International Journal of Industrial Engineering and Management (IJIEM), Vol. 8 No 4, 2017, pp. 219-227
Available online at www.iim.ftn.uns.ac.rs/ijiem_journal.php
ISSN 2217-2661

UDK 004.41

Generating Catalan-Keys Based on Dynamic Programming and their Application in Steganography

Muzafer Saračević
Associate Professor, Department of Computer Sciences, University of Novi Pazar, Dimitrija Tucovića bb, 36300, Novi Pazar, Serbia, muzafer.saracevic@uninp.edu.rs
Muhedin Hadžić
Teaching assistant, Department of Computer Sciences, University of Novi Pazar, Dimitrija Tucovića bb, 36300, Novi Pazar, Serbia, hadzic.muhedin@gmail.com
Edin Korićanin
Teaching assistant, Department of Computer Sciences, University of Novi Pazar, Dimitrija Tucovića bb, 36300, Novi Pazar, Serbia, edinkoricanin@gmail.com

Received (31.08.2017.); Revised (28.09.2017.); Accepted (02.11.2017.)

Abstract

The purpose of this research paper is related to investigating properties of Catalan numbers and their possible application in the procedure of data hiding in a text, more specifically in the area of steganography. The objective of this paper is to explain and investigate the existing knowledge on the application of Catalan numbers, with an emphasis on dynamic key generation and their application in data hiding. Our copyright method was applied, which is based on decomposition of Catalan numbers and is applied in data hiding in other data, so the very existence of codes is hidden in the data carrier.

Key words: *Cryptology, Steganography, Hiding information, Generating cryptographic keys, Catalan numbers.*

1. INTRODUCTION AND RELATED WORK

In this paper, we will try and determine how important the numbers theory is in cryptology and steganography, primarily in algorithm development for generating pseudo random numbers, which are necessary for keys generation. The numbers theory in asymmetrical systems is the most important not only in keys generation but also in design of the crypto logical algorithm, and in crypto-analysis and steganography [3,6]. In most of the symmetric crypto logical procedures, combination schemes are used, which are based on permutation. An important place in these procedures, especially in keys generation, is given to pseudo accidental numbers. The objective of every crypto-method is to find the fastest and most suitable way to save the transferred piece of information. One of the methods which are used nowadays is based on the use of steganography.

In our paper [14] a method for decomposition of Catalan numbers is provided, which uses the procedure of memoization and dynamic programming. In this way, we provide an effective method for generation of all Catalan numbers for large bases. Otherwise, generation of all Catalan numbers for large bases n is an extremely demanding (in terms of time and memory) and complicated problem. Catalan numbers have a wide application in solving many combinatorial problems. In the monograph [4] concrete applications of these numbers are listed with possible solutions with regards to the representation of Catalan numbers. The textbook [15] lists a group of problems which describe over 60 different interpretations of Catalan numbers. In this paper, the objective is to propose an application of Catalan numbers in keys generation: more specifically, these numbers can be used as generators of pseudo accidental numbers. By using Catalan numbers, the main idea is realized, and that is generation of a long and unpredictable sequence of symbols from an alphabet (for instance, binary), based on a short key selected by accident (the base n). Coding can be realized in combination with various combinatorial problems which are based and whose solution hides itself in the before mentioned numbers. In this way, exceptional performance of the cryptography system is reached.

An interesting application of Catalan numbers is given in the paper [8], where new techniques for data hiding using sequences of Catalan-Lucas numbers are suggested. Concretely, in the paper two generators of accidental numbers are used. One generates Catalan numbers and the other Lucas sequences. In the suggested technique, one sequence represents a set of constants and the other a sequence of variables which are conditioned by the given constants. This way represents an improvement compared to the existing

techniques for data hiding. This paper represents a new approach to data hiding in a text as well as in pictures (in pixels). Besides the before mentioned technique, a modified steganographic algorithm is given, which uses Catalan-Lucas series, and it provides high security, where three keys are generated.

Besides the before mentioned paper, techniques in picture steganography by using known sequences of numbers (amongst which are Catalan numbers as well) are listed in the paper [1]. In this paper, several methods for picture steganography by using Catalan and Lucas numbers are suggested, and experimental examinations which give better results compared to the techniques which use Fibonacci numbers are given. The suggested methods use a combination of Lucas-Catalan-Fibonacci numbers and Catalan-Lucas numbers which are far superior compared to Fibonacci's technique for data hiding.

In the classic LSB (Least significant bit) technique it is possible to embed secret data only in the first several bit-plans, because the quality of a picture radically deteriorates when embedding of data in higher bit-plans is implemented. In the last decades, techniques of steganography have been applied in different types of files. The needs of music and photography copyright (amongst others) have forced many software companies to develop many steganographic systems which are used in different areas.

