DOI: https://doi.org/10.31686/ijier.vol10.iss5.3743

Cryptography as an educational tool in counting techniques for high school

Sávia Cristina Vidal
EEL-USP
https://orcid.org/0000-0002-4343-8534

Maria da Rosa Capri
EEL-USP
https://orcid.org/0000-0002-5287-3511

Estaner Claro Romão
EEL-USP
https://orcid.org/0000-0003-4316-2029

Abstract

This paper aims to analyze the feasibility of implementing a didactic sequence for the teaching and learning process of Combinatorial Analysis, using Cryptography as an educational tool for High School. For this, a project was applied in the second semester of 2017, lasting 26 class hours, in a class of the 2nd year of high school, composed of 22 students from a public school in the interior of São Paulo State - Brazil. This teaching proposal appropriated Didactic Engineering as a Research methodology, which enabled the development of a didactic sequence. This in turn was divided into six steps, which approached counting techniques, without the use of formulas, through the encryption of binary numbers, Caesar's code and the encryption present in the film: The Da Vinci Code. This study was exposed by students participating in the project at the school's Science Fair. In order to analyze the learning evolution of the participating students, a pre-test and a post-test were applied, which presented a satisfactory evolution in the students learning. It was also possible to realize, during the project application, the improvement and development of the skills of: teamwork, self-confidence, oratory, time management and autonomy in the pursuit of knowledge.

Keywords: Counting techniques, Cryptography, High school.

1. Introduction

It is common to hear from students that the discipline of mathematics is complicated, difficult and is a subject for a few, the argument most used is that most of the content seen in schools is not applicable in day to day.

Among the contents of Mathematics studied in basic education, we have an area that is designed to work counting techniques, called: Combinatorial Analysis, which we are going to discuss in this work.

This area of study, from the introduction to the end of its teaching, works with examples and problems applicable in everyday life, such as: the possible quantities of combinations of clothes, the possible amounts of car plates, phone numbers, possible combinations in games of chance, among others. Faced with this contradiction, in which, one of the greatest problems in the learning of Mathematics is the little applicability in the daily life of the students and since the Combinatorial Analysis is intended to solve present day-to-day problems, the question arises: Why combinatorial analysis is such a challenging topic for teachers and students?

Carvalho (2015) affirms that combinatorial analysis is seen as a "complex" matter, because the resolution of problem situations associated with Mathematics you need flexibility of reasoning, since there are no an algorithm or model ready to be followed. For Morgado et al. (1991), one of the problems encountered in the teaching and learning of combinatorial analysis are in problems, which often, by the statement, demonstrate to be of simple solution, however it is necessary to high dose of creativity and ingenuity to solve them.

These affirmations they direct us to a possible answer to the previous question, which makes us to perceive that the difficulty in Combinatorial Analysis may be linked to the way Mathematics has been teach, that is, mechanically. However, several factors lead to resistance in the teaching and learning process of Combinatorial Analysis and to discuss them contributes not only to the learning of the content in question, but also to other branches of mathematics widely applied in our daily life, according to Roa and Navarro Pelayo (2001, p. 1):

> The combinatorial problems and techniques for their resolution have profound implications for the development of other areas of mathematics such as: probability, number theory, automata theory, artificial intelligence, operative research, combinatorial geometry and topology. (*our translation*)

Faced with this problematic, we present here a proposal for the teaching and learning of Combinatorial Analysis, which uses Cryptography as an educational tool, being that the Cryptography, will immediately be the main subject and counting techniques will be learned as a means to solve questions related to this subject, after the introduction of these concepts, learning will turn to the study of Combinatorial Analysis. It is important to remember that Cryptography is a science that studies methods to hide the content of a message.

