British Journal of Mathematics & Computer Science
7(3): 229-240, 2015, Article no.BJMCS.2015.118
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

SCIENCEDOMAIN

Development of Okike’s Merged Irregular Transposition Cipher and Its Level Error

Okike Benjamin[1*] and E. J. D Garba[2]

[1]*Department of Computer Science, University of Ghana, Legon, Ghana.*
[2]*Department of Mathematics, University of Jos, Nigeria.*

Article Information

DOI: 10.9734/BJMCS/2015/14869
Editor(s):
(1) Dariusz Jacek Jakóbczak, Computer Science and Management Department, Technical University of Koszalin, Poland.
Reviewers:
(1) M. Thiyagarajan, Nehru Institute of Engineering & Technology, Affiliated to Anna University, India.
(2) Anonymous, India.
(3) Anonymous, Saudi Arabia.
Complete Peer review History: http://www.sciencedomain.org/review-history.php?iid=934&id=6&aid=8129

Original Research Article

Received: 27 October 2014
Accepted: 22 January 2015
Published: 14 February 2015

Abstract

Okike’s Merged Irregular Transposition Cipher is a new technique for enciphering information along the superhighway. In this method, a message to be transmitted along the superhighway is first split into parts and each part is encrypted separately before transmission occurs. The positions of the split encrypted messages may be swapped. This work deployed a message with approximately 58 characters to study the behavior of the error level as the message is split from 2 through 10. It was observed that as the number of split increases, the error level decreases. Similarly, the optimal split number occurs when the integer value of the error begins to repeat as is seen when the split number equals 8.

Keywords: Okike’s merged irregular transposition, error level, model estimation, message encryption, message splitting, message decryption.

1 Introduction

From time immemorial, the hiding of the real meaning of information has always been there. Julius Caesar’s cipher gave him advantage over his opponents during his days. Caesar’s cipher then employed simple substation method to conceal the actual meaning of information to be exchanged.

**Corresponding author: okikeb@yahoo.com;*

Today, due to the growing need of online businesses by individuals, organizations or governments, there is need to keep information relating to these businesses secret. Encryption holds a key to keeping online businesses secret from prying eyes on the superhighway.

Russel [1] stated that cryptography has had a long and colourful history. In other words, it means that cryptography has been in existence since the creation of humans and that it has also existed in many forms. Today, many cryptographic analysis are carried out with computers as against pen and paper that was earlier deployed. The earliest schemes, now termed the classical ciphers, were designed to be carried out with pen and paper rather than by electronics. Many were transpositions: algorithms which rearrange the order of letters in a message. Classical cryptography became obsolete after the invention of computers; more complex ciphers could be used, and older ciphers broken with less difficulty. Nonetheless, modern analogues of classical schemes can still be found as components of larger ciphers.

Transposition cipher on the other hand rearranges the characters contained in the messages, thereby hiding the real meaning of the message. Transposition may be Single Columnar, Double Columnar, Dynamic or Irregular Ciphers.

The new transposition cipher developed by the researchers is called Okike’s Merged Irregular Transposition Cipher which makes it possible for the message to be split into parts before the encryption process takes place. When this happens, each part of the message may be encrypted separately and before the encrypted message is sent out, the positions may be swapped to make decryption by an unauthorized user difficult. In this work, a sample message is deployed in order to study the behavior of a message when split into parts. In the sample message, the split is carried out from 2 through 10 so that a model is estimated. As the message is split from 2 through 10, the average number of characters per split is taken. This is used to determine the error level in the estimated model.

PDF Email encryption method is especially useful when dealing with one-way communications such as sending monthly statements to customers, where no response is required. The message is encrypted as a secure PDF that is sent to the recipient’s mailbox, making it ideal for situations in which individuals need to access encrypted and unencrypted email in the same inbox due to legal reasons or user preference.

Guardian Weekly [2] pointed out that US and British intelligence agencies have successfully cracked much of the online encryption relied upon by hundreds of millions of people to protect the secrecy of their personal data, online transactions and emails, according to top-secret documents revealed by former contractor Edward Snowden. This is bad news for those whose businesses are transacted online since the confidentiality of even their finances are no longer guaranteed. As such, there is an urgent need to develop an encryption technique that may not easily be decrypted by spies.

2 Substitution Cipher

Dhavare stated in his work that substitution ciphers are one of the earliest types of ciphers that was used by men. Examples of classic substitution ciphers include the well-known simple substitution and the less well-known homophonic substitution. Although simple substitution ciphers are indeed simple – both in terms of their use and attacks; the homophonic substitution ciphers are far more challenging to break. Even with modern computing technology, homophonic substitution ciphers remain a significant challenge to criminals on the superhighway [3].