Recursive data hiding in visual cryptography is given in the paper [9]. A cryptographic method is suggested, by which data hiding in a group of pictures is performed, and reconstruction of protected, cryptic data is performed by a direct, visual observation. Such algorithms of visual cryptography are based upon strong mathematical foundations, and they are characterized by a high level of security and resilience, and there is a possibility of solving problems with regards to secret sharing.

2. THEORETICAL BASIS OF THE RESEARCH

Catalan numbers C_n, $n > 0$ represent a sequence of natural numbers which occurs as a solution to a large number of known combinatorial problems (the number of possible ways in discreet grid with the dimension of *n x n,* the number of possible records in the form of n-balanced parentheses, stack of permutations, the Ballot problem, binary trees, polygon triangulation, etc.). Catalan numbers are defined as [4]:

$$C_n = \frac{(2n)!}{(n+1)!n!} \tag{1}$$

$$C_n = \frac{1}{n+1}\binom{2n}{n}, n \geq 0 \tag{2}$$

The other way for defining Catalan numbers is:

$$\binom{2n}{n} - \binom{2n}{n-1} = \frac{(2n)!}{(n!)^2} - \frac{(2n)!}{(n-1)!(n+1)!} = \frac{(2n)!}{n!(n+1)!} = C_n \tag{3}$$

Table 1 represents Catalan numbers for fundamentals n ∈ {1, 2… 30}, which are calculated according to formulae (1) or (3).

Table 1. The value of the first 30 Catalan numbers

n	C_n	n	C_n	n	C_n
1	1	11	58,786	21	24,466,267,020
2	2	12	208,012	22	91,482,563,640
3	5	13	742,900	23	343,059,613,650
4	14	14	2,674,440	24	1,289,904,147,324
5	42	15	9,694,845	25	4,861,946,401,452
6	132	16	35,357,670	26	18,367,353,072,152
7	429	17	129,644,790	27	69,533,550,916,004
8	1,430	18	477,638,700	28	263,747,951,750,360
9	4,862	19	1,767,263,190	29	1,002,242,216,651,368
10	16,796	20	6,564,120,420	30	3,814,986,502,092,304

In this paper, we will use Catalan numbers in the property of keys generators for data hiding in the existing text. In Table 1, we can see that *n* base is for keys generation and C_n determines the number of valid keys, that is, the values that fulfill the property of Catalan number (the keys space).

For example, for base *n=30* we have the keys space C_{30}*=3,814,986,502,092,304*, that is, the values which fulfill the property of the Catalan number. With increasing the base *n,* the keys space is drastically increasing. Table 1 represents the values of the first 30 Catalan numbers. In order to secure a stronger, more resilient mechanism for coding on crypto analysis, for the keys it is necessary to select mostly the values whose bases are bigger than 30.

3. ALGORITHM FOR DECOMPOSITION OF CATALAN NUMBERS

In our papers [10,11,12,13,14] we analyzed Catalan numbers and determined that they have the property of recursiveness. The recursive definition of Catalan numbers holds true for C_n, n>0, where C_0=1, and it defines the relationship of two consecutive Catalan numbers. It can be represented as [4]:

$$C_n = \frac{4n-2}{n+1} C_{n-1}, n \geq 1 \tag{4}$$

A relationship for the Catalan numbers who are not consecutive can be established:

$$C_n = \frac{(4n-2)*(4n-6)}{(n+1)n} C_{n-2} \tag{5}$$

$$C_n = \frac{(4n-2)(4n-6)(4n-10)}{(n+1)n(n-1)} C_{n-3} \tag{6}$$

...

$$C_n = \frac{(4n-2)(4n-6)(4n-10)\cdots 6\cdot 2}{(n+1)n(n-1)\cdots 3\cdot 2} C_0 \qquad (7)$$

$$C_n = \frac{(2n-1)(2n-3)(2n-5)\cdots 3\cdot 1}{(n+1)!} 2^n$$

$$C_n = \frac{(2n)!2^n}{(n+1)!2^n n!} = \frac{(2n)!}{(n+1)!n!} = \frac{1}{n+1}\binom{2n}{n}$$

Therefore, this property of Catalan numbers enables us to apply some problem solving techniques which can be reduced to a recursive solution of independent sub-problems. In that way we can more efficiently (and faster) generate keys with a bigger base *n*.

Dynamic programming can be defined as a method which decreases the time necessary for solving the problems which have repeating sub-problems, and which require searching for the optimal sub-structure, as will be described later. In this procedure, it is necessary to preserve the solutions to those problems which have already been solved, so that these results can be used later.

This procedure is called memoization. If it is obvious that the solved sub-problems are no longer necessary, they can be discharged so that the space for memoization can be saved. Therefore, to some extent the problem with regards to time and memoization is solved.