The choice for this theme is due to the fact that it is a science that depends on the application of mathematical contents to develop, so much so that Singh (2003, p. 13) affirms that

> It has already been said that World War I was the war of chemists, due to the use of mustard gas and chlorine for the first time, and that the Second World War was the war of physicists due to the atomic bomb. In a similar way it is said that a third World War would be the war of the mathematicians, because the mathematicians will have the control over the next great weapon of war, the information. Mathematicians have been responsible for developing the codes currently used for the protection of military information. And it is not surprising that mathematicians are also at the forefront of the battle to try to decipher these codes. (*our translation*)

Jesus (2013) affirms that Cryptography can be used as an educational tool in the classroom to introduce, reinforce, revise and develop mathematical concepts, as well as enabling the teacher to develop coding and decoding activities. Cantoral et al. (2000) adds that this theme enables the development of activities that stimulate interest, the willingness to learn and curiosity from the students by contents studied.

In this way, this work has as general objective to analyze the viability to implement a didactic sequence for the teaching and learning process of Combinatorial Analysis using Cryptography as an educational tool. For this, were defined the following specific objectives: To study the strategies used in the teaching and learning process of Combinatorial Analysis and to create and apply a didactic sequence relating cryptography and combinatorial analysis based on the Fundamental Principle of Counting (FPC).

2. Development

In order to analyze the viability of the methodological proposal presented, an empirical research it was made in a public school in the state of São Paulo, with a class of the second year of high school, composed of 22 students, which used an hour load of 26 class hours (1 hour classroom = 50 minutes), which occurred between September and November 2017. It is worth mentioning that the teacher-researcher was not the titular teacher of the class, however the titular teacher participated in all the meetings.

For the development of this research, didactic engineering was used as a research methodology, which Artigue (1996) describes as an empirical process that intends to conceive, perform, observe and analyze didactic situations.

3. Didactic Engineering

The Didactic Engineering is a methodology in which the teacher, based on theoretical studies, proposes a sequence of classes, organized and adapted to a certain population of students, in order to produce didactic material, which is efficient in the teaching and learning process.

According to Pais (2005) didactic engineering is composed of four phases, being: (I) preliminary analyzes; (II) conception and analysis a priori; (III) application of a didactic sequence and (IV) a posteriori analysis and validation.

In the first phase, from the preliminary analyzes, the identification of the research problem occurs, which can be done initially by observation or even by the application of diagnostic activities. Besides that, is made a theoretical survey the difficulties that the students present and the studies that have been and are being done on the subject in question. Machado (2002) states that at this stage are made ponderations on the general theoretical didactic framework, but also, to address questions about the specific knowledge of the research theme.

In the second phase, from a priori conception and analysis, a survey is made on the possible solutions to the problems encountered and the possibilities of improvement in the teaching and learning process of the subject in question, elaborating a didactic sequence. Berenguer (2010) affirms that in this phase, the researcher has the task of describing the characteristics of the didactic situation, verifying the possibilities of the students 'actions and analyzing the students' behavior regarding the situation applied.

The third phase is responsible for experimentation, it is the moment in which the teacher-researcher applies the didactic sequence, in a predetermined public, and records the information obtained during the course of the classes. Pannuti (2004) describes the didactic sequence as an organized modality, based on a series of actions sequenced, planned and oriented with the purpose of promoting a specific and defined learning of the subject in question.

Finally, Almouloud and Silva (2012) define the fourth phase, posteriori analysis and validation, as a set of data collected during the application, in order to validate them. In this phase is that occurs the comparison of the hypotheses raised in the a priori analysis, with the results obtained in the experimentation.

4. Development of Activities in Accordance with the Phases of Didactic Engineering

In the first phase, preliminary analyzes, was performed a theoretical study over the teaching and learning of combinatorial analysis and about the use of cryptography as an educational tool in the teaching of mathematics. In relation to the applied research in the classroom, to verify the level of knowledge of the students on the counting techniques of the Combinatorial Analysis, a pre-test was proposed, that was performed in the classroom, for this the teacher-researcher used three class hours, divided into two meetings.

