DATA ENCRYPTION AND DECRYPTION USING ANZL ALGORITHM

Artan Luma and Nderim Zeqiri
CST, SEE University, Ilindenska bb, Tetovo, Macedonia

Keywords: Cryptography, Algorithm, Security, ANZL.

Abstract: What is the ANZL Algorithm? It is a genuine result of our work which is theoretically and practically proved. By using the ANZL Algorithm, we can test whether a given number x belongs to Lucas's series. It can also be used to find a sequence of Lucas's numbers, starting from any number x. If a given number x, completes the relation $5 \cdot x^2 \pm 4 = \lambda^2$, we can say that it is a Lucas number and we mark it as $L_n = x$. From the pair of numbers (L_n, λ), we can find the preceding L_{n-1} and the succeeding L_{n+1} e L_n. Based on these three elements of Lucas's series, we can create the key for data encryption and decryption.

1 ALGORITHM ANZL

Based on Fibonacci series:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \dots \qquad (1)$$

We will be able to get the elements of Lucas's series using:

$$L_{n-m-1} = \frac{F_n \pm F_{n-2\cdot m}}{F_{n-m}} \qquad (2)$$

Where $n, m \in N$ and $m \geq 1, n > 2 \cdot m$. If m, is even, we use $+$, if m, is odd, the we use $-$. For $m = 1$ and $n = 3$, we have:

$$L_1 = \frac{F_3 - F_1}{F_2} = \frac{2-1}{1} = 1 \qquad (3)$$

For $m = 2$ and $n = 5$, we have:

$$L_2 = \frac{F_5 - F_1}{F_3} = \frac{5+1}{2} = 3 \qquad (4)$$

For $m = 3$ and $n = 7$, we have:

$$L_3 = \frac{F_7 - F_1}{F_4} = \frac{13-1}{3} = 4 \qquad (5)$$

For $m = 4$ and $n = 9$, we have:

$$L_4 = \frac{F_9 - F_1}{F_5} = \frac{34+1}{5} = 7 \qquad (6)$$

For $m = 5$ and $n = 11$, we have:

$$L_5 = \frac{F_{11} - F_1}{F_6} = \frac{89-1}{8} = 11 \qquad (7)$$

Based on this general formula, using Fibonacci's numbers we will generate Lucas's series of numbers:

$$1, 3, 4, 7, 11, 18, 29, \dots \qquad (8)$$

Theorem 1: For Lucas's seires L_n, $n \in N$, we have:

$$L_{n-1} + L_n = L_{n+1}, \quad n > 1 \qquad (9)$$

Theorem 2: For odd members of Lucas's series L_n, $n \in N$, we have:

$$L_{2\cdot n-1} \cdot L_{2\cdot n+1} = L_{2\cdot n}^2 + 5 \qquad (10)$$

Theorem 3: For even members of Lucas's series L_n, $n \in N$, we have:

$$L_{2\cdot n} \cdot L_{2\cdot n+2} = L_{2\cdot n+1}^2 - 5 \qquad (11)$$

With the help of Theorems 2 and 3 we can find the algorithm to test if a number belongs to Lucas's series or not.

$$L_{2\cdot n-1} \cdot L_{2\cdot n+1} = L_{2\cdot n}^2 + 5 \qquad (12)$$

From Theorem 1, $L_{2\cdot n}$, we can write:

$$L_{2\cdot n} = L_{2\cdot n+1} - L_{2\cdot n-1} \qquad (13)$$

As a result:

$$L_{2\cdot n}^2 = (L_{2\cdot n+1} - L_{2\cdot n-1})^2 \qquad (14)$$

If:

$$(L_{2\cdot n+1} - L_{2\cdot n-1})^2 = L_{2\cdot n+1}^2 - 2 \cdot L_{2\cdot n+1} \cdot L_{2\cdot n-1} + L_{2\cdot n-1}^2 \qquad (15)$$

$$(L_{2\cdot n+1} + L_{2\cdot n-1})^2 = L_{2\cdot n+1}^2 + 2 \cdot L_{2\cdot n+1} \cdot L_{2\cdot n-1} + L_{2\cdot n-1}^2 \qquad (16)$$

Now, the expression $(L_{2\cdot n+1} - L_{2\cdot n-1})^2$, can be written as:

$$(L_{2\cdot n+1} - L_{2\cdot n-1})^2 = (L_{2\cdot n+1} + L_{2\cdot n-1})^2 - 4 \cdot L_{2\cdot n+1} \cdot L_{2\cdot n-1} \qquad (17)$$