Dynamic programming is used with repeating problems, as well as with optimal sub-structures and memoization. There are two approaches:

1. *Top-bottom*: A problem is decomposed to sub-problems, and then the sub-problems are solved and their solutions are memorized, in the case of their future use. This approach represents a combination of recursion and memoization.
2. *Bottom-up*: All sub-problems are solved one by one and are used in finding the bigger problems. This approach is better, because it keeps the space for memoization on a stack, but sometimes it is hard to determine which sub-problems are necessary.

In our decomposition procedure of Catalan numbers [14] we use the Top-bottom approach with the application of memoization procedure. Memoization represents a combination of dynamic programming and recursion.

All the solutions are memorized, so one problem cannot be solved twice. The decomposition method holds true for the Catalan numbers where n>2. In the given paper we provided an effective method of decomposition of Catalan numbers, represented by segments *(2+i)*.

The number 2 can be represented by one initial segment *(2+i)* and that is *(2+0).* The algorithm at the entrance expects the base n and at the exit we get the expression which represents the sum of segment shapes *(2+i)* whose value is C_n, that is, a set of Catalan numbers.

The memoization method has proven to be efficient and favorable, and in some cases it is faster than dynamic programming. That is the case because by the procedure of dynamic programming we solve all possible sub-problems, and by memoization we solve only the ones which are necessary.

Algorithm 1. Decomposition of Catalan numbers [14]

INPUT: n

1: It sets an initial expression *expr(k)=(2+0), k=2.*

2: *for (k=2; k ≤ n; k++)*

2.1: It calculates the number of segments (2+i) in the *expr(k)*

  2.1.1: Returns the *count(k)*

  2.1.2: It calculates the sum in each segment *(2+i)*

  2.1.3: Returns the *sum(s)*

2.2: *for (s=1; s<= count(k); s++)*

  2.2.1: *for (i=0; i<= sum(s); i++)*

  2.2.1.1: Creates the segment of expression in the shape (2+i)

  2.2.1.2: Connects the expressions with the addition operation +

OUTPUT: The expression *expr [n]* for decomposition for the entered *n.*

Example 1:

For *n=4* it follows that $C_4=14.$ In the first step of the algorithm, an initial expression is set *expr[2]=(2+0).*. In the second step of the algorithm for this case there are two cycles. First, the number of segments of expression *(2+i)* is calculated in the initial expression *expr[2]*, and the number of such segments is 1. The sum in that segment is 2. That means that the following expression *expr[3]* will have two segments of the expression *(2+i).* Therefore, we have ***expr[3]=(2+0)+(2+1).***

Now, *expr[3]* is set for the initial and then it is calculated how many segments of the expression *(2+i)* it possesses, and that number is 2, while the sums are 2 and 3, respectively. That means that the following expression *expr[6]* will have 5 segments of the expression *(2+i),* in total. Finally, we have *expr[4]=**(2+0)+(2+1)+(2+0)+(2+1)+(2+2).***

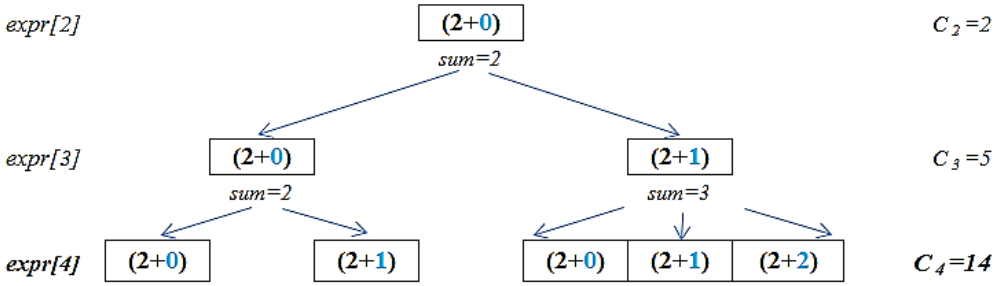

Figure 1. Graphic presentation of decomposition of Catalan numbers

Algorithm 1 works in combination with the method for determining the validity of the generated expressions. Based on the given output in Algorithm 1, it is determined whether the two main conditions are met.

Condition 1: The sum of all segments of the expression *(2+i)* has to be equal to the Catalan number (C_n) for which decomposition is performed:

$$C_n = \sum_{s=1}^{C_{n-1}} \sum_{i=0}^{seg(s)-1} (2+i),\ n>2 \tag{8}$$

Seg(s) are the elements of the set of segments {2,3,2,3,4,…}.

Condition 2: The following equation must be met:

expr[n]=2 * expr[n-1] + rest

Based on formula (8) we can determine that the following is true:

$$rest = C_n - 2C_{n-1} = \sum_{s=0}^{C_{n-1}} \sum_{i=0}^{seg(s)-1} i \tag{9}$$

$$2C_{n-1} = \sum_{s=1}^{C_{n-1}} 2 \tag{10}$$

The rule that is true for two consecutive Catalan numbers also applies to the segments of two consecutive expressions and that is that the previous expression must be found in its entirety two times in the expression of the subsequent level.

