Dicle University
Journal of Engineering

https://dergipark.org.tr/tr/pub/dumf
duje.dicle.edu.tr

Research Article

On Encryption with Continued Fraction

Merve GÜNEY DUMAN[1*]

[1] Sakarya University of Applied Sciences, Department of Engineering Fundamental Sciences, merveduman@subu.edu.tr, Orcid No: 0000-0002-6340-4817

ARTICLE INFO

Article history:

Received 19 December 2021
Received in revised form 5 March 2022
Accepted 30 March 2022
Available online 28 June 2022

Keywords:

continued fractions, cryptology, information security, cryptography

Doi: 10.24012/dumf.1038230

* Corresponding author

ABSTRACT

Many mathematicians have investigated the properties of continued fractions. They made continued fraction expansions of the Pi number, the golden ratio and many more special numbers. With the help of continued fractions, they obtained solutions of some Diophantine equations were. In this study, we make encryption using continued fractional expansions of the square root of non-perfect-square integers. We represent each of the 29 letters in the alphabet as the root of nonperfect square integers starting from 2. Then, we calculate the continued fraction expansions of the square root of each letter's number equivalent. Afterwards, we consider all numbers in the continued fraction expansion as an integer by removing the comma. We consider each word as individual letters, and left spaces between the encrypted versions of each letter. After the encryption process, we deal with the process of deciphering the encrypted text. In the deciphering process, since there is a blank between the numbers, we write the numbers as a continued fraction and calculate the integer expansion. Later, we find the letter corresponding to this number**.**

Introduction

It is known that the discovery of the continued fraction dates back to very old history. The first known information is the calculation of the Euclid algorithm of two relatively prime numbers in 306 BC [1]. In [1], Aryabhata used continued fractions in the solution of linear equations. In 1965, Walls whose book is Opera Mathematica explained how to find continued fractions expansion, and revealed some interesting features related to continued fractions. He demonstrated the term of continued fraction. In 1987, Christiaan Huygens made the first implementation of the theory and explained the best rational approximations. Lagrange found the values of the irrational roots of quadratic equations with the help of continued fractions. References [1-4] can be consulted to have more detailed information about the studies on continued fractions since 306 BC.

Cryptology, on the other hand, is the science that deals with encrypting the data, transferring it from one point to another, and converting the encrypted data to the previous one. Cryptology; includes cryptography and cryptoanalysis. There are two types of encryption systems in cryptology. 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. In private key ciphers, the key is directly decrypted when it is received by untrusted sources. Consequently, it must be protected very well. Many encryption methods have been developed from past to present and these encryption methods have been used in many fields.

Number theory plays a crucial role in cryptology. One of the oldest encryption methods using congruences is Caesar encryption. The Caesar cipher uses replacing each letter of the alphabet with the letter standing three places further down the alphabet. In Affine cipher, the congruences features are used. The RSA cryptosystem was introduced by Rivest et al. (1978), it is based on the hardship of factoring huge numbers. Vast prime numbers were used in RSA encryption. In the discrete algorithm, especially Fermat's theorem was used. The other examples of cryptosystems developed using congruences features are Diffie-Hellman key exchange and El-Gamal encryption. Özyılmaz and Nallı restructured the generalized discrete algorithm problem and generalized El-Gamal cryptosystem based on this problem by using the power Fibonacci number module m [5].

Koblitz worked on cryptosystems using elliptic curve properties [6]. Lately, many authors were interested in Fibonacci coding theory. References [7-23] can be consulted to have detailed information about the studies on number theory or coding theory.

Definitions, Theorems, and Methods

In this section, necessary definitions and theorems about continued fractions will be given. Continued fraction expansion (CFE) table of the first 29 non-square positive integers will be written.

Definition 1. Let $a_0, a_1, a_2, ...$ be integers. An expression in the form

$$[a_0, a_1, a_2, ...] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

is called simple infinite continued fraction where a_i values are called partial divisors for $i = 0,1,2, ...$

Theorem 1. Let $a_0, a_1, a_2, ...$ be integers. In this case, any number with infinite continued fraction expansion is irrational. On the contrary, every irrational number has a unique infinite continued fraction expansion [21].

Theorem 2. Let α be an irrational number. In this case, it is $\alpha = [a_0, a_1, a_2, ...]$ if defined as

$$\alpha = \alpha_0 \ \ , a_k = \llbracket \alpha_k \rrbracket$$

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k} \ \ (k = 0,1,2,3, ...) \,.$$

Also this simple infinite continued fraction expansion is unique [21].