The simple substitution cipher is a cipher that has been in use for many hundreds of years ago, but is still in use today. It basically consists of substituting every plaintext of character for a different ciphertext character. A simple substitution cipher is a method of concealment that replaces each letter of a plaintext message with another letter [4].

3 Transposition Cipher

Collberg [5] defined transposition cipher as a method of encryption by which units of plaintext are rearranged to form the ciphertext. In a transposition cipher the original characters of the plaintext are not changed, but simply moved around in the ciphertext.

With transposition cipher, letter orders are rearranged without altering the actual letters. Row Transposition Ciphers allow letters in rows to be written out, reorder the columns according to the key before reading off [6].

4 Okike's Merged Irregular Transposition Cipher

A geometrical transposition which was developed in order to solve the problem of ease of decryption of earlier types of ciphers is also called the irregular transposition cipher and is one which employs the use of keyword with 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 improve on the Irregular Transposition Cipher, the researchers intend to develop cipher to be known as Okike's Merged Irregular Transposition Cipher. Unlike the Irregular Transposition Cipher already in existence, Okike's Merged Irregular Transposition Cipher will utilize many tables and keywords to encrypt information. The first step toward the use of this model will be to divide the entire message into multiple equal or nearly equal parts. The number of parts will depend on 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 behaviour of the cipher.

4.1 Structure of Okike's Merged Irregular Cipher

As in [7], the structure of the table is depicted in Table 4.1 below:

Table 4.1. 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							
4							
:							
:							
:							
:							
:							
n							

The above contains n rows and m columns. In Table 4.1, the keyword is written against the columns. However, it is possible to write 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.

4.2 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 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.

$$S=2$$

If UNIVERSE is the 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 would in turn produce the ciphertext below:

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

Looking through the Table above, it may be observed the ordinal value of the chosen keyword is written under each of the letter in the keyword. For instance, the first letter E in the keyword UNIVERSE has ordinal value of 1 and the second has ordinal value of 2. Similarly, the Letter I has ordinal value of 3. These ordinal values are obtained through their positions in the English alphabets. In other words if the letters ‘k’ and ‘e’ occur in a keyword, the ordinal value of e would be 1 since letter ‘e’ comes before letter ‘k’ in the English alphabet.

As the letters contained in the message are inserted row-wise, each row must terminate with the column’s ordinal value. In other words, row 1 must terminate in column with ordinal value of 1, row 2 must terminate in column with ordinal value of 3 etc.

Again if SCIENCES is the 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							

would produce the ciphertext below:

LNMNEDX   HRX   ANMNX   AX   MOASEX   YBTX
PEAARIS. X

Combing the first part of the encrypted message with the second part will produce the 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 take the first position which would increase the complexity of the encryption algorithm.

Going through the same process of splitting when S becomes 3 is shown below:

S= 3

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

If FORSEE is chosen as the keyword, the first part of the message “ATTENTION: POLICE BOS” would be encrypted as below:

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

Choosing VISION as the keyword to encrypt the second part of the message “S - HOODLUMS PLAN MAYHE” would appear as below:

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 as well 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.” is as in the Table below:

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	

This produces the ciphertext message shown below:

AX AA NRSS OBEDT MMRIEN NX
If the 3 separate ciphertext is combined, the result would appear as below:

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

When the message is split into 4 parts, the first 2 parts have 14 characterseach and the last 2 parts have 15 characters each.

S= 4

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

The first part of this message which reads “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 would produce 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

If WIPER is used as a keyword to encrypt the fourth part of the message, which is "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		R			
3		S	I		
4	D	E	N	T	S
5	.				

.

produces the ciphertext message below:

RT MRSE BIN S AAED.

Combining the 4 different encrypted ciphertext messages would produce the encrypted message below:

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

Further Splitting the message into 5 through 10 and choosing appropriate keywords would result in Table 4.2 below:

Table 4.2. Merged transposition cipher defined values of variables

No. of split(S)	Average no. of characters per split (L)
2	29
3	19.33333
4	14.5
5	11.6
6	9.666667
7	8.285714
8	7.25
9	6.444444
10	5.8

From Table 4.2 above, the researchers intend to estimate a model and determine the level of error with respect to the number of split, S.

5 Model Estimation

As the parameter changes in value, different probability distributions are generated. Jae {8] defined a model as the family of probability distributions indexed by the model's parameters.

In this section, the researchers intend to estimate a model and use the model to determine the level of error, ε with respect to the number of split, S of a given message sample.