Luma A. and Zeqiri N. (2008).
DATA ENCRYPTION AND DECRYPTION USING ANZL ALGORITHM.
In *Proceedings of the Tenth International Conference on Enterprise Information Systems - ISAS*, pages 220-223
DOI: 10.5220/0001688102200223

So that we have:

$$L_{2\cdot n}^2 = (L_{2\cdot n+1} - L_{2\cdot n-1})^2 = (L_{2\cdot n+1} + L_{2\cdot n-1})^2 - 4 \cdot L_{2\cdot n+1} \cdot L_{2\cdot n-1} \quad (18)$$

From Theorem 2:

$$L_{2\cdot n}^2 = (L_{2\cdot n+1} + L_{2\cdot n-1})^2 - 4 \cdot (L_{2\cdot n}^2 + 5) \quad (19)$$

$$L_{2\cdot n}^2 = (L_{2\cdot n+1} + L_{2\cdot n-1})^2 - 4 \cdot L_{2\cdot n}^2 - 20 \quad (20)$$

$$5 \cdot L_{2\cdot n}^2 + 20 = (L_{2\cdot n+1} + L_{2\cdot n-1})^2 \quad (21)$$

$$5 \cdot L_{2\cdot n}^2 + 20 = (L_{2\cdot n+1} + L_{2\cdot n-1})^2 = \Omega^2 \quad (22)$$

Ω is the sum of adjacent members of $L_{2\cdot n}$, of Lucas's series. We can prove in the same way that:

$$5 \cdot L_{2\cdot n+1}^2 - 20 = (L_{2\cdot n} + L_{2\cdot n+2})^2 = \Psi^2 \quad (23)$$

Ψ is the sum of adjacent members of $L_{2\cdot n+1}$. Based on the above-mentioned relations, we can test wthether a given number x, belongs to Lucas's series. We can also use this to find a sequence of Lucas's numbers starting from any number x. If x, completes the relation $5 \cdot x^2 \pm 20 = \lambda^2$, we cab say that it is Lucas's number and we mark it as $x = L_n$. From the pair (L_n, λ), we can also find the preceeding and succeeding numbers L_{n-1} and $L_{n+1}$of L_n.

$$L_{n-1} = \frac{\lambda - L_n}{2} \quad \text{and} \quad L_{n+1} = \frac{\lambda + L_n}{2} \quad (24)$$

Since we have found L_{n-1}, L_n, L_{n+1}, we can find the whole series of Lucas's numbers:

$$2, 1, 3, 4, 7, 11, \cdots, L_{n-1}, L_n, L_{n+1}, \cdots \quad (25)$$

Table 1.

x	λ	L_{n-1}	L_n	L_{n+1}
1	5	2	1	3
2	0	-1	2	1
3	5	1	3	4
4	10	3	4	7
7	15	4	7	11
11	25	7	11	18
18	40	11	18	29
29	65	18	29	47

We will now see how we can encrypt or decrypt a message by using the ANZL algorithm to create the key. Let p be the message (plaintext), and k the key. c is the encrypted message (ciphertext). If we want to encrypt a message, we will use this formula:

$$c = p + k \pmod{26} \quad (26)$$

If we want to decrypt a text, we will use:

$$p = c - k \pmod{26} \quad (27)$$

We will now show how to create the key. First of all, we choose a number x and this number is put in the ANZL algorithm to test whehter it belongs to Lucas's series or not. The formula of the ANZL algorithm which tests the number $x \in N$, is:

$$5 \cdot x^2 \pm 4 = \lambda^2 \quad (28)$$

If x, meets this condition, then $F_n = x$, which means that x, is a number in the Lucas's series. Since F_n and λ, we can easily find F_{n-1} and F_{n+1}. These two elements of Lucas's series are found by using the formulas:

$$L_{n-1} = \frac{\lambda - L_n}{2} \quad \text{and} \quad L_{n+1} = \frac{\lambda + L_n}{2} \quad (29)$$

Now that we have found Lucas's elements L_{n-1}, L_n, L_{n+1}, we can construct the whole series if Lucas's numbers:

$$0, 1, 1, 2, 3, 5, 8, \cdots, L_{n-1}, L_n, L_{n+1}, , \cdots \quad (30)$$

We will now design a scheme to create the key. In order to do this, the most important are the levels.

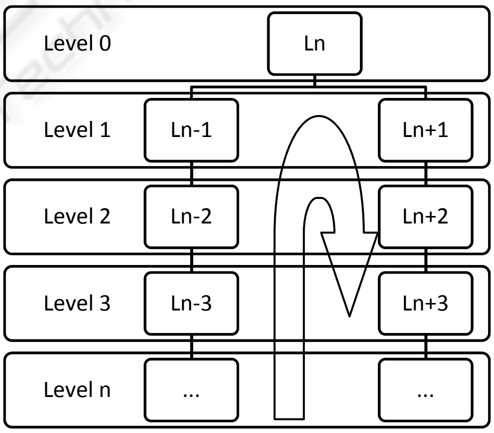

Figure 1.

