2(b) below:

M	Y	C	E	N	A	E
5	7	2	3	6	1	4
S	R	E	R	N	D	D
J	A	A	U	E	E	A
S	D	C	Q	R	R	A
M	T	R	U	H	E	O
O	T					

Table 2.1.2(b): Second Double Columnar Transposition with keyword Mycenae

This will in turn give the cryptogram:

DERE EACR RUQU DAAO SJSMO NERH RADTT

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, Torbjorn (1998). 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.

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. 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 (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. To illustrate how the Geometrical Transposition Cipher works, the keyword CONVENIENCE may be employed for this purpose. Similarly, the message to be encrypted reads:

Here Is A Secret Message Enciphed By Transposition

Table 2.1.3(a) below shows how Geometrical Transposition can be used to encrypt the information above:

C	O	N	V	E	N	I	E	N	C	E
1	10	7	11	3	8	6	4	9	2	5
H										
E	R	E	I	S	A	S	E	C	R	
E	T	M	E	S						
S	A	G	E	E	N	C	I			
P	H	E	R	E	D	B	Y	T	R	A
N	S	P	O	S	I	T				
I	O	N								

Table 2.1.3(a): Geometrical Transposition with keyword convenience

This produces the ciphertext message below:

HEESPNI RR SSEES EIY A SCBT EMGEPN ANDI CT RTAHSO IEERO

Here, the first row is filled in only up to the column with the key number 1; the second row is filled in only up to the column with the key number 2; and so on. The key number represents the letter' ordinal value. Of course, one still stops when one runs out of plaintext letters, so the eighth row stops short of the key number 8 in this example. This method has the Advantage Of Dividing The Text Being Transposed In A More Irregular Fashion Than Ordinary Columnar Transposition. The Keyword "CONVENIENCE" As Used Is Called Taking-Off Keyword. The Columns Are Taken Off Alphabetically From Left To Right With Duplicates Being Assigned The Next Ordinal Value.

Merged Irregular Transposition Cipher

The researcher has 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 is split into multiple parts and encrypted. At the end, the encrypted parts will be combined together for the ciphertext information to be sent. 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 researcher intends to develop a new type of cipher to be known as 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 behaviour of each of the part in relation to the overall behavior of the cipher.

Structure of Merged Irregular Cipher

The structure of the table is depicted in table 3.1 below:

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

Table 3.1 : Keyword written against Column

From the tables above, there are n rows and m columns. In table 3.1, the keyword is written against the columns. There would not be much difference if the keywords are written against the rows. To illustrate how the 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.

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 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 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"

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-U 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 PAEARIS. X

which will produce the combined ciphertext below:

N:OS L TOE-U 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 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

S= 4

ATTENTION: POLI 14

CE BOSS – HOODLUM 14
S PLAN MAYHEM ON AN 15
AMBRA RESIDENTS. 15

The first part of this message "ATTENTION: POLI" may be encrypted using the keyword BREAD as below:

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

This will produce the ciphertext message below:

EN ANTPI : TOL TIOX

Applying the keyword MONEY to encrypt the second part of the message "CE BOSS – HOODLUM"

Col	1	2	3	4	5
K/W	M	O	N	E	Y
O/V	2	4	3	1	5
Row					
1	C	E	B	O	
2	S				
3	S	–	H		
4	O	O			
5	D	L	U	M	X

which produces the ciphertext message below:

OM CSSOD BHU E-OL X

The keyword PAPER when applied to encrypt the third part of the message with 15 characters" S PLAN MAYHEM ON AN"

Col	1	2	3	4	5
K/W	P	A	P	E	R
O/V	3	1	4	2	5
Row					
1	S	P			
2	L	A	N	M	
3	A				
4	Y	H	E		
5	M	O	N	A	N

will give rise to the ciphertext below:

PAHO MA SLAYM NEN N

The keyword WIPER if applied to the fourth part of the message "AMBRA RESIDENTS."

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

will produce the ciphertext message below:

RT MRSE BIN S AAED.