Theorem 3. Let d be a positive integer that is not a perfect square. Then there is a continued fraction expansion of $\sqrt{d}$ such that

$$\sqrt{d} = [a_0, \overline{a_1, a_2, .. a_{n-1}, 2a_0}]$$

where n is the period length.

Example 1. Find the CFE of the $\sqrt{19}$ by using Theorem 2.

Solution 1. Let $\alpha = \alpha_0 = \llbracket \sqrt{19} \rrbracket$. By using Theorem 2, we get

$$a_0 = \llbracket \sqrt{19} \rrbracket = 4,\ \alpha_1 = \frac{1}{\sqrt{19} - 4} = \frac{\sqrt{19} + 4}{3}$$

$$a_1 = \left\llbracket \frac{\sqrt{19}+4}{3} \right\rrbracket = 2,\ \alpha_2 = \frac{1}{\frac{\sqrt{19}+4}{3} - 2} = \frac{3}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{5}$$

$$a_2 = \left\llbracket \frac{\sqrt{19}+2}{5} \right\rrbracket = 1,\ \alpha_3 = \frac{1}{\frac{\sqrt{19}+2}{5} - 1} = \frac{5}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{2}$$

$$a_3 = \left\llbracket \frac{\sqrt{19}+3}{2} \right\rrbracket = 3,\ \ \alpha_4 = \frac{1}{\frac{\sqrt{19}+3}{2} - 3} = \frac{2}{\sqrt{19}-3} = \frac{\sqrt{19}+3}{5}$$

$$a_4 = \left\llbracket \frac{\sqrt{19}+3}{5} \right\rrbracket = 1,\ \alpha_5 = \frac{1}{\frac{\sqrt{19}+3}{5} - 1} = \frac{5}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{3}$$

$$a_5 = \left\llbracket \frac{\sqrt{19}+2}{3} \right\rrbracket = 2,\ \alpha_6 = \frac{1}{\frac{\sqrt{19}+2}{3} - 2} = \sqrt{19} + 4$$

$$a_6 = \llbracket \sqrt{19} + 4 \rrbracket = 8 = 2a_0.$$

Then, according to Theorem 3,

$$\sqrt{19} = [4, \overline{2,1,3,1,2,8}]$$

is obtained. Using Theorem 2, CFE of positive numbers which are not a perfect square and between 2 and 34 has been found and these values are given in Table 1.

Table 1. *Continued fraction expansion of some positive numbers.*

d	$\sqrt{d}$	d	$\sqrt{d}$
2	$[1,\overline{2}]$	20	$[4,\overline{2,8}]$
3	$[1,\overline{1,2}]$	21	$[4,\overline{1,1,2,1,1,8}]$
5	$[2,\overline{4}]$	22	$[4,\overline{1,2,4,2,1,8}]$
6	$[2, \overline{2,4}]$	23	$[4,\overline{1,3,1,8}]$
7	$[2,\overline{1,1,1,4}]$	24	$[4,\overline{1,8}]$
8	$[2,\overline{1,4}]$	26	$[5,\overline{10}]$
10	$[3,\overline{6}]$	27	$[5,\overline{5,10}]$
11	$[3,\overline{3,6}]$	28	$[5,\overline{3,2,3,10}]$
12	$[3,\overline{2,6}]$	29	$[5,\overline{2,1,1,2,10}]$
13	$[3,\overline{1,1,1,1,6}]$	30	$[5,\overline{2,10}]$
14	$[3,\overline{1,2,1,6}]$	31	$[5,\overline{1,1,3,5,3,1,1,10}]$
15	$[3,\overline{1,6}]$	32	$[5,\overline{1,1,1,10}]$
17	$[4,\overline{8}]$	33	$[5,\overline{1,2,1,10}]$
18	$[4,\overline{4,8}]$	34	$[5,\overline{1,4,1,10}]$
19	$[4,\overline{2,1,3,1,2,8}]$		

In this part, information about how the coding technique is done by means of CFE will be given.

Existence: According to Theorem 1, each irrational number has an infinite CFE [21].

Uniqueness: According to Theorem 1, the CFE of each irrational number is unique [21].

In Table 2, the matching of each letter with non-square integers is given.