At the first meeting, the researcher-teacher made a personal presentation and also of the project that they were going to develop for all students present, and applied a pre-test, consisting of basic questions about Combinatorial Analysis and some questions that introduced the concept of Cryptography. It is noteworthy that at the moment the students came across this test, there was a lot of rejection, as they claimed the lack of previous study on the subject, however, after it was explained that this evaluation would not score, the students calmed down and tried to solve her the way they considered it right. In the second meeting, the answers presented in the evaluation were discussed.

In the second phase, conception and a priori analysis, was developed didactic sequence, presented in Table 1.

Table 1: Didactic Sequence.

Phases	Developed Activities	Time Class Hour
Introduction to Cryptography	Magic Cards and Caesar Cipher	4
Introduction to Counting Techniques	Counting activities from the magic cards and the Caesar Cipher	3
Development of counting techniques from the movie: The Da Vinci Code	Movie: The Da Vinci Code and its Mathematical Interpretation	5
Science Fair	Science Fair	4
Use of counting formulas	Exercises and resolutions	4

In the third phase, Experimentation, occurred to application of the didactic sequence presented in Table 1, which was used twenty class hours.

The first activity had the two-hour class, divided into two days. The aim was to arouse students' curiosity about the “math” used in magic cards (Figure 1), so that the cryptography theme was introduced.

From Figure 1, it's possible guess a number from 1 to 63, only with the information if the number belongs or not to each of the 6 tables.

In the first class, it was presented to the students, through a data show, the magic cards, and then the teacher-researcher asked that three students volunteered to participate in the magic, for the joke to be played three times. The role given to the student volunteer was to pick a number between 1 and 63 and reveal that number only to classmates, the teacher-researcher did not has access to the chosen number.

After all colleagues have knowing about the “secret” number, the teacher applied it to magic and guessed it. For this, the students answered the following question made by the teacher: “Does the number chosen have in the first table?” Soon after, the students answered only yes or no, this question was asked for all six tables. As soon as the teacher had access to all tables that the number belonged to, she "discovered" it.

1	3	5	7	9	11	13	15
17	19	21	23	25	27	29	31
33	35	37	39	41	43	45	47
49	51	53	55	57	59	61	63

8	9	10	11	12	13	14	15
24	25	26	27	28	29	30	31
40	41	42	43	44	45	46	47
56	57	58	59	60	61	62	63

2	3	6	7	10	11	14	15
18	19	22	23	26	27	30	31
34	35	38	39	42	43	46	47
50	51	54	55	58	59	62	63

16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

4	5	6	7	12	13	14	15
20	21	22	23	28	29	30	31
36	37	38	39	44	45	46	47
52	53	54	55	60	61	62	63

32	33	34	35	36	37	38	39
40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63

Figure 1: Magic Cards (www.google.com.br).

After the joke, it was proposed to the students that found the mathmagic of these cards, this proposal was passed as a homework, which was part of the score obtained in this project.

This activity aroused a great interest in the students, all were participative and intrigued by the magic of the cards. However, only nine students performed the required activity, but they all claimed not to understand the math of the cards, which involved encryption of binary numbers, but claimed to have discovered the trick, which summed the first digit of each table which belonged the number chosen by a particular person.

To explain the magic card math, the teacher made a brief review of binary numbers, and showed the coding and decoding of Hindu-Arabic numbers in binary and vice versa, applying again to magic and explaining the present cryptography step by step. At this moment, it was made a chat about the use of technologies and the application of binary numbers to computers and mobile phones.

Relevant information is that the effective participation in this activity by a student that presented a big disinterest by subject of Mathematics, according to the professor, besides that, this student carried out the research proposed by the teacher-researcher.

The second activity, about the Caesar Cipher, it was used a time of two class hours, which aimed to know Caesar's cipher and apply it in the coding and decoding of words. For the development of this activity, the students were grouped in teams composed of a maximum of four students. The researcher-teacher delivered for each group a paper with the following coded words:

1º) R F Y J R F Y N H F
2º) G V M T X S K V E J M E

As soon as all groups received the paper, it was explained that these words were encrypted and began the challenge of deciphering and finding his keys, then the students could do research on the internet through their cell phone. At this moment the teacher-researcher assumed the function of facilitating and guiding groups when needed.