An example for examining condition 1 and 2:

We examine, using a concrete example, whether the first condition is met for C_4. By analyzing the obtained expression we determine:

I. *expr[4]=(2+0)+(2+1)+(2+0)+(2+1)+(2+2), the expression according to the segments of the expression (2+i)*
II. *expr[4]= 2+3+ 2+3+4 ,the expression with the sums in the segments*
III. *expr[4]= 5+5+4,the expression with the previous, double Catalan number and the rest*
IV. *expr[4]= 14, the Catalan number for the given fundamental n=4.* An example for condition examination 2:

For two expressions *expr[3]* and *expr[4]*, we investigate whether the second condition is met:

I. *expr[3]=(2+0)+(2+1)*
II. *expr[4]=**[(2+0)+(2+1)]+ [(2+0)+(2+1)]+**(2+2)*
III. *expr[4]=2*expr[3]+(2+2)*
IV. *expr[4]=2*expr[3]+rest, where rest=4.*

In Table 2 the elements of the set and the number of determining segments are presented.

Table 2. The number of segments of the expression (2+i)

n	The sums of segments (2+i)	count(seg[s])	sumAll(seg[s])
2	{2}	1	2
3	{2,3}	2	5
4	{2,3,2,3,4}	5	14
5	{2,3,2,3,4,2,3,2,3,4,2,3,4,5}	14	42

4. APPLICATION OF THE DECOMPOSITION METHOD IN DYNAMIC GENERATION OF THE VALID BINARY CATALAN-KEYS

In this section, we will present some examples of valid binary keys records generation based on the decomposition procedure of Catalan numbers. We will present the way of generation of all keys for base *n*, if we already have keys in base *n-1* (the procedure of dynamic programming).

Catalan numbers have the property of recursiveness and their generation can be efficiently realized by applying the decomposition method. In the paper [16], an advanced technique for coding is presented which uses the characteristics of key recursiveness. Each advanced value of the key is twice as big as the previous one. That means that a special emphasis is put on cryptosystem design with the techniques for recursive keys generation. This method decreases the execution time for base *n*, which requires searching for

the optimal sub-structure *n–1*, but this is only for those techniques which have repeating sub-problems (steps). We will present the way of generating binary values of Catalan numbers for base *n=4*, where based on formulae (1) or (3) we have $C_4=14$, that is, 14 values which fulfill the property of Catalan number for the given base *n=4*. The condition for generating all keys combinations is to have the previous block of binary records for *n–1=3*, and their number is $C_3=5$, and their binary records are: *101010, 101100, 110010, 110100* and *111000.*

The second parameter at the entrance is the expression of decomposition for the base for which generation of binary records is required, and that is ***expr[4]=(2+0)+(2+1)+(2+0)+(2+1)+(2+2).***

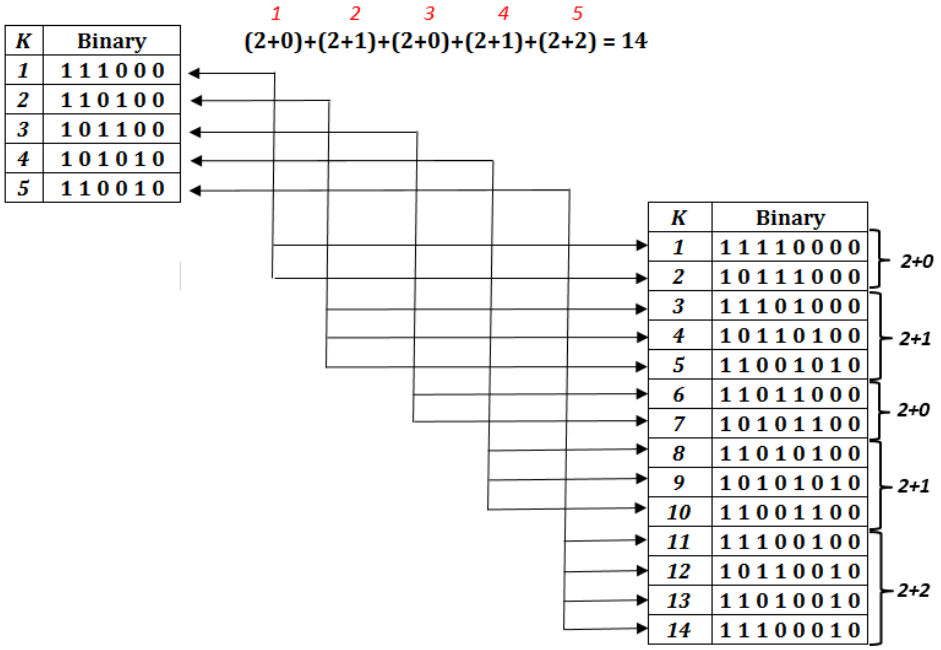

Figure 2. The procedure of generating binary records for base *n*, under the condition that there is *n-1* and the decomposition expression *exp [n]*

