Düzce University Journal of Science & Technology

Research Article

Encryption and Decryption of the Data by Using the Terms of the Lucas Series

Mehmet DUMAN [a,*], Merve GÜNEY DUMAN [b]

[a] *Faculty of Engineering, Department of Electrical and Electronics Eng., Düzce University, Düzce, TURKEY*
[b] *School of Eng. and Natural Sciences, Department of Basic Sciences, Altınbaş University, İstanbul, TURKEY*
* *Corresponding author's e-mail address: mehmetduman@duzce.edu.tr*
DOI: 10.29130/dubited.825315

ABSTRACT

The sequence, whose initial condition is 2 and 1, obtained by summing the two terms preceding it, is called the Lucas sequence. The terms of this series continue as 2, 1, 3, 4, 7, 11, 18, 29, ... respectively. The features of the Lucas sequence have been studied in many projects in the literature and many studies have been done on Lucas series in applied sciences. Cryptology is the science that deals with encrypting data, transferring it securely from one point to another, and converting the encrypted data to the previous one. It includes cryptography and cryptoanalysis. Different encryption-decryption methods have been developed to ensure the security of the data from the past to the present. Some of these are Caesar, Affine, Vigenere and RSA. There are two types of encryption systems in cryptology. The first one is symmetric (secret key) encryption and the another one is asymmetric (public key) encryption. In this study; using the features of the Lucas sequence, studies on cryptology, which deals with the correct encryption, transfer and decryption of data, have been carried out and an example of cryptology algorithm has been given. With Lucas cipher, the letters in the alphabet and the space character are each mapped to the terms of the Lucas sequence. Later, starting from the first term of the Lucas sequence, the encryption was strengthened by adding Lucas terms. As a result, the text to be encrypted has been turned into a symbolic representation of the numbers. Then, the necessary information for deciphering the text which is encrypted with numbers is given.

Keywords: *Lucas numbers, Cryptology, Information security, Cryptography*

Lucas Dizisinin Terimleri Kullanılarak Verinin Şifrelenmesi ve Şifrenin Çözülmesi

ÖZET

Başlangıç şartı 2 ve 1 olan ve sonraki terimleri kendinden önceki iki terimin toplanmasıyla elde edilen diziye Lucas dizisi denir. Uygulamalı bilimlerde Lucas dizisi ile ilgili birçok çalışma yapılmıştır. Kriptoloji; verinin şifrelenmesi, güvenli bir şekilde bir noktadan başka bir noktaya transfer edilmesi ve şifrelenen verinin birebir önceki haline getirilmesi ile ilgilenen bilim dalıdır. Kriptoloji; kriptografi ve kriptoanalizi içerir. Geçmişten bugüne kadar verinin güvenliğini sağlamak amacıyla farklı kriptolama yöntemleri geliştirilmiştir. Bunlardan bazıları Sezar (Caesar), Affin, Vigenere ve RSA algoritmalarıdır. Kriptolojide iki çeşit şifreleme sistemi vardır. Birincisi simetrik (gizli anahtarlı) şifreleme diğeri ise asimetrik (açık anahtarlı) şifrelemedir. Bu çalışmada; Fibonacci dizisinin terimlerinden yararlanarak yeni bir şifreleme metodu geliştirildi. Bu şifreleme ile alfabemizdeki harflerin her biri Fibonacci dizisinin terimleri ile eşleştirildi. Böylece, şifrelenmek istenen metin, sayıların sembolik gösterimi haline getirildi. Şifreli metin oluşturulurken küçük harfler dikkate alındı. Daha sonra da sayılarla şifrelenmiş metnin deşifre edilmesi için gerekli olan dönüşüm hakkında bilgiler verildi.