Only one group correctly decoded the words, however when explaining their method of resolution they stated that they did as a guessing prank after discovering the letter A. That is, by the first coded word, they realized that the letter F was the most repeated, so they changed it to the letter A, so, by guessing, they found that the word was MATEMATICA (*in portuguese*), and therefore the second word was CRIPTOGRAFIA (*in portuguese*), because it was referring to the project. they were developing and the amount of letters in the words were the same.

This reasoning was excellent, because even without realizing it, the students used the concept of letter frequency to start the resolution. However, they could not discover the security key by the cryptographic method, which required the intervention of the teacher-researcher to explain this concept.

Then an activity was performed in which each group coded a different word, using the Caesar cipher, which they just learned, and challenged another group to decode it. Most groups coded words in which no letters were repeated in order to make it difficult to break the code they chose. However, at this moment many doubts arise about the discovery of the key through the frequency of letters, requiring the intervention of the teacher-researcher.

At the end of the class, there was a brief conversation about the history of Julius Caesar's cryptography.

The third activity, about counting activities from previously learned cryptography, aimed to teach counting techniques, initially using exercises on magic cards and Caesar's cipher, addressing the contents of: factorial, simple permutation and simple arrangement, without the use of formulas, using only the multiplicative principle. This activity lasted three hours. The first two classes were conducted from the following exercises:

a) How many binary numbers can we form using 4 bits?

b) By Julius Caesar's cryptography, how many possible keys are there for this encoding?

c) If by applying the substitution technique to encrypt messages using the 26 letters of the alphabet without a predetermined order, how many different modes of encryption can we have?

The teacher solved the exercises concurrently with the students, starting from their previous knowledge about counting, so that they could understand the reasoning involved in each resolution. Then she proposed the following questions, in which the students had time to try to solve them individually:

1) How many different ways can a person who has 5 blouses, 3 pants and 2 shoes dress?

2) How many anagrams, with or without sense, can we form with the word LOVE?

3) How many three letter words (with or without sense) can we write using the letters: A, B, C, D, E, F, G, H, I and J?

Finally, the teacher-researcher corrected the exercises on the board.

In the next class the students were divided into groups to solve the following questions:

1) Let's say that on planet Tico the alphabet is made up of 45 letters. How many different ways will we have to encrypt messages? Since the technique used is that of substitution, without a predetermined order.

2) How many four-digit numbers can we form using the digits 0, 1, 2, 3, 4, 5 and 6?

How many 5-bit binary numbers can we form, with the 3rd digit (counting left to right) being occupied by bit 1?

In this class the research-teacher and the titular professor were just mediators, directing students in solving exercises when needed. Finally, the exercises were corrected in the blackboard.

In this activity it was possible to realize that most students were more concerned with guessing what were the possibilities for each exercise than how many possibilities each exercise presented. In addition, it was possible to realize that the students did not believe in the answer, being necessary to list one by one. The teacher-researcher then made a conversation round about the subject of Combinatorial Analysis, emphasizing your objective, that is, to facilitate counting, using examples which listed all the possibilities and also used the multiplicative principle, in order to show students that by both methods we arrived at the same answer.

After correcting all the exercises one of the students made the following comment: “Teacher, I changed letters, I did magic and now I'm just doing multiplying, and I already know, what again am I learning?” Before teacher-researcher answering, another student answered “our poor is poor and will always be poor, you have not seen the teacher explain to another class that this is part of the math business, and now if you take the test she gave in the beginning, you will know how to solve a lot and in our government exam a lot of this question fell ”, at that moment the teacher made an intervention and talked to the student who questioned her, which stated that I was used to with formulas and formula applications, so he demonstrated this strangeness in the way of teaching and learning.

