Development of Okike's 2-Tail Reversed Cipher Algorithm

Okike Benjamin, Garba EJD

Abstract— Today, many cryptographic algorithms exist that may be deployed to conceal cyberspace information from unauthorized access. There is no doubt that some of these algorithms can easily be decrypted, there are others that may prove difficult decrypting. This work looks at a new encryption technique that may be used to encrypt information on the cyberspace from illegal accessors. This new technique deploys randomly generated numbers to encrypt information that may travel over the web. Because this new technique employs random numbers for its encryption process, it will be very difficult to decrypt.

Index Terms— Random numbers, 2-Tail Reversed Cipher, Algorithm, Cryptography, Cyberspace

1 INTRODUCTION

According to the UK Government, Information security is: "the practice of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so [1]. Information systems need to be secure if they are to be reliable. Since many businesses are critically reliant on their information systems for key business processes. (e.g. webs items, production scheduling, transaction processing), security can be seen to be a very important area for management to get right

Information Security has to do with a way of keeping information especially those in transit from people who may want to intercept it for various reasons from doing that, but even if they do, such information would be meaningless to them. This can be achieved with the use of ciphers. The two major types of ciphers are the substitution and transposition ciphers. These ciphers are meant to encrypt information. In most cases, the information been encrypted are messages that are usually routed through the Internet where hardly identified people have access to such information. There are no doubts that among those people who can access information routed through the Internet are criminals. The researchers propose new encryption technique that uses randomly generated numbers to encrypt web information.

1.1 Aims and Objective

The aim of this research work is to dvelop a new encryption algorithm which would be used to conceal information that may be sent from source to destination. The objective is to deploy randomly generated numbers which would make any information encrypted using this new encryption algorithm very difficult to decrypt by those without the appropriate key.

2 LITERATURE REVIEW

Some of the works already carried out by some researchers are examined in this section. This is to ensure that the new encryption technique being proposed will overcome some of the problems associated with these encryption methods.

2.1 Substitution Cipher

Substitution ciphers are ciphers that are defined by some permutation of a plaintext alphabet. Every character of a plaintext string is consistently mapped to a single character of an output string using this permutation.Letter-substitution ciphers encode a document from a known language into an unknown writing system or an unknown encoding of a known writing system. This problem has practical significance in a number of areas, such as in reading electronic documents that may use one of many different standards to encode text [2].

2.2 Transposition Cipher

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. Transposition means rearranging the order of appearance of the elements of the plaintext. Transposition is also referred to as permutation.

The cipher can be made more secure by performing multiplerounds of such permutations [3].

2.3 Playfair Cipher

The Playfair cipher is a substitution cipher invented in 1854 by Charles Wheatstone. The name of the cipher as it is known in the cryptology literature comes from the name of the lord Playfair who strongly promoted the cipher. Playfair cipher is unlike a simple substitution cipher, which takes a message one letter at a time and replaces each letter with another letter, a Play fair cipher takes a message two letters at a time and replaces each pair of letters with another pair of letters[4].

2.4 Double Playfair Cipher

The Two-square cipher, also called double Playfair, is a manual symmetric encryption technique. It was developed to ease the cumbersome nature of the large encryp-

tion/decryption matrix used in the four-square cipher while still being slightly stronger than the (single-square) Playfair cipher. the The alphabet square is a five-by-five digram. The key phrase is first written without repeating any letters. The remaining letters of the alphabet are filled in an order.

The Double Playfair Cipher is an extension of the previously examined Playfair Cipher. The Double Playfair Cipher uses the same digraph substitution methodology with two 5x5 squares in place of one. It is orthodox to use a different keyword for each square [5].

3 2-TAIL REVERSED CIPHER

This consists of two tables. Each table is made up of 5 rows and 5 columns; hence there are 25 cells in each table. This is shown in table 1:

Table 1: Ten Random Integers

ric1	ric2	ric3	ric4	ric5
r1c1	r1c2	r1c3	r1c4	r1c5
r2c1	r2c2	r2c3	r2c4	r2c5
r3c1	r3c2	r3c3	r3c4	r3c5
r4c1	r4c2	r4c3	r4c4	r4c5
r5c1	r5c2	r5c3	r5c4	r5c5

Where i=0,1. . .5.