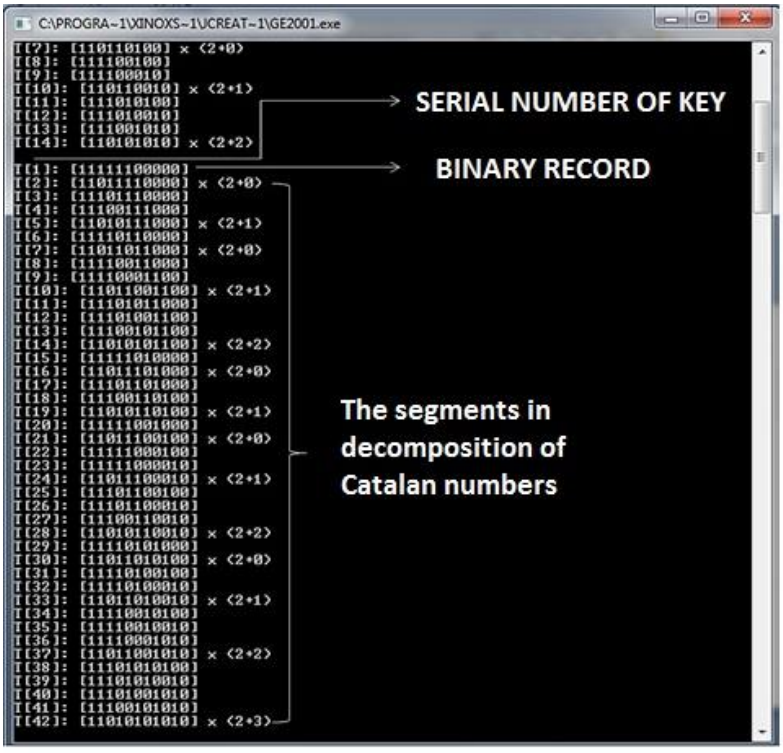

Figure 3. Dynamic keys generation (a repoort from a Java application for decomposition of Catalan numbers)

From *Example 1* and based on the report from the Java application, we can observe that the block of binary records in C_3 was copied twice to C_4 with adequate additions.

$$C_3 = \begin{bmatrix} 1&1&1&0&0&0 \\ 1&1&0&1&0&0 \\ 1&0&1&1&0&0 \\ 1&0&1&0&1&0 \\ 1&1&0&0&1&0 \end{bmatrix} \quad C_4 = \begin{bmatrix} 1&1&1&1&0&0&0&0 \\ 1&1&1&0&1&0&0&0 \\ 1&1&0&1&1&0&0&0 \\ 1&1&0&1&0&1&0&0 \\ 1&1&1&0&0&1&0&0 \\ 1&0&1&1&1&0&0&0 \\ 1&0&1&1&0&1&0&0 \\ 1&0&1&0&1&1&0&0 \\ 1&1&0&0&1&1&0&0 \\ 1&1&0&0&1&0&1&0 \\ 1&0&1&0&1&0&1&0 \\ 1&0&1&1&0&0&1&0 \\ 1&1&0&1&0&0&1&0 \\ 1&1&1&0&0&0&1&0 \end{bmatrix}$$

The way for generating additional new binary records is described in our paper [14] in detail. Based on the results, we can classify the obtained binary records in C_n. We can observe a regularity – the addition of transferred blocks from C_{n-1} to C_n is realized in two new forms. In this case we can observe two types of binary records: **10 [C_{n-1}] and 1 [C_{n-1}] 0.**

Tables 3 and 4 present the examples of chain generation from C_3 to C_4 and then from C_4 to C_5 , according to the principle of transferring two blocks of binary records from the previous level in the form of addition of two new forms *10 [C_3], 1 [C_3] 0, 10 [C_4]* and *[C_4] 0.*

Table 3. Generation of binary blocks in C_4 based on C_3

C3	C4					Rest
	10 [C3]		1 [C3] 0			
111000	10	**111000**	1	**111000**	0	**11001010**
110100	10	**110100**	1	**110100**	0	**11001100**
101100	10	**101100**	1	**101100**	0	**11010010**
101010	10	**101010**	1	**101010**	0	**11100010**
110010	10	**110010**	1	**110010**	0	

Table 4. Generation of binary blocks in C_5 based on C_4

C4	C5		Rest
	10 [C4]	1 [C4] 0	
11110000	**1011110000**	**1111100000**	**1100101010**
11101000	**1011101000**	**1111010000**	**1100101100**
11011000	**1011011000**	**1110110000**	**1100110010**
11010100	**1011010100**	**1110101000**	**1100110100**
11100100	**1011100100**	**1111001000**	**1100111000**
10111000	**1010111000**	**1101110000**	**1101001010**
10110100	**1010110100**	**1101101000**	**1101001100**
10101100	**1010101100**	**1101011000**	**1101010010**
10101010	**1011001100**	**1110011000**	**1101100010**
10110010	**1010110010**	**1110010100**	**1110001010**
11001010	**1011010010**	**1101010100**	**1110001100**
11001100	**1011100010**	**1101100100**	**1110010010**
11010010	**1011001010**	**1110100100**	**1110100010**
11100010	**1010101010**	**1111000100**	**1111000010**