Anahtar kelimeler: *Lucas sayıları, Kriptoloji, Bilgi güvenliği, Kriptografi*

Received: 13/11/2020, Revised: 10/02/2021, Accepted: 21/02/2021

I. INTRODUCTION

It has been very important to ensure the security of data from past to present and its importance is increasing day by day. New studies are constantly being made to ensure data security. Encryption methods are used in many fields such as military, engineering and health in order to counterwork the information from falling into the hands of black hackers. As the risk increases, more tight precautions are taken to protect important information. For this, many different encryption techniques have been developed. Even the course of history has changed with some encryption techniques used in history. Therefore; cryptology has been popular since its inception. In the future, it will continue to be a very important issue.

The first known cryptological document BC is the Rosetta tablet that was estimated to be written in 1900 [1]. The Enigma device used by the Germans during World War II between 1940 and 1944 gave the Germans superiority in the military field. It is thought that the course of the war changed after the password of Enigma was broken.

There are two types of encryption systems. The first is symmetric (secret key) encryption and the other is asymmetric (public key) encryption. Although the key is known in encryption with public keys, it is not possible to crack the password without performing a complex mathematical operation. It requires a lot of processing. In private key ciphers, the key is directly decrypted when it is received by hackers. So it must be protected very well.

Different encryption methods have been developed to ensure the security of the data from the past to the present. Some of these are Caesar (Caesar), Affin, Vigenere, block encryption and RSA. While some of the ciphers are simple enough to be deciphered with paper and pencil, some ciphers can only be analyzed analytically.

In 1553, the Vigenere cipher is known to be developed by Bellaso. This cipher is a method of encrypting alphabetic text by using a keyword. The encryption method used in is called multi-alphabet encryption. A keyword is selected. Each letter of the text to be encrypted is shifted by the number equivalent of the letter in the keyword. Then, it is arranged, if necessary, according to the modular arithmetic. For more information on cryptology, refer to references [1-11].

In 1202, Fibonacci published his modern decimal number system, known as Arab-Indian numbers, in his book “Liber Abaci”. Moreover, in this book, the increase problem of a rabbit family in a closed environment is mentioned. The number sequence that shows the increase in the population of this rabbit family is called Fibonacci [12-16]. Later, Lucas sequences were initiated by changing only the initial conditions with a similar way.

Many studies have been done in different fields related to Lucas and Fibonacci numbers. For more information on Lucas, refer to references [17-21].

II. DEFINITIONS, THEOREMS AND METHODS

Lucas series

$$L_0 = 2,\ L_1 = 1 \text{ and } n \geq 2; L_n = L_{n-1} + L_{n-2} \quad (1)$$

is defined by the recurrence relation. L_n number is called n. Lucas number. The terms of this series are 2, 1, 3, 4, 7, 11, 18, 29, ... respectively.

Let’s improve our method:

A. FOR ENCRYPTION (E)

E1) Space character is numbered 26. All letters in the alphabet are numbered from 0 to 25, respectively. The number equivalent of the letters is given in Table 1.

Table 1. *Numbered letters starting at 2*

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	24	24	25

E2) Lucas numbers, corresponding to the numbers in which the letters of the alphabet match, are obtained. The equivalent of the Lucas number of letters is given in Table 2, each with 6 digits.

Table 2. *Matching letters and space char. with Lucas numbers*

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
L_0	L_1	L_2	L_3	L_4	L_5	L_6	L_7	L_8
000002	000001	000003	000004	000007	000011	000018	0000029	000047
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
L_9	L_{10}	L_{11}	L_{12}	L_{13}	L_{14}	L_{15}	L_{16}	L_{17}
000076	000123	000199	000322	000521	000843	001364	002207	003571
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**Space**
L_{18}	L_{19}	L_{20}	L_{21}	L_{22}	L_{23}	L_{24}	L_{25}	L_{26}
005778	009349	015127	024476	039603	064079	103682	167761	271443

We wrote the numbers in this encryption model as 6 digits. Because the largest number of Lucas to be used is the 6-digit $L_{26} = 271443$ number. Therefore, a maximum number of $6n$ digits correspond to a text with the letter n. We can show this encryption as Lucas-6. However, at least 7-digit numbers may occur when Lucas numbers are added to the text to be encrypted that contains more than 28 characters, similar to Vigenere encryption. In this case, if each letter is not written with more digits, an error occurs. So the model can be named Lucas-x to show the number of digits where x is required. For example, if each character has 8 digits, it can be shown as Lucas-8.