A cell is an intersection between a column and row. A cell in the table contains a letter of an English alphabet. Since there are 26 letters in the English alphabet, it then means that in order to contain the 26 letters of the alphabets, 2 letters of the alphabet are to be contained in one cell. Any of the letters adjacent to each other may be combined. However, the researchers chose to combine the letters I and J. Other letters such as U and V could also be combined in a cell. The two letters to be combined must be such that their occurrence in a word is not too common.

Like the Double Playfair Cipher, this 2-Tail Reversed Cipher makes use of two keywords. The first keyword may be arranged in the first table and the second keyword arranged in the second table. However, the first keyword may also be arranged in the second table and the second keyword arranged in the first table. The keywords may be any words, but the researchers have chosen two towns in Nigeria as keywords for the purpose of illustration. The choice of keywords are selected with the constrains that the letters to be combined in a cell are not contained in the keywords. For example if the letters I and J are to combined in a cell, then the choice of the towns Jos or Bauchi as keywords are not acceptable.

3.1 Structure of a 2-Tail Reversed Cipher Table

The choice of the name, 2-Tail Reversed Cipher is chosen by the researchers because of the arrangement of the letters of the alphabets in the tables.

The rules for the application of a 2-Tail Reversed Cipher are as below:

i. Choose a keyword.
ii. Arrange the keyword in a 5 x 5 table starting from the first cell in the table
iii. Fill the others cells in the table with the others letters of the alphabets starting with the last alphabet, Z and skipping any letter already contained in the chosen keyword.

To illustrate this, AKURE, a town in Nigeria may be used as shown in table 2 below:

Table 2: 2-Tail Cipher with AKURE as keyword

ric1	ric2	ric3	ric4	ric5
A	K	U	R	E
Z	Y	X	W	V
T	S	Q	P	O
N	M	L	I/J	H
G	F	D	C	B

In the second table, the same rules apply as above. The difference here is the keyword letters are arranged starting from the last cell in the table. The first letter of the keyword is entered in the last cell, r5c5, followed by r5c4. After entering the letters in the keyword, the remaining cells in the table are filled up with the remaining letters of the alphabet starting with the letter, A, followed by letter, B in that order skipping any letter already contained in the keyword. The letters are entered in ascending order, until the first cell of the table is reached. This is depicted in table 3 below with another town in Nigeria YOLA as a keyword:

Table 3: 2-Tail Cipher with YOLA as keyword

ric1	ric2	ric3	ric4	ric5
Z	X	W	V	U
T	S	R	Q	P
N	M	K	I/J	H
G	F	E	D	C
B	A	L	O	Y

4 RANDOM SEQUENCE GENERATOR

The random sequence developed by Mads [6] was depoyed to generate the random integers displayed in table 4 below:

Table 4: 100 Random Integers by Mads

RI	RI	RI	RI	RI
95	44	84	12	2
76	23	74	64	7
28	48	56	21	67
57	43	46	0	18
65	93	97	52	10
82	17	72	78	5
35	71	26	62	24
47	58	1	34	27
49	3	88	63	16
41	19	40	50	85
6	45	4	61	83
59	77	14	98	68
42	96	39	51	20
54	75	92	13	87
99	11	8	86	69
31	79	29	37	30
94	91	89	25	73
36	66	81	53	80
70	90	33	15	32
38	55	9	60	22

RI	RI	RI	RI	RI
66	17	9	13	29
70	97	3	14	80
83	95	32	44	75
62	26	90	63	74
25	77	65	96	72
41	1	58	2	61
20	78	10	30	37
93	22	87	99	71
82	33	76	21	54
94	31	68	98	53
43	38	67	57	15
8	47	59	16	40
1	45	51	24	39
81	69	42	92	36
35	50	34	23	27
4	28	48	87	19
60	49	6	86	18
91	55	46	64	12
50	73	89	85	7
0	52	79	88	5

In other to contribute to knowledge, the researchers decided rather than just apply the random integers generated by Mads as shown above embarked on developing a new algorithm that would generate similar random integers as above using a new technique. The algorithm is as shown below:

i. Develop a Random Generator
ii. Define an Empty List and the range for the random integers
iii. Use the Random Generator to generate any random integer
iv. Check if the random integer is within the defined range
v. If the random integer is within the range, then test if it is already in the list
vi. If it is within the range, but not yet in the list, place it in the list, otherwise, discard it.
vii. Check if the list is full
viii. If it is not yet full, go back to step iii
ix. Stop

The code to this algorithm is written in Visual Basic.