Table 2. *Numbered letters*

A	B	C	Ç	D	E
2	3	5	6	7	8
F	**G**	**Ğ**	**H**	**I**	**İ**
10	11	12	13	14	15
J	**K**	**L**	**M**	**N**	**O**
17	18	19	20	21	22
Ö	**P**	**R**	**S**	**Ş**	**T**
23	24	26	27	28	29
U	**Ü**	**V**	**Y**	**Z**	
30	31	32	33	34	

The numerical equivalent of each letter of the word to be encrypted is found with the help of Table 2. Then the CFE of each natural number is calculated by Theorem 2. These CFEs are given in Table 1. Then the symbols in the CFEs are purified and the numerical equivalent of the letters is found. The most important point to note here is that since $\sqrt{26}$ continued fractional expansions start with 5, the last term ends with 10. Since the last digit is a two-digit natural number, it causes an error while deciphering. Only the number 0 was used instead of the number 10 to provide uniform deciphering. Anyway, there is no probability that any other term will be 0 in the $\sqrt{d} = [a_0, \overline{a_1, a_2, .. a_{n-1}, 2a_0}]$ expansion, including $a_0 = [\![\sqrt{d}]\!]$ because it is $a_i > 0$ for $i \geq 1$.

Now, let's give an example of a word encrypted with continued fractions.

Example 2. Encrypt the message "CODES" by using CFE cipher.

Solution 2. First, let's find the numerical equivalent of each letter with the help of Table 2.

"$C = 5$", "$O = 22$", "$D = 7$", "$E = 8$", "$S = 27$"

Now the c. f. expansion of the square root of these numbers should be calculated using Theorem 2 or found by using Table 1. Then we get

"$C = \sqrt{5} = [2, \overline{4}]$", "$O = \sqrt{22} = [4, \overline{1,2,4,2,1,8}]$",

"$D = \sqrt{7} = [2, \overline{1,1,4}]$", "$E = \sqrt{8} = [2, \overline{1,4}]$",

"$S = \sqrt{27} = [5, \overline{5,10}]$".

Now it should be examined whether any CFE contains 10. Since the letter S contains 10, the last digit must be coded by writing 0 instead of 10. Therefore, the encrypted form of the letters is

"$C = 24$", "$O = 4124218$", "$D = 2114$",

"$E = 214$", "$S = 550$".

As a result, the encrypted form of the word "CODES" is

"24 4124218 2114 214 550".

In this part, the encrypted text will be deciphered by means of CFE.

Existence: According to Theorem 1, $[a_0, a_1, \dots, a_n, \dots]$ infinite continued fraction is irrational[21].

Uniqueness: According to Theorem 1, since CFE is unique, every infinite continued fraction has a unique irrational number equivalent[21].

Firstly, it should be checked whether the number to be decoded contains the number 0. If it does not contain 0, then there isn't any problem.

The first part of the given number is written as an integer part and the next part as repeating part. As a result; CFE is found. If it contains 0, then we write this digit as the natural number 10 instead of 0. Then, this number is written in Definition 1 format. After the format is arranged, the CFE will be calculated or Table 1 will be used. You will find non-square number for every CFE. Finally, by using Table 2, we find out which number corresponds to the letter. Thus, it is uniquely deciphered.

Example 3. The following array is the ciphertext of a message encrypted with CFE cipher:

"24 4124218 2114 214 550"

Decrypt the message.

Solution 3. First, it should be examined whether any numbers contain 0. There is a "0". Since the last number letter contains 0, the number in the last digit should be 10 instead of 0. Now, each number is written as a CFE. For this, the first digit of the number should be written as the integer part of the continued fraction and the next part should be written as a repeating part. This message can be arranged in the form of

"$24 = [2, \overline{4}]$" , "$4124218 = [4, \overline{1,2,4,2,1,8}]$"

"$2114 = [2, \overline{1,1,4}]$" , "$214 = [2, \overline{1,4}]$",

"$550 = [5, \overline{5,10}]$".

Now we will write in the form of fractions them and find irrational number values.

$$[2, \overline{4}] = 2 + \cfrac{1}{4 + \cfrac{1}{4 + \cfrac{1}{\ddots}}} = \sqrt{5}$$

$$[4, \overline{1,2,4,2,1,8}] = 4 + \cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{8+\cfrac{1}{1+\cfrac{1}{\ddots}}}}}}}} = \sqrt{22}$$

$$[2, \overline{1,1,4}] = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}}} = \sqrt{7}$$

$$[2,\overline{1,4}] = 2+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{\ddots}}}} = \sqrt{8}$$

$$\left[5,\overline{5,10}\right] = 5+\cfrac{1}{5+\cfrac{1}{10+\cfrac{1}{5+\cfrac{1}{\ddots}}}} = \sqrt{27}.$$

So, we get the numbers “5-22-7-8-27”. By using Table 2, it can be seen here

“$C = 5$”, “$O = 22$”, “$D = 7$”, “$E = 8$”, “$S = 27$”.