The teacher-researcher again explained about the concept of combinatorial analysis and added that in the future, the formulas present in this content would be presented, however, the objective at that time was to develop combinatorial reasoning, without the use of formulas, for them to develop the competence of problem solving.

This step was of fundamental importance to introduce the concept of the multiplicative principle. Most students participated in the class and were able to absorb the content worked, at this stage the students were able to really understand what an anagram is, had initial concepts about the definition of factorial, which they immediately liked, as a way of representing the result without the need to perform many operations, and even without labeling, solved simple arrangement exercises through the multiplicative principle.

The fourth activity, about the movie: “The Da Vinci Code”, aimed to develop the concept of repetition permutation, repetition arrangement and simple combination, without the use of formulas, only by the

multiplicative and additive principle, based on the codes presented in the movie. For the development of this activity were used five class hours.

Initially, the film was passed to the students: The Da Vinci Code, which required 3 class hours. The students were immediately interested, but as the movie is long and needs a lot of attention to understand the story, over time they became discouraged to watch it.

After watching the movie the students had as homework, deliver, via email or facebook for the teacher-researcher, a digitized document containing: the film summary, the Mathematics of the Da Vinci Code and the personal opinion of each student. This activity was part of the note given to the "work done".

By this activity it was possible to realize that some students did not like, because the film cited many religious contents and that did not meet their religious beliefs. From this the professor-researcher emphasized that this was a fictional story and that its purpose was not of religious nature, but in the cryptography presented throughout the film.

In the next two classes, the researcher-teacher gave the students a paper with the codes presented in the film, so that, from them, the concept of permutation with repetition, arrangement with repetition and simple combination, without being labeled, was introduced developed through the multiplicative and additive principle.

The fifth activity was the science fair, which aimed to put into practice the theory studied, improve oral communication, share the acquired knowledge and encourage them in the pursuit of scientific knowledge. The development of this activity required four class hours.

In the first class the students were explained the purpose of the science fair. Then the students were divided into 5 groups and the research teacher proposed the task of each team, namely: (i) Presentation of the fair, concept of Cryptography and the application of Mathematics in this science, (ii) Magic cards and present mathematics, (iii) The codes present in the film: The Code da Vinci, with an emphasis on the anagrams, (iv) Cryptéx and its possible passwords and (v) Caesar's Cipher.

In the second class, the students were given a video entitled "Dicas poderosas para se dar bem ao falar em público" (*in portuguese*), available in: https://www.youtube.com/watch?v=Brm_rfIXN10, followed by some tips from the research-teacher and the titular professor. In that same class there was a rehearsal of the presentations. In the next two classes, the science fair actually took place, which was attended by members of the school's direction and coordination and the presence of a professor from the University of São Paulo - USP. This science fair composed a grade, worth from 0 to 10.

This activity aroused a lot of interest in the students, the students showed excellent resourcefulness and commitment to participate. A fact that caught the eye was that of the group that made the presentation of the Science Fair, which was composed of students who were very withdrawn, however, in the presentation they showed that they had actually researched the subject of "cryptography" and surpassed their limits.
At the end of the presentation, the USP teacher and the participants of the school coordination praised and encouraged the students to participate in the academic life and to continue the search for knowledge.

The sixth activity aimed to show students the existence of counting formulas and teach them how to apply them. This required four class hours.

In the first two classes, the researcher-teacher resumed some exercises already solved and added some different exercises, classifying each one according to its type, that is, if the exercise was a simple permutation or with repetition, whether it was simple arrangement or with repetition or combination.

After defining each topic and presenting their formulas, after the explanation the students were challenged to solve 8 exercises, all with two forms of resolution: with and without the use of formula. All exercises were corrected on the board, and shortly after the correction the students were given a paper with five questions to be delivered in the next class; the students had the freedom to solve them with or without the use of formulas.