However, the developed Random Generator has the relation below:

$$rx = (rand + j + \exp(i) * j) \bmod m \quad (1)$$

where m is the modulus and has the value, 1023 (2^{10}-1) and i and j are loop variables whose range values are defined appropriately. Table 5 that follows is the result of executing the coded algorithm using the above relation.

Table 5 Random Integers Using
rx = (rand + j + exp(i) * j) mod m

After the generation of the 100 random integer sequences, the next step toward the encryption process is how 25 of them would be selected for the encryption model, bearing in mind that there are only 25 letters to be used. Again, the researches visited the Encyclopedia of Online Integer Sequences where many functions are used to generate a non-arithmetic progression sequences. These functions differ from the arithmetic progression sequence in that there is no common difference between the terms in the sequence. This will in turn be a "mountain" whose top may not easily be reached by code breakers. This function (A032721) by Geest in 1998 that is located in Encyclopedia of Online Integer Sequences whose page is displayed in figure 1 that follows [7]:

Figure 1: A032721 Function for Non-Arithmetic Progression Sequence

The first 25 terms of the sequence is shown below:
5,6,8,12,15,17,21,29,32,33,35,39,44,45,50,51,54,56,59,63,665,78, 81,87,93,

However, the mathematical details of this function are not discussed by the researchers. In any case, it will be good to mention that there exist some conditions that surround this function. One of the conditions is that the numbers in the sequence is such that the number, n should produce a prime number when inserted in-between the numbers 4 and 7 with offset of 0. The following are the advantages of the non-arithmetic progression sequence over the arithmetic progres-

sion sequence:

i. There is no common difference between the terms in the sequence.
ii. The sequence is more difficult to compute when compared to their arithmetic progression counterpart, which can easily be computed once the first term and the common difference is known.

Although, there are many other functions that may be found in that Encyclopedia of Online Integer Sequences web page, the choice of the function to employ should conform to the following criteria:
i. The value of the 25th term of the non-arithmetic progression sequence should not exceed the
maximum value in the range of the random integer sequence generated.
ii. The values in the non-arithmetic progression sequence should be evenly distributed through the range of the generated random integer sequence.
iii. The selection of the 25 random integer numbers from the generated sequence should be based on the values of the first 25 terms of the non-arithmetic progression sequence.

In order to use non-arithmetic sequence that would conform to the above criteria, the researchers again embarked on developing a new algorithm that would best meet the purpose of this work [8]. The algorithm is written down below:

i. Develop a Non-Arithmetic Progression Sequence Generator
ii. Define a loop range
iii. Apply the Non-Arithmetic Sequence Generator
iv. Check if still within the loop range
v. If still within the loop range, go back to step iii
vi. Stop

Also, the program is coded in Visual basic. The generator has the relation shown below:

x = (abs(int(3 / exp(2/3) * n – (n/5) + ((n ^ (3/2))))) + 1) (2)

where n is the loop variable.

Table 6 shows the application of the described generator to obtain the first 25 terms of the sequence:

Table 6: Non-Arithmetic Progression Sequence Using x=(abs(int(3 / exp(2/3) * n – (n/5) + ((n ^ (3/2))))) + 1)

S/N	X
1	1
2	2
3	3
4	5
5	7
6	9
7	12
8	15
9	18
10	22
11	25
12	29
13	34
14	38
15	42
16	47
17	52
18	57
19	63
20	68
21	74
22	80
23	86
24	92
25	98

Looking at table 6 above, one can deduce that the first 25 terms of the sequence best meet all the three requirements stated earlier in this work. Table 7 that follow shows Non-arithmetic progression sequence and their corresponding random integers:

Table 7: Non-arithmetic progression sequence and their corresponding random integers

S/N	X	RX
1	1	66

2	2	70
3	3	83
4	5	25
5	7	20
6	9	82
7	12	8
8	15	35
9	18	91
10	22	97
11	25	77
12	29	33
13	34	69
14	38	55
15	42	3
16	47	10
17	52	59
18	57	6
19	63	44
20	68	99
21	74	92
22	80	88
23	86	61
24	92	40
25	98	12

Finally, table 8 is obtained by assigning the 25 letters of the English alphabet after combining two letters of I and J into a single cell:

Table 8: Non-arithmetic progression sequence, their corresponding random integers and alphabets

S/N	X	RX	Alphabet
1	1	66	A
2	2	70	B
3	3	83	C
4	5	25	D
5	7	20	E
6	9	82	F
7	12	8	G
8	15	35	H
9	18	91	I/J
10	22	97	K
11	25	77	L
12	29	33	M
13	34	69	N
14	38	55	O
15	42	3	P
16	47	10	Q
17	52	59	R
18	57	6	S
19	63	44	T
20	68	99	U
21	74	92	V
22	80	88	W
23	86	61	X
24	92	40	Y
25	98	12	Z