As a result, the decrypted message is “CODES”.

Conclusion

By using CFE, each word can be encrypted and deciphered uniquely. Since letters are converted into numbers with this encryption method, they can be easily integrated and used in digital systems. This encryption may be preferred for digitizing and storing electronic information. If the encryption method used in this study is used alone, its security will be low. Instead, encryption will increase security if used several times or combined with other encryption methods. With this encryption method, it will take a long time to fully decipher the text encrypted with existing programs. In addition, this study is open to improvement, considering the features and usage patterns of continued fractions and other encryption methods. This encryption method is weaker than encryption methods such as RSA, AES, but stronger than primitive encryption methods. The longer the password, and the more times the method is applied in succession, the longer it will take to crack. The password is not unbreakable, but it may require a very fast computer and a long time depending on the process applied.

References

[1] Collins, D. C., “Continued Fractions,” *The MIT Undergraduate J. of Mathematics*, vol. 1, pp. 11-20, 1999.

[2] Kline, M., *Mathematical Thought from Ancient to Modern Times*, New York, USA: Oxford University Press, 1972.

[3] Koshy, T., “Fibonacci and Lucas Numbers with Application”, New York, USA: Wiley, 2001.

[4] Brezinski, C., “History of Continued Fractions and Padè Approximants”, Berlin, Germany: Springer-Verlag, 1990.

[5] Özyılmaz, C., Nallı, A., “Restructuring of Discrete Logarithm Problem and Elgamal Cryptosystem by Using the Power Fibonacci Sequence Module M”, *Journal of Science and Arts*, ss. 61-70, 2019.

[6] Koblitz, N., “Elliptic Curve Cryptosystems*”, Mathematics of Computation*, 48, 203-209, 1987.

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

[8] Prajapat, S., Jain, A., Thakur, R. S., “A Novel Approach For Information Security With Automatic Variable Key Using Fibonacci Q-Matrix”, *IJCCT 3*, no. 3, 54–57, 2012.

[9] Prasad, B., “Coding Theory on Lucas p Numbers”, *Discrete Mathematics, Algorithms and Applications*, 8, no.4, 2016.

[10] Stakhov, A., Massingue, V., Sluchenkov, A., “Introduction into Fibonacci Coding and Cryptography”, Osnova, Kharkov, 1999.

[11] Stakhov, P., “Fibonacci matrices, a Generalization of the Cassini Formula and a New Coding Theory”, *Chaos Solitons Fractals*, 30, no. 1, 56–66, 2006.

[12] Kodaz, H., Botsalı, F. M., “Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması”, *Selçuk Üniversitesi Teknik Bilimler Meslek Yüksekokulu Teknik-Online Dergi*, 9, 10-23, 2010.

[13] Kraft J. S., Washington L. C., “An Introduction to Number Theory with Cryptography”, Boca Raton, New York, London, CRC Press Taylor & Francis Group, 2014.

[14] Stinson, D. R., “Cryptography Theory and Practise. 3. edition”, London, England: Chapman &Hall/CRC Press Taylor & Francis Group, 2006.

[15] Kahn, D., “The Codebreakers”, New York, USA: The Macmillan Company, 1996.

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

[17] National Bureau of Standard., Data Encryption Standard, Federal ˙Information Processing Standards, NBS., 1977.

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

[19] Redmond, D., “Number Theory: An Introduction”, New York, USA: Markel Dekker, Inc, 1996.

[20] Adler, A., Cloury, J.E., “The Theory of Numbers, A Text and Source Book of Problems”, Boston, London, Singapore, Jones and Bartlett Publishers, 1995.

[21] Mollin, R. A., “Fundamental Number Theory with Applications”, Boca Raton, New York, London, Tokyo, CRC Press, 1998.

[22] Kalman, D., Mena, R., “The Fibonacci Numbers Exposed”, *Mathematics Magazine*, 76, 2003.

[23] Wiener M. J., “Cryptanalysis of short RSA secret exponents”, *IEEE Transactions on Information Theory*, 36, 553-558, 1990.