E3) Lucas numbers are added similar to Vigenere encryption. Lucas number of each letter and space chac. are obtained. Later, the number of Lucas is added to each character, starting with L_0.

E4) The resulting numbers are combined.

E5) After removing the zeros from the left of the number, the text is encrypted with the numbers and encryption is completed. For example; let's encrypt the 5-letter word "LUCAS" with Lucas-6. Since the text to be encrypted has 5 letters, Table 2 is used.

For example;

E1) According to Table 1, the letters of the word "LUCAS" correspond to the numbers "11, 20, 2, 0, 18", respectively.

E2) Lucas numbers that should be calculated are "$L_{11}, L_{20}, L_2, L_0, L_{18}$". Then, according to Table 3, it is in the format of "000199, 015127, 000003, 000002, 005778", respectively.

E3) The first 5 Lucas numbers are added to each character, starting from the left and L_0, respectively. Thus, "000201, 015128, 000006, 000006, 005785" is found.

Table 3. *Numerical representation of letters with the help of continued fractions.*

Text	L	U	C	A	S
New Lucas number	L_{11}	L_{20}	L_2	L_0	L_{18}
Number	000199	015127	000003	000002	005778
Number of Lucas to be added	$L_0 = 2$	$L_1 = 1$	$L_2 = 3$	$L_3 = 4$	$L_4 = 7$
Final state	000201	015128	000006	000006	005785

E4) If the values found are combined, "000201015128000006000006005785" is found.

E5) Finally, if the zeros on the left are removed, the word "LUCAS" is encrypted with the number "20101512800006000006005785".

B. FOR DECRYPTION (D)

The encryption method is reversed to Lucas-x decipher the encrypted words. To divide numbers correctly, x, which is the digit number of each character, must be given.

D1) Zeros are added to the left of the encrypted number which will be the exact number of digits given. So x must be an integer multiple.

D2) The encrypted number is divided into sections according to the number of digits given.

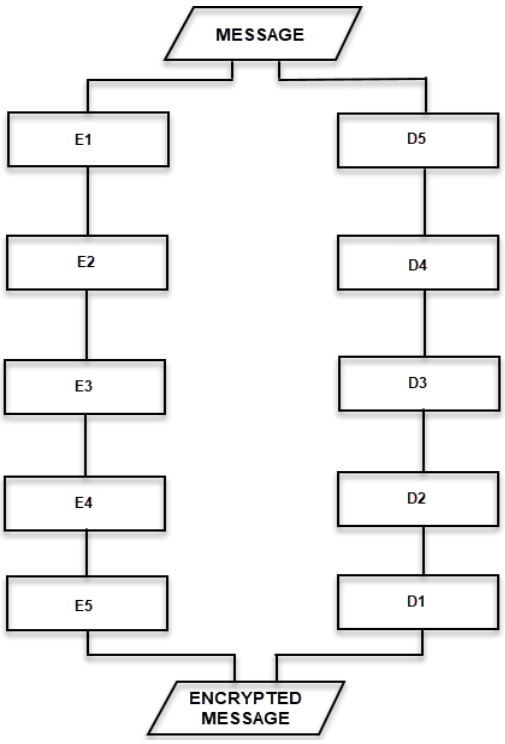
D3) Starting from the left and L_0, Lucas numbers are subtracted from each segmented number.

D4) It is found the number obtained corresponds to which Lucas number.

D5) Finally, letters corresponding to these numbers are found and combined. Table 1 can also be used for this process.