5. PROCEDURE FOR ENCIPHERING INFORMATION

Using this method to encipher information involves the steps below:

i. Form a table that will contain the 100 generated random integers.
ii. Form another table that will contain first 25 terms of integer sequence from the chosen function, the 25 letters of the English alphabets, and their corresponding random sequence from the previous table.
iii. Choose a period, which is simply the number of letters that the information to be enciphered can be broken into.
iv. Break the information into groups based on the period.
v. Arrange the groups accordingly. This is done by placing the second group below the first, the forth below the third, etc.
vi. If the last two groups do not contain the same number of letters as the other groups, break it into equal period and use x to fill the last if the group has odd number of letters. For example, if 7 letters are contained in the last two group where a period of 6 was selected, then the first group should contain 4 letters whereas the second group should contain the remaining 3 letters and an x will be added to make it 4.
vii. Use the corresponding random integers to represent the letters contained in the information to be enciphered.

6. CASE STUDY EXAMPLE

At this juncture, an example will be used to illustrate how a 2-Tail Reversed Cipher works. Assuming there is a security

report from security agents to the Federal Government of Nigeria on plans to embark on crisis in a particular locality within the country by some group of people. If the content of the information to be generated by the security agents to the Federal Government reads:

MISCREANTS PLANS FRESH CRISIS IN PANKSHIN. FORESTALL OCCURRENCE IMMEDIATELY.

Following the steps outlined earlier this information can be enciphered by:

i. Form a table as in table 8 using the 100 generated random integers:
ii. Form another table that will contain the first 25 terms of the chosen non-arithmetic progression sequence, the 25 letters of the English alphabets and their corresponding random integer.
iii. Choose any period say, 5.
iv. Break the entire information into groups of 5 letters using the corresponding integer sequence. This is shown below:

MISCR EANTS PLANS FRESH CRISI
SINPA NKSHI NFORE STALL OCCUR
RENCE IMMED IAT ELY

The last two groups are broken down into a period of 3 letters each.
The above grouping is then converted as below using their corresponding random integers:

3391068359 2066699906 0377666906 8259200635
8359910691 0691690366 6997063591 6982555920
0699667777 5583839259 5920698320 9133332025
916699 207740

v. Arrange the groups in pairs placing the second below the first, fourth below the third etc as shown below:

MISCR PLANS CRISI NKSHI STALL
EANTS FRESH SINPA NFORE OCCUR
RENCE IAT
IMMED ELY

This is then translated as shown below using the generated random numbers:

3391068359 0377666906 8359910691 69970635
2066699906 8259200635 0691690366 69825559
0699667777 5920698320 916699
5583839259 9133332025 207740

vi. To encipher the information, choose any two towns as keywords. The towns to be chosen in this example are Gombe and Ekpoma.
vii. Arrange the first keyword in the first table using the corresponding random integer values and fill up the other cells in the table with the remaining integer values corresponding to the letters of the alphabets in descending order as shown in table 9 which follows:

Table 9: 2-Tail Cipher with GOMBE as keyword

ric1	ric2	ric3	ric4	ric5
G	O	M	B	E
Y	Y	X	W	V
U	T	S	R	Q
P	N	L	K	I/J
H	F	D	C	A

Table 9 above will result to table 10 below substituting the corresponding random integer values.

Table 10: Random Integer values of table 9

ric1	ric2	ric3	ric4	ric5
08	55	33	70	20
12	40	61	88	92
99	44	06	59	10
03	69	77	97	91
35	82	25	83	66

The second keyword is arranged in the second table starting from the last cell and filling up the other alphabets in the table in ascending order as indicated in table 11 below

Table 11: 2-Tail Cipher with EKPOMA as keyword

ric1	ric2	ric3	ric4	ric5
Z	Z	X	W	V
U	T	S	R	Q
N	L	I/J	H	G
F	D	C	B	A
M	O	P	K	E

Similarly, table 11 will produce the corresponding table 12 shown below:

Table 12: Random Integer values of table 11

ric1	ric2	ric3	ric4	ric5
12	40	61	88	92
99	44	06	59	10
69	77	91	35	08
82	25	83	70	66
33	55	03	97	20

Encipher each vertical pair of 2 digit numbers as in (v) above by observing the rules below:

(1) Take the 2-digit number at the bottom of the pair from table 10 and the other 2-digit number at the top in the pair from table 12.
(2) Replace each of the 2-digit number in the pair with the 2-digit numbers above it in tables (10 and 12 respectively), wrapping around if necessary.