5. EXAMPLE OF APPLICATION OF DECOMPOSITION CATALAN NUMBERS IN STEGANOGRAPHY

Data hiding due to security reasons is a common occurrence in all organizations whose business is based on protected data transfer. To hide a piece of information means not to allow that it be readable to a third person. In order to solve the problem, besides the application of certain cryptographic algorithms, steganographic methods are also possible which allow data hiding in pictures, text, audio and video recordings, in the way that the original data carrier remains verifiable.

Steganography is a science which is concerned with hiding data in other data, so that the very existence of codes is hidden in the data carrier. The objective of every crypto-method is to find the fastest and most suitable way to save the transferred piece of information.

In the paper [8], new techniques for data hiding are suggested that use combinations of *Catalan – Lucas* numbers sequences, which represents an improvement compared to the existing techniques for data hiding. Based on many other research papers, we can observe that *Lucas – Catalan – Fibonacci* numbers combinations are used, which are far superior compared to Fibonacci technique for data hiding.

In this section of the paper, we will present only one example of Catalan numbers decomposition application in steganography. More precisely, we will use sequences in form of combinations of *Catalan numbers sequences – decomposition of Catalan numbers.*

Namely, in the mentioned techniques, one sequence represents one set of constants and the other sequence is represented by variables which are ''conditioned'' by the given variables, that is, they are calculated based on them. The formula for Catalan numbers will serve as generator for the first numbers sequence (constants) and the decomposition method will serve as generator for the second sequence (variables). These two sequences are interchangeably connected, that is, the other sequence is conditioned by the first. The decomposition method generates variables based on constant Catalan numbers (example: 1,2,5,14,42, etc.). In that way we avoid application of other numbers (like Fibonacci or Lucas numbers).

Guided by the *Catalan – Lucas* technique given In the papers [1,8], we will take one sequence from the sequence of Catalan numbers and based on the decomposition of those numbers generate another sequence of numbers which will be dependent on the first sequence. In that way we will have a combination of sequences *Catalan – Decomposition – Catalan.*

Example 2: We will use the declining sequence of the first 5 Catalan numbers *C (5) = {42, 14, 5, 2, 1}***.** Based on this sequence, we can get sequences which fulfill the decomposition conditions of the given Catalan numbers. A question is raised, how many different sequences can occur?

The number of such sequences is directly dependent on the number of different *(2+i)* segments in the decomposition expression. If we take that the generator of new sequences is C_4, the decomposition expression for *C(4) ={(2+0), (2+1), (2+0), (2+1), (2+2)}*, then we can observe that in this expression there are three different *(2+i)* segments, and those are: *(2+0), (2+1), (2+2).* That means that we have **2^3=8 different combinations** of new sequences, in total.

We will notice one more regularity which occurs in all new combinations of sequence numbers generation. If we apply the decomposition rule where we have that every following Catalan number is generated in the way that it contains the doubled previous number and some rest, then the sum of all the elements of the new sequence is the next Catalan number.

Next, we will examine whether the given rule for, in this case, all 8 combinations is true:

- **Case 1:**
  According to decomposition rules for Catalan numbers, we will multiply the Catalan numbers sequence *C(5)={42,14,5,2,1}* by the expression C_{decomp}*(4)={(2+0),(2+1),(2+0),(2+1),(2+2)}* and we get *(42*2+0),(14*2+1),(5*2+0),(2*2+1),(1*2+2).* The obtained sequence is *D1={84,29,10,5,4}.* The D1 sequence is obtained, where we can observe that the sum of its elements is 132, that is, it is the next Catalan number. Guided by the Catalan – Lucas technique we will unify sets *C(5)* and *D1* and get *X1={1,2,4,5,10,14,29,42,84}.*
  We can use this sequence in the data hiding procedure. Later we will demonstrate in what way we do that. Now we will check whether the decomposition expression really enables generation of a sequence which fulfills the properties of the Catalan number, that is, whether the sum of the obtained sequence is equal to the next Catalan number, in this case 132.
- **Case 2:**
  If we take the second combination of expression C_{decomp} *(4)={(2+0),(2+2),(2+0),(2+1),(2+1)}*,
  by multiplication of sequence of Catalan numbers and the given decomposition expression we get
  *(42*2+0), (14*2+2), (5*2+0), (2*2+1), (1*2+1).*
  The obtained sequence is *D2={84, 30, 10, 5, 3}.* We can notice that the sum in set D2 is also 132, which is the next Catalan number. Guided by the Catalan – Lucas technique we will unify the two sets and get *X2={1,2,3,5,10,14,30,42,84}***.**
  We can use this sequence in the data hiding procedure as well. We can exemplify the remaining combinations of decomposition expression.
  Again we will get a sequence which fulfills the properties of Catalan number and decomposition:
- **Case 3:**
  C_{decomp} *(4)*= (2+0), (2+2), (2+1), (2+1), (2+0). The obtained sequence is *D3={84, 30, 11, 5, 2},* the sum of the elements is 132. Unifying the sets we get *X3={1,2,5,11,14,30,42,84}*
- **Case 4:**
  C_{decomp} *(4)*= (2+1), (2+0), (2+0), (2+1), (2+2). The obtained sequence is *D4={85, 28, 10, 5, 4}*, the sum of the elements is 132. Unifying the sets we get *X4={1,2,4,5,10,14,28,42,85}*
- **Case 5:**
  C_{decomp} *(4)*= (2+2), (2+1), (2+0), (2+1), (2+0). The obtained sequence is *D5={86, 29, 10, 5, 2}*, the sum of the elements is 132. Unifying the sets we get *X5={1,2,5,10,14,29,42,86}*
- **Case 6:**
  C_{decomp} *(4)*= (2+0), (2+2), (2+1), (2+0), (2+1). The obtained sequence is *D6={84, 30, 11, 4,3}*, the sum of the elements is 132. Unifying the sets we get *X6={1,2,3,4,5,11,14,30,42,84}*
- **Case 7:**
  C_{decomp} *(4)*= (2+1), (2+2), (2+1), (2+0), (2+0). The obtained sequence is *D7={85, 30, 11, 4, 2}*, the sum of the elements is 132. Unifying the sets we get *X7={1,2,4,5,11,14,30,42,85}*
- **Case 8:**
  C_{decomp} *(4)*= (2+1), (2+0), (2+2), (2+0), (2+1). The obtained sequence is *D8={85, 28, 12, 4, 3}*, the sum of the elements is 132. Unifying the sets we get *X8={1,2,3,4,5,12,14,28,42,85}*

Example: Let us take an open text P="**SINGIDUNUM BG"**. If the convertor *ASCII Text to Binary* is applied we get a sequence of bits, which is the following binary record: *01010011 01001001 01001110 01000111 01001001 01000100 01010101 01001110 01010101 01001101.*

By applying the presented *Catalan – Decomposition – Catalan* technique we can use sequences (X1 – X8) for hiding a piece of information inside an open text P. For example, we can take sequences *X3, X4, X5* and based on their values determine the hidden position of bits in the binary record of the message SINGIDUNUM BG.

The positions of Catalan numbers are fixed (static), and the positions obtained based on the decomposition expression can vary, and their position is directly determined by the existence of fixed positions, that is,

the other values are variables (blue colour). Based on this example, in the record of SINGIDUNUM BG message there is a hidden message **FiR**.

The first sequence which determines the first character: *X3={1,2,5,11,14,30,42,84}*

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

Segment (1): 01000110, SECRET CHARACTER **F** (Binary to ASCII Text Converter)

The second sequence which determines the second character: *X4={1,2,4,5,10,14,28,42,85}*

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

Segment (2): 011010010, SECRET CHARACTER **i** (Binary to ASCII Text Converter)

The third sequence which determines the third secret character: *X5={1,2,5,10,14,29,42,86}*

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

Segment (3): 01010010, SECRET CHARACTER **R** (Binary to ASCII Text Converter)

FINAL RESULT (1+2+3): (01000110, 011010010, 01010010); **SECRET MESSAGE = FiR**

6. CONCLUSION AND FURTHER WORK

Cryptography and steganography are two very dynamic areas, popular and widespread. This paper encompasses some of their basic mathematical concepts and a contribution is given with regards to number theory application in the area of cryptography.

Theoretical research foundations are mentioned where the basic properties of Catalan numbers were investigated and an algorithm for Catalan numbers decomposition is analyzed.

The idea to apply Catalan numbers in cryptography and steganography occurred based on our previous research in the area of numbers theory, applied mathematics and combinatorial problems. With this paper, we gave several propositions and examples of application in steganography, as well as the way of dynamic regeneration of cryptographic keys.

The suggested methods can be further upgraded and modified by more contemporary approaches in cryptography. Some studies deal with numbers theory application in realization of visual cryptography algorithms, that is, in solving the problem of secret sharing. Visual cryptography is primarily based on cryptographic methods which are used to crypt and hide data in a set of pictures, and reconstruction of protected or cryptic data is realized by a direct, visual examination. Besides, numbers theory is nowadays more and more popular in realization of basic cryptographic techniques which are concerned with data transfer.

Besides steganography and visual cryptography, more suggestions for future work in the field of Catalan number application in cryptography can be given. In the paper [2], the authors state the possibility of Catalan numbers application in quantum cryptography.