These exercises were the ones that made up Evaluation of Learning in Process, which the students had already done in the 2017 school year. The resolution of these exercises was part of the score for "work done".

In the other two classes, was performed the correction on the blackboard of the proposed exercises, all with and without the use of formulas.

At this stage, it was possible to notice that the presentation of the formulas generated a feeling of fear in the students. In the moment that the formulas were presented and applied, many students stated that the teacher-researcher was confusing their minds, that this was a very difficult subject, that they had the feeling that they had learned nothing and many even said that they hate mathematics for it, that is, it immediately seems easy, but then complicate.

In solving classroom exercises, the biggest difficulty faced was figuring out which formula to use, even with the help of research teacher and the full professor. The student who had questioned the teacher-researcher about the teaching method thanked for teaching by the "multiplication" method, because there were many formulas and confusing each other to be able to apply them. Another student interrupted the teacher, as he was presenting the classes, and said: "here, owner, I just do it sometimes and I get the same answer as you, why use these things there? I won't even pay attention, because it will confuse my mind". The teacher-researcher explained to him and the class that it was not necessary to memorize the formulas, but was presenting it, because it is a second method of resolution, and it may be that some student identified with this tool, and therefore could not help but present them and explain about each topic separately.

After the didactic sequence was applied, a post-test was applied, which lasted two hours, the required content was the same as the pre-test content, with minor changes to assess whether students were able to absorb the Combinatorial Analysis content and whether progress was made over the first test.

5. A posteriori analysis and validation

In the fourth step there is the analysis of the data obtained during the application from the project, so that the hypotheses raised in the a priori analyzes can be validated.

For this, the researcher-teacher, at the end of the development of the didactic sequence, applied a post-test, to compare the number of correct answers with the pretest, and to measure the size of the educational gain according to the <g> factor for Gery (1972).

The factor <g> Gery (1972) is calculated as follows:

$$\langle g \rangle = \frac{\bar{n}_2 - \bar{n}_1}{\bar{n}_m - \bar{n}_1} \quad (2)$$

Where:

$\bar{n}_1$: Average hit of pretest;

$\bar{n}_2$: Average hit of post-test;

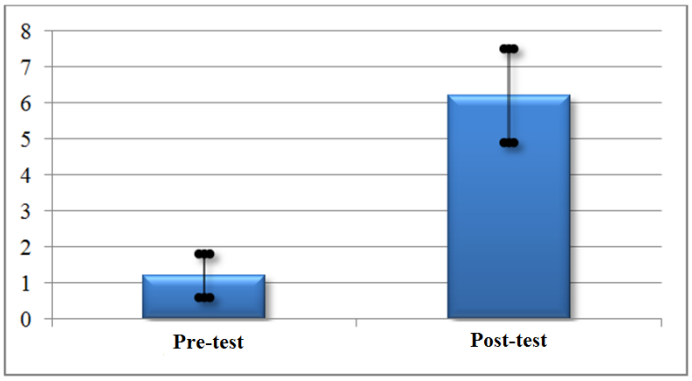
$\bar{n}_m$: Maximum store the student can achieve.

The values obtained are classified according to Table 2.

Table 2 – Rating of values of size of gain educational by Gery's G factor (Gery, 1972).

Classification	Values
Low gain	0,00 < g < 0,30
Average gain	0,30 < g < 0,70
High gain	g > 0,70

Analyzing the results of the students who participated in the two tests, that is, 20 students from the 22 participants, we have that the pretest average was 1.2, with a standard deviation of 0.6; while the post-test mean was 6.2 with a standard deviation of 1.3. As can be seen from Graph 1.