If we want to create a key with level 2, then its keys will be:

$$L_{n-2}, L_{n-1}, L_n, L_{n+1}, L_{n+2} \quad (31)$$

This means that the key will consist of five elements. The number of elements is determined by this formula:

$$N = 2 \cdot m + 1 \quad (32)$$

N, is the number of elements of the key and m, are the levels. Let's have a plaintext now: South East

European University which we want to encrypt. First of all we have to have $x \in N$, so that it meets the condition of the ANZL algorithm:

$$5 \cdot x^2 \pm 4 = \lambda^2 \quad (33)$$

For $x = 8$, we will get:

$$5 \cdot 8^2 + 4 = 324 = 18^2 \quad (34)$$

This means that the condition of the ANZL algorithm has been met so that we have $L_n = 8$ and $\lambda = 18$. Knowing the pair $(x, \lambda) = (8, 18)$, we will find the preceeding and succeeding numbers of $L_n = 8$:

$$L_{n-1} = \frac{\lambda - L_n}{2} \quad \text{and} \quad L_{n+1} = \frac{\lambda + L_n}{2} \quad (35)$$

$$L_{n-1} = \frac{25-11}{2} = \frac{14}{2} = 7 \quad (36)$$

$$L_{n+1} = \frac{25+11}{2} = \frac{36}{2} = 18 \quad (37)$$

After we have found these three elements of Lucas's series: L_{n-1}, L_n, L_{n+1}, we will design the scheme of creating the key.

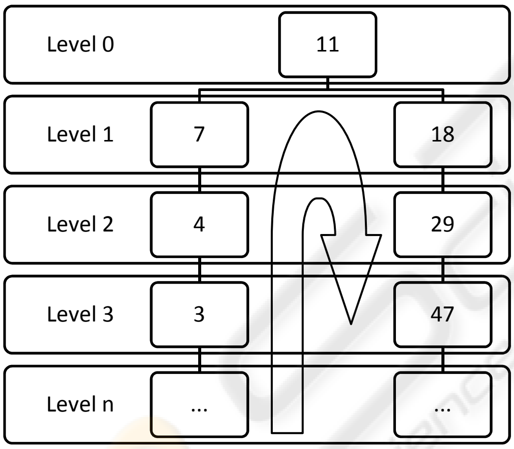

Figure 2.

If we decide to create a Level 2 key që do të thotë $m = 2$, we get:

$$N = 2 \cdot m + 1 = 2 \cdot 2 + 1 = 4 + 1 = 5 \quad (38)$$

This means that the key will consist of five elements:

$$4,\ 7,\ 11,\ 18,\ 29 \quad (39)$$

The text is now being converted into numbers. In order to do this we use the Table 1:

We get the text: South East European University and we convert it into numbers.

Table 2.

a	b	c	d	e	f	g
0	1	2	3	4	5	6
h	i	j	k	l	m	n
7	8	9	10	11	12	13
o	p	q	r	s	t	u
14	15	16	17	18	19	20
v	w	x	y	z		
21	22	23	24	25		

Table 3.

s	o	u	t	h	e	a	s
18	14	20	19	7	4	0	18
t	e	u	r	o	p	e	a
19	4	20	17	14	15	4	0
n	u	n	i	v	e	r	s
13	20	13	8	21	4	17	18
i	t	y					
8	19	24					

In order to encrypt the message, we use:

$$c = p + k \pmod{26} \quad (40)$$

The key is:

$$4,\ 7,\ 11,\ 18,\ 29 \quad (41)$$

We take the key and we put it into the message which we want to encrypt:

Table 4.

s	o	u	t	h	e	a	s
18	14	20	19	7	4	0	18
4	7	11	18	29	4	7	11
22	21	5	11	10	8	7	3
W	V	F	L	K	I	H	D
t	e	u	r	o	p	e	a
19	4	20	17	14	15	4	0
18	29	4	7	11	18	29	4
11	7	24	24	25	7	7	4
L	H	Y	Y	Z	H	H	E
n	u	n	i	v	e	r	s
13	20	13	8	21	4	17	18
7	11	18	29	4	7	11	18
20	5	5	11	25	11	2	10
U	F	F	L	Z	L	C	K
i	t	y					
8	19	24					
29	4	7					
11	23	5					
L	X	F					