Given a model:

$L = \alpha + \beta S + \varepsilon$, where

L is the dependent variable, which is the average
character No. in each split, S
S is the Split No. which is the independent
variable.
α is point of interception of L at the point where S=0
β is the rate of change of L for each unit change in S.
ε is the error, the difference between the actual value of L and
the estimated value, أ,

the model estimate أ may be computed so as to find out error in the estimate with respect to the number of split., S.

From Table 4.2 above, s, which is the difference between S and mean of S can be computed. Also l, the difference between L and mean of L are computed for each value of S [9]. This is depicted in Table 5.0 below:

Table 5.0. Values of S, L, l and s

S	L	s = S- Ś	l = L- Ĺ	sl	s^2
2	29	-4	16.56887	-66.2755	4
3	19.33333	-3	6.902202	-20.7066	9
4	14.5	-2	2.068872	-4.13774	16
5	11.6	-1	-0.83113	0.831128	25
6	9.666667	0	-2.76446	0	36
7	8.285714	1	-4.14541	-4.14541	49
8	7.25	2	-5.18113	-10.3623	64
9	6.444444	3	-5.98668	-17.9601	81
10	5.8	4	-6.63113	-26.5245	100
54	111.8802			-149.281	384

Statistically,

$$\acute{S} = \frac{\sum S}{n} = \frac{54}{9} = 6$$

$$\acute{L} = \frac{\sum L}{n} = \frac{111.8802}{9} = 12.43113$$

$$\beta = \frac{\sum sl}{\sum s^2} = \frac{-149.281}{384} = -0.38875$$

$$\alpha = \acute{L} - \beta\acute{S} = 12.43113 - (-0.38875 * 6)) = 14.76363$$

Therefore, the model is of the form:

$L = 14.76363 - 0.38875S + \varepsilon$, which means that S is inversely proportional to L.

$L = 14.76363 - 0.38875S + \varepsilon$ ----------i
$\acute{l} = 14.76363 - 0.38875S$ -----------------ii

Then the error in the estimate can be computed from equation ii – i as shown in the Table 5.1 below:

From the Table 5.1 above, it could be seen that as the split number, S of the message being encrypted increases, the error level in the model decreases. However, it is worthy of mention that the optimal error level occurred when the split number has a value of 8. That is the first time the integer part of the error value repeated itself for the first time.

Table 5.1. Values of S, L, l and ε

S	L	أ	ε
2	29	13.98613	15.01387
3	19.33333	13.59738	5.73595
4	14.5	13.20863	1.29137
5	11.6	12.81988	-1.21988
6	9.666667	12.43113	-2.76446
7	8.285714	12.04238	-3.75667
8	7.25	11.65363	-4.40363
9	6.444444	11.26488	-4.82044
10	5.8	10.87613	-5.07613

6 Conclusion

The error level of the estimated model is inversely proportional to the number of split, S of the message. Also, the more the number of splits, the more complex it becomes for unauthorized users to decrypt the message. The number of splits depends on the message length. Because of the length of the message under consideration, the optimal split value occurred at the value of 8.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Russell MD, Clark JA, Stepney S. Making the most of two heuristics. Breaking Transposition Ciphers with Ants; 2003.
Available: http://pdf.aminer.org/000/226/812/

[2] Guardian Weekly. Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security; 2013.
Available: http://www.theguardian.com/world/2013/

[3] Dhavare A. Efficient attacks on homophonic substitution ciphers, being a masters project submitted to the Department of Computer Science, San Jose State University; 2011. Available: http://www.scholarworks.sjsu.edu/cgi/

[4] Christensen C. Simple substitution ciphers; 2006.
Available: www.nku.edu/~christensen/

[5] Collberg C. Cryptography — Introduction. Being lecture delivered in the department of computer science, University of Arizona; 2012.
Available: www.cs.arizona.edu/~collberg/Teaching/466-566/2012/

[6] Jain R. Classical encryption techniques, Washington University in Saint Louis; 2011. Available: www.cse.wustl.edu/~jain/cse571-11/

[7] Okike B, Garba EJD. Pattern In splitting sequence in Okike's merged irregular transposition cipher technique in securing web information. The International Journal of Engineering and Science (IJES). 2013;2(1):314-338.
Available: http://www.theijes.com/papers/v2-i1/AZ02103140338.pdf

[8] Jae M. Tutorial on maximum likelihood estimation. Journal of Mathematical Psychology. 2003;90–100.
Available: http://www.elseveier.com/locate

[9] Okike B. Some new encryption techniques using firewalls and random generators, LAP Lambert Academic Publishing, Berlin – Germany; 2012.
Available: https://www.lap-publishing.com/

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
www.sciencedomain.org/review-history.php?iid=934&id=6&aid=8129