Thus, the numbers are deciphered.

Figure 1. *Flow chart of encryption and decryption*



For example;

Let's decipher the number of "201015128000006000006005785" to be Lucas-6. Here the encrypted number is 27 digits and $x = 6$. Since $x = 6$, Table 2 can be used.

D1) So we should write our encrypted number as 30 digits. So, we have to add 3 zeros to the left side. Thus, it is regulated as "000201015128000006000006005785".

D2) Now let's divide the series of numbers into 6 digits. Then, there are the numbers "000201, 015128, 000006, 000006, 005785".

D3) Now, starting from the left and L_0, Lucas numbers are subtracted. Then, there are the numbers "000199, 015127, 000003, 000002, 005776".

D4) The letters equivalent of the numbers obtained are found as "L, U, C, A, S" according to Table 2.

D5) If the found characters are combined, the word "LUCAS" is formed.

Thus, deciphering is completed as Table 4.

Table 4. *Deciphering example*

Encrypted number	000201	015128	000006	000006	005785
Number of Lucas to be subtracted	$L_0 = 2$	$L_1 = 1$	$L_2 = 3$	$L_3 = 4$	$L_4 = 7$
New number	000199	015127	000003	000002	005776
New Lucas number	L_{11}	L_{20}	L_2	L_0	L_{18}
Found Letter	L	U	C	A	S

III. FINDINGS AND DISCUSSION

In this encryption model, texts were encrypted by being translated into numbers. (But it can also be used by converting to text if desired.) Here, the number equivalent of each text is unique. Deciphering the data in one way is as important as hiding the data by encrypting it. Some arrangements have been made on this subject. Since the encrypted text is written in blocks, it is necessary to know how to separate the blocks so that it can be deciphered in one way. The letters are numbered from 0 to 25, and the space character is numbered with 26 and the number L_{26} is a 6-digit number. For this reason, the Lucas number that all letters match is written in 6 digits. However, if the length of the text to be encrypted is more than 28, it may exceed the digit number used. For this reason, it was preferred to use the Lucas-x notation where x is the length of each block. If a high-security encryption is to be made, then the x number must be very well protected and unauthorized persons must be prevented. Because if x is unknown, the longer the length of the text given, the harder it is to crack the password. When trying to decipher through trial and error, first of all, it should be checked whether the length of the ciphered text is a multiple of 6. If the length of the ciphertext is not a multiple of 6, then zeros had deleted from the left or the length of the text is more than twenty-eight. If the length of the ciphertext is not a multiple of 6, processes become more complicated. In this case, encryption and decryption steps should be controlled in multiple ways. If length of ciphertext is the multiple of 6, then it is divided into 6-digit blocks. After following the steps given before, it is checked whether the Lucas sequence gives its terms. If yes, the deciphering process is completed. If not, the result is reached by trying a higher number of digits in order. Of course, this means a lot of time and cost. It is important that the file size of the data is also small so that the storage cost is minimal. In order to reduce the storage cost in the designed encryption, unnecessary zeros in the encrypted text were deleted and the size of the text was reduced. In fact, encryption got stronger while the cost decreased. Because when deciphering it became unclear how many zeros would be added to the

encrypted text. Therefore, first, it must be checked the number of digits in order to avoid deleting zeros causing problems in deciphering. If it is missing, deciphering should be started after the necessary additions are made. In fact, while the storage cost decreases, the total cost and time increase as the processes to be applied for decryption increases. In summary, determining the number of zeros deleted from the ciphertext and the number of digits of the block (i.e.x) is important for correct deciphering in this encryption.

IV. CONCLUSION AND SUGGESTIONS

As a result, in this study; after matching the terms of the Lucas sequence with the letters of the alphabet, these terms were strengthened with a Vigenere encryption method. Thus, a new cryptology method was developed. This created technique can be used in encryptions that require simple security. By means of this system, since the words are converted to numbers, encryption is possible only using the numerical keyboard. Encrypted numbers can be deciphered and converted back into words, so they can be uniquely reverted.