The information from the security agents to the Federal Government of Nigeria can be enciphered as in table 13 below by placing tables (10 and 12) side by side below using the corresponding random integer values as follows:

Table 13: Tables 10 and 12 placed side by side

	Table	10				Table	12		
ric1	ric2	ric3	ric4	ric5	ric1	ric2	ric3	ric4	ric5
08	55	33	70	20	12	40	61	88	92
12	40	61	88	92	99	44	06	59	10
99	44	06	59	10	69	77	91	35	08
03	69	77	97	91	82	25	83	70	66
35	82	25	83	66	33	55	03	97	20

The information when arranged in groups form a 2-digit vertical pairs of numbers as shown below:

3391068359 0377666906 8359910691 6997063591
2066699906 8259200635 0691690366 6982555920
0699667777 5920698320 916699
5583839259 9133332025 207740

The result of the application of rules 1 and 2 is shown below:

2033=>6682, 6691=>9106, 6906=>4461, 9983=>1291,
0659=>6188, 8203=>6983, 5977=>8844, 2066=>6608,
0669=>6199, 3506=>0361, 0683=>6191, 9159=>1088,
6991=>4406, 0306=>9961, 6691=>9106, 6969=>4499,
8297=>6970, 5506=>8261, 5935=>8859, 2091=>6606,
5506=>8261, 8399=>9712, 8366=>9708, 9277=>2044,
5977=>8844, 9159=>1088, 3320=>2592, 3369=>2599,
2083=>6691,2520=>7766,2091=>6606,7766=>0608,
4099=>5572

Hence, the information when enciphered produces the vertical pair of ciphertext made up of numbers as below:

6682910644 6112916188 6983884466 0861990361
0699619106 4499697082 6188596606 82619712 97
6191108844 1088259225 660606
0820448844 9966917766 085572

The above ciphertext numbers will produce the information below when rearranged accordingly:

6682910644 4499697082 6112916188 6188596606
6983884466 82619712 97 0861990361 0820448844
6191108844 1088259225 0699619106 9966917766
660606 085572

7. OKIKE'S 2-TAIL REVERSED CIPHER DECRYPTION

In order for the encrypted message to be decrypted, the procedure for the encryption is carried out in a reverse order. The message recipient must have access to both the keywords and the random numbers generated which is used for the encryption process for a successful decryption process to be achieved. This information could be sent through a different route to the recipient. In order for the German receivers to be able to decrypt an encrypted text, which the enemy was not supposed to be able to do, the German receivers needed additional information. This was provided through a codebook or a monthly list of daily keys, distributed under high security to all the relevant German participants in the war [9].

8. CONCLUSION

There is no doubt that the new developed scheme follows a substation cipher methodology, but the weakness of the substation cipher which includes statistical attacks using the knowledge of English alphabets have been eliminated through the introduction of generated random numbers. To decipher information decrypted using this methodology requires additional effort of 100! (factorial) x 100! (factorial) due to the random numbers generated and deployed for the encryption.

Refernces

[1] UK Online for Business, Introduction to Information System Security, 2005. http://www.tutor2.net/default.asp

[2] E. Corlet and G. Penn. An Exact A* Method for Deciphering Letter-Substitution Ciphers, 2010. http://aclweb.org/anthology/P/P10/P10-1106.pdf

[3] A. Kak, Classical Encyption Techniques, 2013. https://engineering.purdue.edu/kak/compsec/

[4] H. K. Obayes, Suggested Approach to Embedded Playfair Cipher Messages in Digital Image, 2013. http://www.ijera.com/papers/Vol3_issue5/DY35710714.pdf

[5] D. Abbott, Cipher Cross-off List, 2013. https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/Cipher_Cross-f_List#Playfair_Cipher_.28Double.29

[6] H. Mads, True Random Numbers, 2002. http://www.random.org/mads,

[7] P. Geest, Integer Sequence. http://www.research.att.com/project

[8] B. Okike, New Encryption Techniques Using Random Generators, Ph. D. Thesis, 2005.

[9] C. Christensen , I. Peterson, The German cipher machine Enigma, 2007. http://www.matematiksider.dk/enigma_eng.html