Which will produce the combined ciphertext message below:

EN ANTPI : TOL TIOX OM CSSOD BHU E-OL X PAHO MA SLAYM NEN N
RT MRSE BIN S AAED.

S=5

ATTENTION: P	11
OLICE BOSS – H	11
OODLUMS PLAN M	12
AYHEM ON ANAMB	12
RA RESIDENTS.	12

Using the keyword CARES to encrypt the first part of the message "ATTENTION: P"

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

This will produce the ciphertext message

TNNX ATEOP IX T:X X

Using the keyword THANK to encrypt the second part of the message" OLICE BOSS – H"

Col	1	2	3	4	5
K/W	T	H	A	N	K
O/V	5	2	1	4	3
Row					
1	O	L	I		
2	C	E			
3	B	O	S	S	–
4	H	X	X	X	

This will produce the ciphertext message

ISX LEOX - SX OCBH

To encrypt the third part of the message "OODLUMS PLAN M" using the keyword SIGNS

Col	1	2	3	4	5
K/W	S	I	G	N	S
O/V	4	2	1	3	5
Row					
1	O	O	D		
2	L	U			
3	M	S	P	L	
4	A				
5	N	M	X	X	X

which will produce ciphertext message below:

DPX OUSM LX OLMAN X

Using the keyword SENDS to encrypt the fourth part of the message “AYHEM ON ANAMB”

Col	1	2	3	4	5
K/W	S	E	N	D	S
O/V	4	2	3	1	5
Row					
1	A	Y	H	E	
2	M	O			
3	N	A	N		
4	A				
5	M	B	X	X	X

This will produce the ciphertext message below:

EX YOAB HNX AMNAM X

Finally, to complete the last part of the message “RA RESIDENTS.”, the keyword GANGS is used

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

will produce the ciphertext message below:

ASN. RREES DX ITX X

will produce the combined ciphertext message below:

TNNX ATEOP IX T:X X ISX LEOX - SX OCBH
DPX OUSM LX OLMAN X EX YOAB HNX AMNAM X
ASN. RREES DX ITX X

S=6

ATTENTION	9
: POLICE BO	9
SS – HOODLUM	10
S PLAN MAYHE	10
M ON ANAMBRA	10
RESIDENTS.	10

To encrypt the first part of the message “ATTENTION” using the keyword SAND

Col	1	2	3	4
K/W	S	A	N	D
O/V	4	1	3	2
Row				
1	A	T		
2	T	E	N	T
3	I	O	N	

.

will the ciphertext message below:

TEO T NN ATI

To encrypt the second part of the message ": POLICE BO" using the keyword COME

Col	1	2	3	4
K/W	C	O	M	E
O/V	1	4	3	2
Row				
1	:			
2	P	O	L	I
3	C	E	B	
4	O	X		

will produce the ciphertext message below:

:PCO I LB OEX

Encrypting the third part of the message" SS – HOODLUM" using the keyword GAME

Col	1	2	3	4
K/W	G	A	M	E
O/V	3	1	4	2
Row				
1	S	S		
2	-	H	O	O
3	D			
4	L	U	M	

will produce the ciphertext message below

SHU O S-DL OM

To encrypt the fourth part of the message "S PLAN MAYHE" using the keyword GONE

Col	1	2	3	4
K/W	G	O	N	E
O/V	2	4	3	1
Row				
1	S	P	L	A
2	N			
3	M	A	Y	
4	H	E		

will produce the ciphertext message below:

A SNMH LY PAE

To encrypt the fifth part of the message "M ON ANAMBRA" using the keyword SAKE

Col	1	2	3	4
K/W	S	A	K	E
O/V	4	1	3	2
Row				
1	M	O		
2	N	A	N	A
3	M	B	R	
4	A			

will produce the ciphertext message below:

OAB A NR MNMA

The final part of the message" RESIDENTS." using the keyword JAIL

Col	1	2	3	4
K/W	J	A	I	L
O/V	3	1	2	4
Row				
1	R	E		
2	S	I	D	
3	E			
4	N	T	S	.

will produce the ciphertext message below:

EIT DS RSEN .

will produce the combined ciphertext message below:

TEO T NN ATI :PCO I LB OEX SHU O S-DL OM A SNMH
LY PAE OAB A NR MNMA EIT DS RSEN .