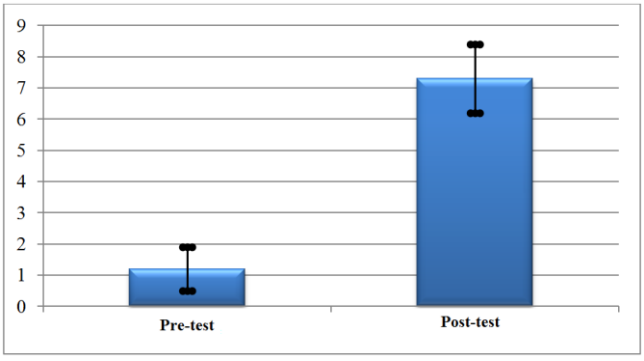


Graph 1: Average and standard deviation of the participating class from the project.

Calculating the size of the educational gain <g> of the whole class, a value of approximately 0.57 was obtained, which is considered an average gain.

However, only 15 students obtained at least 75% attendance of classes for the project implementation, noting that these 15 students participated in both evaluations.

Comparing the pre-test mean with the post-test mean, of the 15 students who had the largest participation in the project application, an evolution of 6.1 points was observed, and a standard deviation of 0.7 in the pre-test and 1.1 in the post-test; which can be seen in Graph 2.

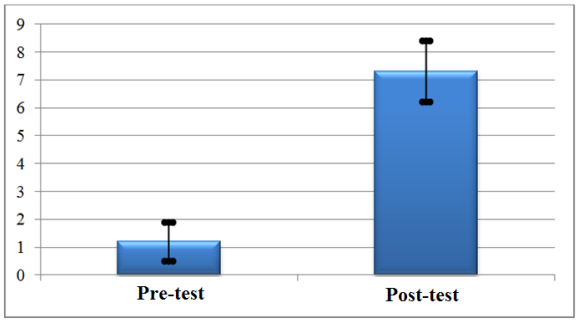


Graph 2: Average and standard deviation of frequent students in the pre-test and post-test.

By calculating the size of the educational gain effect <g> of these 15 students, a value of approximately 0.69 was obtained, which is also considered an average gain, almost a high gain.

Although the name, average gain, indicates a median evolution, it was considered a great evolution, because we see the teaching and learning process as something continuous and that needs a lot of commitment and dedication for a long period of time achieve a development considered high. Thus, in the period given to us, that is, 26 hours of classes, obtaining an average educational gain is very satisfactory.
Of the 22 participating students, only 2 students scored less than 5 on the project, as we can see in Graph 3.

Of the students who did not reach an average higher than 5, one of them refused to participate in the Science Fair, because he said he had no knowledge of what happened, thus, he obtained zero in this activity, a fact that decreases his average, but his score in the post-test was 8.25. The other student, in addition to not participating in the Science Fair, due to absence, obtained a score of 2.23 in the post-test, thus, did not reach an average considered reasonable.



Graph 3: Average and standard deviation of the score of students in the project.

According to these results, that is, with the evolution seen in the first and in the last evaluation and with an educational gain considered average, we realized that with this class, it was possible to teach counting techniques using cryptography as an educational tool. Moreover, the topics of combinatorial analysis were approached based on the multiplicative and additive principle, proving to be efficient, even knowing that the students were conducted, since the beginning of the project to use the multiplicative principle. We do not condemn the use of the formula-application method, but rather prioritize the use of combinatorial reasoning by the FPC (Fundamental Principle of Counting), which enables further development of problem solving competence.
The development of this project enabled students to develop group work, increased self-confidence and self-esteem, improved public speaking skills, better time management, and autonomy in the pursuit of knowledge.

At the last meeting, some students came to the teacher-researcher, asking for references of websites and video classes about Cryptography, because they found the topic interesting and said they would continue this study.

The titular teacher stayed surprised by the participation of some students in the classroom, and especially by the resourcefulness of the students at the Science Fair. He stated that he liked the method used and

pointed out that, after the project was applied, the students pointed out that they liked the methodology used, as learning was not remarkable as following a handout or textbook, and they had no obligation to memorize the formulas just to apply them to the test.

6. Final Considerations

During the project implementation, it was noticed that the teaching and learning process of the Combinatorial Analysis through Cryptography, presents itself as an alternative and attractive way to the students, and that, if worked in a coherent way, the chances of bringing good results are great.