In many scientific studies, papers and monographs, when the issue of the future of cryptography is touched upon, quantum cryptography is mentioned, which appeared as a consequence of discoveries in the area of quantum computer engineering [5]. It is important to mention that quantum and DNK cryptography, in near future, will represent the basis for protection of classified documents. Therefore, a proposition for a future research paper could be centred on the application of Catalan numbers in quantum cryptography and advancement of the existing algorithms and methods.

7. REFERENCES

[1] Aroukatos, N., Manes, K., Zimeras, S., Georgiakodis, F. (2013), "Techniques in Image Steganography using Famous Number Sequences", International Journal of Computers & Technology, Vol. 11, No.3, pp. 2321-2329.

[2] Cohen, E., Hansen, T., Itzhaki, N. (2016), "From entanglement witness to generalized Catalan numbers", Scientific Reports, Vol. 6, pp. 302-321.

[3] Higgins, P.M. (2008), Number Story: From Counting to Cryptography, Springer Science & Business Media, Berlin, Germany.

[4] Koshy, T (2009), Catalan Numbers with Applications, Oxford University Press, New York.

[5] Kościelny, C., Kurkowski, M., Srebrny, M. (2013), Modern Cryptography Primer: Theoretical Foundations and Practical Applications, Springer Science & Business Media, Berlin, Germany.

[6] Lachaud, G., Ritzenthaler, C., Tsfasman, M.A. (2009), Arithmetic, Geometry, Cryptography, and Coding Theory, American Mathematical Society, United States.

[7] Mašović, S., Saračević, M., Stanimirović, P. (2014), "Alpha-Numeric notation for one Data Structure in Software Engineering", Acta Polytechnica Hungarica: Journal of Applied Sciences, Vol.11, No.1, pp.193-204.

[8] Pund-Dange, S., Desai, C.G. (2017), "Data Hiding Technique using Catalan-Lucas Number Sequence", Indian Journal of Science and Technology, Vol. 10, No.4, pp. 12-17.

[9] Sandeep, K. (2010), "Recursive Information Hiding in Visual Cryptography", available at: https://arxiv.org/abs/1004.4914 (accessed: 24.05.2017.)

[10] Saračević, M. (2013), Methods for solving the polygon triangulation problem and their implementation (in Serbian). Doctoral dissertation, University of Niš, Faculty of Science and Mathematics.

[11] Saračević, M. (2017), Application of Catalan numbers and some combinatorial problems in cryptography (Bachelor's thesis), Singidunum University in Belgrade.

[12] Saračević, M., Mašovic, S., Miloševic, D. (2013), "Java implementation for triangulation of convex polygon based on Lukasiewicz's algorithm and binary trees", Souteast European Journal of Soft Computing, Vol.2, No.2, pp. 40-45.

[13] Saračević, M., Stanimirović, P., Krtolica, P., Mašović, S. (2014), "Construction and Notation of Convex Polygon Triangulation based on ballot problem", ROMJIST- Journal of Information Science and Technology, Vol.17, No.3, pp. 237-251.

[14] Stanimirović, P., Krtolica, P., Saračević, M., Mašović, S. (2014), "Decomposition of Catalan numbers and Convex Polygon Triangulations", International Journal of Computer Mathematics, Vol. 91, No. 6, pp. 1315-1328.

[15] Stanley, R. P. (2012), "Catalan addendum to Enumerative Combinatorics", available at: http://www-math.mit.edu/~rstan/ec/catadd.pdf.(accessed: 24.05.2017.)

[16] Srikantaswamy, S.G., Phaneendra, H.D. (2012), "A Cryptosystem Design with Recursive Key Generation Techniques", Procedia Engineering, Vol. 30, pp. 170-173.

Generisanje katalonskih ključeva zasnovanih na dinamičkom programiranju i njihova primena u steganografiji

Muzafer Saračević, Muhedin Hadžić, Edin Korićanin

Primljen (31.08.2017.); Recenziran (28.09.2017.); Prihvaćen (02.11.2017.)

Abstrakt

Svrha ovog istraživačkog rada je istraživanje osobina katalonskih brojeva i njihove moguće primene u postupku prikrivanja podataka u tekstu, konkretnije u oblasti steganografije. Cilj ovog rada je objasniti i istražiti postojeće znanje o primeni katalonskih brojeva, s naglaskom na dinamičko generisanje ključeva i njihove primene u skrivanju podataka. U radu je primenjen sopstveni, autorizvan metod, koji se temelji na dekompoziciji katalonskih brojeva i aplikaciju u podacima koji se skrivaju u drugim podacima, tako da je samo postojanje kodova skriveno u nosiocu podataka.

Ključne reči: *kriptologija, steganografija, skrivanje informacija, generisanje kriptografskih ključeva, katalonski brojevi.*