If want to send this encrypted message to anyone, apart from the message itself, we also need to send the pair of numbers $(L_n, m) = (11, 2)$. The person receiving the message can decrypt it by finding first

λ and then the key. Based on the ANZL algorithm, we find the values of λ:

$$5 \cdot x^2 \pm 4 = \lambda^2 \tag{42}$$

For $x = 11$, we get:

$$5 \cdot 11^2 + 20 = 625 = 25^2 \tag{43}$$

$\lambda = 25$. Knowing $(x,\ \lambda) = (11,\ 25)$, we will find the preceeding and the succeeding numbers $L_n = 11$:

$$L_{n-1} = \frac{\lambda - L_n}{2} \quad \text{and} \quad L_{n+1} = \frac{\lambda + L_n}{2} \tag{44}$$

$$L_{n-1} = \frac{25-11}{2} = \frac{14}{2} = 7 \tag{45}$$

$$L_{n+1} = \frac{25+11}{2} = \frac{36}{2} = 18 \tag{46}$$

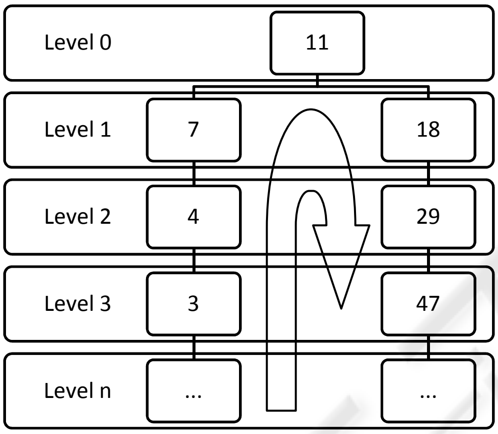

Figure 3.

Table 5.

W	V	F	L	K	I	H	D
22	21	5	11	10	8	7	3
4	7	11	18	29	4	7	11
18	14	20	19	7	4	0	18
s	o	u	t	h	e	a	s
L	H	Y	Y	Z	H	H	E
11	7	24	24	25	7	7	4
18	29	4	7	11	18	29	4
19	4	20	17	14	15	4	0
t	e	u	r	o	p	e	a
U	F	F	L	Z	L	C	K
20	5	5	11	25	11	2	10
7	11	18	29	4	7	11	18
13	20	13	8	21	4	17	18
n	u	n	i	v	e	r	s
L	X	F					
11	23	5					
29	4	7					
8	19	24					
i	t	y					

After having found these three elements of Lucas's series: L_{n-1}, L_n, L_{n+1}, we will design the scheme for creating the key.

We know that Level of key is 2, which means $m = 2$, so that:

$$N = 2 \cdot m + 1 = 2 \cdot 2 + 1 = 4 + 1 = 5 \tag{47}$$

This means thta the key will consist of five elements of Lucas's series:

$$4,\ 7,\ 11,\ 18,\ 29 \tag{48}$$

Having the key, is quite easy to encrypt the text by using:

$$p = c - k \pmod{26} \tag{49}$$

2 CONCLUSIONS

The aim of the ANZL Algorithm is to test whether a number x belongs to Lucas's series or not. If it does, then it is very easy to find the preceeding and succeeding numbers L_{n-1}, L_n, L_{n+1}.This algorithm can also be used for purposes of data encryption and decryption in terms of creating the keys.

REFERENCES

Introduction to cryptography: with coding theory by Wade Trappe; Lawrence C Washington, Publisher: Upper Saddle River, N.J.: Pearson Prentice Hall, ©2006, ISBN: 0131862391

Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition (Paperback) by Bruce Schneier; Paperback: 758 pages; Publisher: Wiley; 2nd edition (October 18, 1996); Language: English; ISBN-10: 0471117099; ISBN-13: 978-0471117094

Modern Cryptography: Theory and Practice (Hardcover)by Wenbo Mao; Hardcover: 740 pages; Publisher: Prentice Hall PTR; 1st edition (July 25, 2003); Language: English; ISBN-10: 0130669431; ISBN-13: 978-0130669438

Practical Cryptography (Hardcover) by Niels Ferguson, Bruce Schneier; Hardcover: 432 pages Publisher: Wiley (April 17, 2003); Language: English; ISBN-10: 047122894X; ISBN-13: 978-0471228943

Schneier's Cryptography Classics Library: Applied Cryptography, Secrets and Lies, and Practical Cryptography (Paperback) by Bruce Schneier; Paperback: 1664 pages; Publisher: Wiley (October 22, 2007); Language: English; ISBN-10: 0470226269; ISBN-13: 978-0470226261.