S=7

ATTENTIO	8
N: POLICE	8
BOSS – HOO	8
DLUMS PLA	8
N MAYHEM O	8
N ANAMBRA R	9
ESIDENTS.	9

The first part of the message “ATTENTIO”, using SEES as a keyword

Col	1	2	3	4
K/W	S	E	E	S
O/V	3	1	2	4
Row				
1	A	T		
2	T	E	N	
3	T			
4	I	O	X	X

This will produce the ciphertext below:

TEO NX ATTI X

The second part of the message “N: POLICE” using keyword SONG

Col	1	2	3	4
K/W	S	O	N	G
O/V	4	3	2	1
Row				
1	N	:	P	O
2	L	I	C	
3	E	X		

This will produce the ciphertext message

O PC :IX NLE

To encrypt the third part of the message “BOSS – HOO” using keyword KNOW

Col	1	2	3	4
K/W	K	N	O	W
O/V	1	2	3	4
Row				
1	B			
2	O	S		
3	S	–	H	
4	O	O	X	X

This will produce the ciphertext message below:

BOSO S-O HX X

To encrypt the fourth part of the message "DLUMS PLA"

Col	1	2	3	4
K/W	G	A	V	E
O/V	3	1	4	2
Row				
1	D	L		
2	U	M	S	P
3	L			
4	A	X	X	

This will produce the ciphertext message

LMX P DULA SX

To encrypt the fifth part of the message "N MAYHEM O" using YOUR as keyword

Col	1	2	3	4
K/W	Y	O	U	R
O/V	4	1	3	2
Row				
1	N	M		
2	A	Y	H	E
3	M	O	X	

will produce the ciphertext message

MYO E HX NAM

To encrypt the sixth part of the message "N ANAMBRA R" using SANK as keyword

Col	1	2	3	4
K/W	S	A	N	K
O/V	4	1	3	2
Row				
1	N	A		
2	N	A	M	B
3	R	A	R	

Will produce ciphertext message below:

AAA B MR NNR

To encrypt the last part of the message "ESIDENTS." Using SEAT as keyword

Col	1	2	3	4
K/W	S	E	A	T
O/V	3	2	1	4
Row				
1	E	S	I	
2	D	E		
3	N	T	S	
4	.	X	X	X

will produce the ciphertext message below:

ISX SETX EDN. X

will produce the combined ciphertext message below:

TEO NX ATTI X O PC :IX NLE BOSO S-O HX X LMX PDULA SX
MYO E HX NAM AAA B MR NNR ISX SETX EDN. X

S=8

ATTENTI	7
ON: POLI	7
CE BOSS –	7
HOODLUM	7
S PLAN MA	7
YHEM ON A	7
NAMBRA RE	8
SIDENTS.	8

To encrypt the first part of the message "ATTENTI" using the keyword FALL

Col	1	2	3	4
K/W	F	A	L	L
O/V	2	1	3	4
Row				
1	A	T		
2	T			
3	E	N	T	
4	I	X	X	X

will produce the ciphertext message below:

TNX ATEI TX X

To encrypt the second part of the message "ON: POLI" using the keyword VIEW

Col	1	2	3	4
K/W	V	I	E	W
O/V	2	1	3	4
Row				
1	O	N		
2	:			
3	P	O	L	
4	I	X	X	X

will produce the ciphertext message below:

NOX O:PI LX X

To encrypt the third part of the message "CE BOSS –" using the keyword SOLD

Col	1	2	3	4
K/W	S	O	L	D
O/V	2	1	3	4
Row				
1	C	E		
2	B			
3	O	S	S	
4	–	X	X	X

will produce the ciphertext message below:

ESX CBO- SX X

To encrypt the fourth part of the message "HOODLUM" Using CARD as keyword

Col	1	2	3	4
K/W	C	A	R	D
O/V	2	1	4	3
Row				
1	H	O		
2	O			
3	D	L	U	M

will produce the ciphertext message below:

OL HOD M U

To encrypt the fifth part of the message "S PLAN MA" Using TALK as keyword

Col	1	2	3	4
K/W	T	A	L	K
O/V	4	1	3	2
Row				
1	S	P		
2	L	A	N	M
3	A	X	X	

will produce the ciphertext message below:

PAX M NX SLA

To encrypt the sixth part of the message "YHEM ON A" using the keyword DISK

Col	1	2	3	4
K/W	D	I	S	K
O/V	1	2	4	3
Row				
1	Y			
2	H	E		
3	M	O	N	A

will produce the ciphertext message below:

YHM EO A N

To encrypt the seventh part of the message "NAMBRA RE" using SACK as keyword

Col	1	2	3	4
K/W	S	A	C	K
O/V	4	1	2	3
Row				
1	N	A		
2	M	B	R	
3	A	R	E	X

will produce the ciphertext message below:

ABR RE X NMA

To encrypt the last part of the message "SIDENTS." Using TELL as keyword

Col	1	2	3	4
K/W	T	E	L	L
O/V	4	1	2	3
Row				
1	S	I		
2	D	E	N	
3	T	S	.	X

will produce the ciphertext message below:

IES N. X SDT

will produce the combined ciphertext message below:

TNX ATEI TX X NOX O:PI LX X ESX CBO- SX X OL
HOD M U PAX M NX SLA YHM EO A N ABR RE
X NMA IES N X SDT

S=9

ATTENT	6
ION: PO	6
LICE BO	6
SS – HOO	6
DLUMS P	6
LAN MAYH	7
EM ON ANA	7
MBRA RES	7
IDENTS.	7

To encrypt the first part of the message " ATTENT" using CAN as keyword

Col	1	2	3
K/W	C	A	N
O/V	2	1	3
Row			
1	A	T	
2	T		
3	E	N	T

will produce the ciphertext message below:

TN ATE T

To encrypt the second part of the message "ION: PO " using CAN as keyword

Col	1	2	3
K/W	G	E	T
O/V	2	1	3
Row			
1	I	O	
2	N		
3	:	P	O

will produce the ciphertext message below:

OP IN: O

To encrypt the third part of the message "LICE BO" using AND as keyword

Col	1	2	3
K/W	A	N	D
O/V	1	3	2
Row			
1	L		
2	I	C	E
3	B	O	

will produce the ciphertext message below:

LIB E CO

To encrypt the forth part of the message "SS – HOO" using OFF as keyword

Col	1	2	3
K/W	O	F	F
O/V	3	1	2
Row			
1	S	S	
2	-	H	O
3	O		

will produce the ciphertext message below:

SH O S-O

To encrypt the fifth part of the message "DLUMS P" using FOR as keyword

Col	1	2	3
K/W	F	O	R
O/V	1	2	3
Row			
1	D		
2	L	U	
3	M	S	P

will produce the ciphertext message below:

DLM US P

To encrypt the sixth part of the message "LAN MAYH" using HELP as keyword

Col	1	2	3	4
K/W	H	E	L	P
O/V	2	1	3	4
Row				
1	L	A		
2	N			
3	M	A	Y	
4	H	X	X	X

will produce the ciphertext message below:

AAX LNMH YX X

To encrypt the seventh part of the message "EM ON ANA" using FAME as keyword

Col	1	2	3	4
K/W	F	A	M	E
O/V	3	1	4	2
Row				
1	E	M		
2	O	N	A	N
3	A			

will produce the ciphertext message below:

MN N EOA A

To encrypt the eighth part of the message "MBRA RES" using TERM as keyword

Col	1	2	3	4
K/W	T	E	R	M
O/V	4	1	3	2
Row				
1	M	B		
2	R	A	R	E
3	S	X	X	

will produce the ciphertext message below:

BAX E RX MRS

To encrypt the last part of the message "IDENTS. "using TERM as keyword

Col	1	2	3	4
K/W	T	O	R	N
O/V	4	2	3	1
Row				
1	I	D	E	N
2	T	S		
3	.	X	X	

will produce the ciphertext message below:

N DSX EX IT

will produce the combined ciphertext message below:

TN ATE T OP IN: O LIB E CO SH O S-O DLM US P AAX
LNMH YX X MN N EOA A BAX E RX MRS N DSX EX IT.
S=10

ATTEN	5
TION:	5
POLICE	6
BOSS – H	6
OODLUM	6
S PLAN M	6
AYHEM O	6
N ANAMB	6
RA RESI	6
DENTS.	6

To encrypt the first part of the message "ATTEN" using TAB as keyword

Col	1	2	3
K/W	T	A	B
O/V	3	1	2
Row			
1	A	T	
2	T	E	N

will produce the ciphertext message below:

TE N AT

To encrypt the second part of the message "TION:" using DON as keyword

Col	1	2	3
K/W	D	O	N
O/V	1	3	2
Row			
1	T		
2	I	O	N
3	:	X	

will produce the ciphertext message below:

TI: N OX

To encrypt the third part of the message "POLICE" using MAY as keyword

Col	1	2	3
K/W	M	A	Y
O/V	2	1	3
Row			
1	P	O	
2	L		
3	I	C	E

will produce the ciphertext message below:

OC PLI E

To encrypt the fourth part of the message "BOSS – H" using MAY as keyword

Col	1	2	3
K/W	S	O	N
O/V	3	2	1
Row			
1	B	O	S
2	S	–	
3	H		

will produce the ciphertext message below:

S O- BSH

To encrypt the fifth part of the message "OODLUM" using SAN as keyword

Col	1	2	3
K/W	S	A	N
O/V	3	1	2
Row			
1	O	O	
2	D	L	U
3	M		

will produce the ciphertext message below:

OL U ODM

To encrypt the sixth part of the message "S PLAN M" using THE as keyword

Col	1	2	3
K/W	T	H	E
O/V	3	2	1
Row			
1	S	P	L
2	A	N	
3	M		

will produce the ciphertext message below:

L PN SAM

To encrypt the seventh part of the message "AYHEM O" using DID as keyword

Col	1	2	3
K/W	D	I	D
O/V	1	3	2
Row			
1	A		
2	Y	H	E
3	M	O	

will produce the ciphertext message below:

AYM E HO

To encrypt the eight part of the message "N ANAMB" using SUN as keyword

Col	1	2	3
K/W	S	U	N
O/V	2	3	1
Row			
1	N	A	N
2	A		
3	M	B	

will produce the ciphertext message below:

N NAM AB

To encrypt the ninth part of the message "RA RESI" using TWO as keyword

Col	1	2	3
K/W	T	W	O
O/V	2	3	1
Row			
1	R	A	R
2	E		
3	S	I	

will produce the ciphertext message below:

R RES AI

To encrypt the last part of the message "DENTS. " using CUT as keyword

Col	1	2	3
K/W	C	U	T
O/V	1	3	2
Row			
1	D		
2	E	N	T
3	S	.	

will produce the ciphertext message below:

DES T N.

will produce the combined ciphertext message below:

TE N AT TI: N OX OC PLI E S O- BSH OL U
ODM L PN SAM AYH E HO N NAM AB R RES AI DES T N.

4.0 Analysis of Results

Table 4. 0 below contains the values of the variables defined earlier from the illustration and the application of the Merged Irregular Transposition Cipher.