This encryption using the terms of the Lucas sequence can be done similarly for other specific number sequences. Even new cryptology techniques can be developed by using with other cryptology techniques. For example; new cryptology techniques can be developed using the Fibonacci, Pell-Lucas sequence and Pell sequence.

V. REFERENCES

[1] D. Kahn, *The Codebreakers*, rev. sub. ed., New York, USA: Scribner Publishing, 1996.

[2] S. Yılmaz, O. Salcan, *Siber Uzayda Güvenlik ve Türkiye*, 1st ed., İstanbul, Turkey: Milenyum Publishing, 2008.

[3] *National Research Institute of Electronics and Cryptology*, TÜBİTAK, [Online]. Available: https://uekae.bilgem.tubitak.gov.tr/tr/kurumsal/tarihce Accessed: 1 May, 2020,

[4] H. Kodaz, F. M. Botsalı, "Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması," *Journal of Selcuk-Technic*, vol. 9, pp. 10 – 23, 2010.

[5] E. Yeşilbaş, "Cebirsel kriptoloji yöntemleri ve bazı uygulamaları," MSc Thesis, Department of Mathematics, Recep Tayyip Erdoğan University, Rize, Turkey, 2016.

[6] J. S. Kraft, L. C. Washington, *An Introduction to Number Theory with Cryptography*, 2nd ed., Broken Sound Parkway, Northwestern United States: Chapman and Hall/CRC Press, Taylor & Francis Group, 2018.

[7] D. R. Stinson, *Cryptography Theory and Practise*, 3rd ed., London, UK: Chapman & Hall/CRC Press Taylor & Francis Group, 2006.

[8] D. R. Stinson, *Cryptography Theory and Practice*, New York, USA: Chapman & Hall / CRC, 2002.

[9] *Data Encryption Standard*, Federal Information Processing Standards Publication 46-1, National Institute of Standards and Technology 1988.

[10] R. A. Mollin, *An Introduction to Cryptography*, Boca Raton, New York, London, Chapman and Hall/CRC, 2006

[12] R. A. Dunlap, *The Golden Ratio and Fibonacci Numbers*, 1st ed., 5 Toh Tuck Link, Singapore: World Scientific Publishing, 1997.

[13] S. Vajda, *Fibonacci & Lucas Numbers, and the Golden Section, Theory and Applications*, Chichester, UK: Ellis Horwood Ltd. Pub., 1989.

[14] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, New York, USA, Toronto, Canada: John Wiley & Sons, Proc., 2001.

[15] P. Ribenboim, W. L. McDaniel, *My Numbers, My Friends*, New York, USA: Springer – Verlag Publishing, 2000.

[16] T. Nagell, *Introduction to Number Theory*, 2nd ed., New York, USA: W. C. Brown Publisher, 1989.

[17] M. Basu, B. Prasad, "The Generalized Relations Among the Code Elements for Fibonacci Coding Theory," *Chaos Solitons Fractals*, vol. 41, no. 5, pp. 2517-2525, 2019.

[18] S. Prajapat, A. Jain, R. S. Thakur, "A Novel Approach for Information Security with Automatic Variable Key Using Fibonacci Q-Matrix*," IJCCT*, vol. 3, no. 3, pp. 54–57, 2012.

[19] B. Prasad, "Coding Theory on Lucas p Numbers," *Discrete Mathematics, Algorithms and Applications*, vol. 8, no. 4, 2016.

[20] A. Stakhov, V. Massingue, A. Sluchenkov, "Introduction into Fibonacci Coding and Cryptography", Osnova, Kharkov, 1999.

[21] P. Stakhov, "Fibonacci Matrices, a Generalization of the Cassini Formula and a New Coding Theory," *Chaos Solitons Fractals*, vol. 30, no. 1, pp. 56–66, 2006.