The class benefited from the application of the proposal, showed satisfactory results. Initially the theme of Cryptography caught the attention of students and aroused their curiosity. The Combinatorial Analysis learned as a consequence, that is, initially, counting techniques were used to solve situations involving encryption content, made the students acquire knowledge about the FPC without directly realizing that they were learning new content.

Thus, when new exercises were proposed, outside the context of Cryptography, it was easier to work, because the students had already learned, without even realizing, counting techniques. Immediately, students were surprised by a new Mathematics topic, without the frequent use and application of formulas, but in presenting the formulas to students, many said they preferred the FPC method.

As shown in the results presented, an average educational gain was obtained, which was considered satisfactory.

Thus, it is possible to implement a didactic sequence for the Combinatorial Analysis using the concept of Cryptography with emphasis on the FPC and obtain satisfactory results, of course adapted to the worked school reality.

Based on the school reality of the class benefited from the project application, it was realized that with this teaching method one has the possibility to develop or even improve the problem solving competence, work time management skills, autonomy in seeks knowledge, improve teamwork and public speaking skills, and stimulate curiosity regarding the applicability of mathematics in the world.We emphasize that even with all the difficulties imposed by the educational system, it is essential to develop differentiated activities, at least in the subjects that cause the most difficulties, because in this way, we enable students to awaken by interest and a taste for mathematics.

References

ALMOULOUD, S. A.; SILVA, M. J. F. **Engenharia Didática: Evolução e Diversidade**. *Revista Revemat*, Florianapóles, v. 7, n. 2. 2012. Disponível em: <http://dx.doi.org/10.5007/1981-1322.2012v7n2p22> Acesso em 15 ago. 2017.

ARTIGUE, M. **Engenharia Didática**. In: BRUN, J. **Didática das Matemáticas**. Tradução de: Maria José Figueiredo. Lisboa: Instituto Piaget, 1996. Cap. 4. p. 193-217.

BERENGUER, M. I. S. **A Aplicação da Engenharia Didática no Ensino das Ciências Exatas**. 2010. 36 f. Monografia (Especialização) – Instituto a Vez do Mestre, Universidade Candido Mendes, Rio de Janeiro.

Cantoral, R. et al. **Desarrollo del pensamiento matemático**. México, Trillas: ITESM, Universidade

Virtual, 2000.

CARVALHO, P. C. P. **Métodos e contagem e probabilidade**. 11º Ed. Rio de Janeiro. IMPA, 2015

GERY, F. W. Does mathematics matter? *In:* WELCH, A. (ed.). **Research papers in economic education**. New York: Joint Council on Economic Education, 1972. p. 142-157.

JESUS, A. L. N. **Criptografia na educação básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes**. 2013. 82f. Dissertação (Mestrado profissional em Matemática em Rede Nacional) – Universidade Federal do Vale do São Francisco, Juazeiro.

MACHADO, S. D. A. **Engenharia Didática**. In: MACHADO, S. D. A. (org.). **Educação Matemática:** Uma introdução. 2 ed. São Paulo: Educ., 2002. p. 197-208.

MORGADO, A. C. O. et al. **Análise Combinatória e Probabilidade**. 9. ed. Rio de Janeiro: Graftex, 1991.

PAIS, L. C. **Didática da Matemática** – Uma análise da influência francesa. 2.ed. Belo Horizonte: Autêntica, 2005.

PANNUTI, M.R.V. **Caminhos da prática pedagógica**. TVE Brasil. Rio de Janeiro, p. 01- 05, jun. 2004.

ROA, R. e NAVARRO-PELAYO, V. Razonamiento Combinatorio e Implicaciones para la Enseñanza de la Probabilidad. Jornadas europeas de estadística, Ilhas Baleares, 10 e 11 de outubro de 2001.

SINGH, S. **O Livro dos Códigos**: A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica. Rio de Janeiro: Record, 2003.