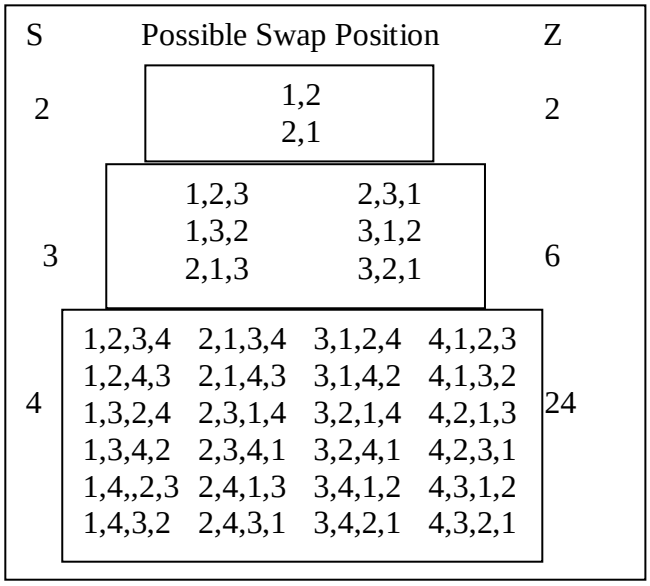
No. Of Split (S)	Table Available Spaces No. (A)	Table Fill Characters No. (X)	Table Empty Characters No. (Q)	Table Non-empty Spaces No. (B)	Possible Swap Position per Split (Z)
2	112	9	45	67	2
3	102	5	39	63	6
4	100	2	40	60	24
5	120	16	46	74	120
6	92	1	33	59	720
7	100	11	31	69	5040
8	96	13	25	71	40320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

Table 4. 0: Merged Transposition Cipher Defined values of variables

From table 4. 0 above, the researcher intends to determine the pattern in the splitting sequence

4.1 Pattern in Splitting Sequence

The pattern in the 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 pattern sequenc**e**. This is shown in table 4.1 (a) that follows:



From table 4.1 (a) above, it could be observed that the number of swap positions, Z of message is equal to factorial of the number of splitting, S of that same message. Mathematically, it can be shown that:

$$Z = S !$$

Table 4.1 (b) below shows split No., S and the number of swap positions, Z obtained from table 4. 0 seen earlier in this work. This is in conformity with $Z = S !$.

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 4.1 (b) 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.

Summary

The researcher has just developed a new transposition cipher known as Merged Irregular Transposition Cipher which may not be easily decrypted. However, the researcher may want to state that transposition cipher generally offers a better information security than substitution ciphers which often times may be subjected to frequency analysis. During the course of this research work, the Single Columnar Transposition, Double Columnar Transposition ciphers were both reviewed and found to have the weaknesses that both may easily be decrypted as a result of their almost fixed number of characters. However, the Irregular Transposition Cipher was invented to solve the above problem, but not without its own weaknesses. The Merged Irregular Transposition Cipher has just been invented to make use of multiple keywords and multiple tables in which the entire message is subdivided into multiple parts and each part encrypted separately. To make this cipher more secure than the Irregular Transposition Cipher already in existence, the positions of the parts that make up the

encrypted cipher may be swapped for one another thereby creating more problems for the cryptanalysts to overcome. Finally, the researcher may wish to state that the issue of information security is one which has existed for as long as the act of reading and writing have existed, although, it has not been given the prominence it deserves. Some people may argue that no new knowledge exist in this area, whatever knowledge that may come up may not be entirely new, rather it may be as a result of recycled and modified knowledge to improve on the existing one.

References

[1]. Anderson, C. J. (2002), "Simple Encipherment Techniques" URL:http://neworder.box.sk/
[2]. Graham N. (2004), "On Transposition Cipher", University of Southampton
[3]. Harry B. (2004), "Single Columnar Transposition", URL: http://www.cipher.maths.soton.ac.uk
[4]. Henk C.A. (1999), "Fundamentals of Cryptology", Eindhoven University of Technology, The Netherland
[5]. John S. (2002), "Method of Transposition", URL: http://home.ecn.ab.ca/~/savard/
[6]. Luigi S. (2000), "Geometrical Transposition", URL: http://www.ridex.co.uk/cryptology/
[7]. Randy N. (1996), "Classical Cryptography", URL: http://www.und.nodak.edu/crypto/
[8]. Terry R. (2001), "Dynamic Transposition Revisited", URL: http://www.ciphersbyritter.com