


Article

Math Learning in a Science Museum—Proposal for a Workshop Design Based on STEAM Strategy to Learn Mathematics. The Case of the Cryptography Workshop

Juan Roldán-Zafra ¹ and Carmen Perea ^{2,*} 

¹ Department of Statistics, Mathematics and Computer Science, Faculty of Social and Legal Sciences, Salesas Campus, Miguel Hernández University, 03300 Orihuela, Spain

² Department of Statistics, Mathematics and Computer Science, The Institute Centre of Operations Research (CIO), Higher Polytechnic School of Orihuela, Los Desamparados Campus, Miguel Hernández University, 03312 Orihuela, Spain

* Correspondence: perea@umh.es; Tel.: +34-686-888-962

Abstract: In mathematics teaching, great efforts are made, and diverse teaching strategies are employed in order to facilitate students' learning process. Informal environments have proven to be conducive and motivating spaces for science learning. In particular, science museums can be used as a complement and collaborate in order to leverage each of their strengths to motivate mathematics learning. Educational models give a global explanation to the learning process. Taking into account all these aspects and considering van Hiele's model as didactic reference, we propose the design of a general workshop that has among its objectives the learning of mathematics. To do this, we start from the three main elements and processes set forth in van Hiele's model: insight, reasoning levels and learning phases. The insight or student's competence are formulated through Hoffer's abilities, and for the development of the activities of the learning phases, the STEAM (science, technology, engineering, art and maths) strategy. Once the general proposal has been made, we use it to design a scientific workshop for learning mathematics about cryptography. Our greatest challenge was in generating activities adapted to the established requirements. It would be interesting, for future works, to design research to evaluate the effectiveness of the proposal presented. Moreover, it would be interesting to develop a proposal for assessing student learning.

Keywords: cryptography; mathematics workshops; science museums; STEAM education

MSC: 97D40



Citation: Roldán-Zafra, J.; Perea, C. Math Learning in a Science Museum—Proposal for a Workshop Design Based on STEAM Strategy to Learn Mathematics. The Case of the Cryptography Workshop.

Mathematics **2022**, *10*, 4335.

<https://doi.org/10.3390/math10224335>

math10224335

Academic Editors: David Pugalee, Michelle Stephan and Erdiç Çakıroğlu

Received: 25 September 2022

Accepted: 16 November 2022

Published: 18 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Informal environments have proven to be propitious and motivating spaces for science learning. A great number of studies have pointed to the didactic importance of museum visits [1,2].

Designing activities that connect classroom work with informal learning is complicated [3]. Trying to use the museum as an extension of the school would be a mistake. It would be better to make them complement each other and collaborate in order to leverage each of their strengths to motivate mathematics learning [4]. It is essential that museum education teams and teachers collaborate with each other to design the different experiences. These experiences should start in the education centre, continue during the museum visit, and end back in the classroom. Thanks to this structure we can achieve didactic interventions that create real learning spaces [5,6].

The museum activities have to be focused on the visitors, motivating them to participate. Their interaction with museum staff, instruments and materials should enable their own learning process. All this while soliciting their own manual, intellectual and

affective intervention. Active learning defines a space where visitors are curious, can participate creatively and use their own knowledge to build more knowledge [7]. Practical experiments and people's interactive participation are a proven way of improving learning and retention of concepts [8]. Museum staff or a companion takes on the role of facilitator. Thus, learning becomes an enjoyable and relevant process.

1.1. Mathematics Learning in a Science Museum Based on van Hiele's Theory with STEAM Strategy

This active learning methodology has a very effective design for workshop activities when using games to learn mathematics. Plenty of bibliography supports playing as a powerful learning tool [9–12].

Owing to games, we obtain activities that are easily accepted by visitors. These activities improve the relationship between visitors, attention to diversity, use of strategies similar to troubleshooting [13] and awaken competitiveness.

The theoretical framework for learning upon which we base our didactic sequence design is van Hiele's Model [14].

The van Hiele model was initially designed for primary education and geometry-related topics. However, since the 1990s the field of application of the model has been successfully extended to other areas of mathematics and to pre-university and university courses [15–22]. This proven generality of the model provides it with the solidity necessary to be used in works that deal with the teaching–learning process of mathematical content.

In this work, we make use of these extensions, to which the reference is Llorens 94 [15]. He states the model as follows:

- There are different levels of reasoning in students, referring to mathematics.
- Each level supposes a way of understanding, a particular way of thinking, so that a student can only understand and reason with the mathematical concepts appropriate to his or her level of reasoning.
- Therefore, the teaching process must be adapted to the student's level of reasoning. Teaching that takes place at a higher level than that of the students will not be understood.
- The teaching process must be oriented towards facilitating progress at the level of reasoning, so that this progress is made quickly and effectively.

The elements and processes set forth in the model are structured into its three main components: insight, thinking levels and learning phases.

The insight can be translated or defined as the student's competence in the subject matter. In this sense, the purpose of insight is to ensure that students are competent, that is, capable of acting correctly and appropriately in unfamiliar situations, with the actions required in each situation. Students learn the tasks they must perform, why they must perform them, and when they must be performed, and they are thus able to apply their knowledge to solve problems.

In this acquisition of "understanding" the second element arises, the levels of thinking. These levels are: Level 1. Visualization or recognition. Level 2. Analysis. Level 3. Organization and classification. Level 4. Formal deduction and Level 5. Rigor [23,24]. Van Hiele himself in [14] highlights the importance of levels I, II and III.

The different levels are characterized by descriptors or main characteristics that allow us to recognize each of these levels of mathematical thinking from the student's activity.

Through the descriptors, each student can be located at the level of thinking at which he or she is, since they indicate the actions that he or she is capable of carrying out on the concept. In addition, as they show what difficulties they have in progressing to the next level, it makes it possible to focus efforts to help them in their learning.

This model highlights the hierarchical and sequential nature of the levels (it is not possible to move on to the next level of thinking if the previous has not been passed), and the continuous movement from one level to the next (with a transition period in which thinking from two levels will be combined). Moreover, there is a strong relationship

between language and levels. Each level has a specific type of language. Thus, the different thinking skills associated with each of van Hiele's levels are reflected in the ways of troubleshooting. However, they are also manifested in the manner of expression and in the meaning given to the specific vocabulary. Therefore, the teaching process must be adapted to the student's level of reasoning so that it can be understood and, once established at its level, try to progress to the next level.

That is what the learning phases are for. The phases of learning guide us on how to organize contents in order to facilitate students' progress from one level to the next. These phases are: (1) information, (2) directed orientation, (3) explicitness, (4) free orientation, and (5) integration [25]. Therefore, we define five types of activities for each phase.

In information, the first type of activity, a first contact is made. Here, the companion lets the visitors know about the problematic situation to work with. It also serves to find out students' previous knowledge about the concepts to be addressed.

In directed orientation, the second type of activity, visitors discover, understand and learn main concepts and characteristics.

In explicitness, the third type of activity, visitors exchange their own experiences. In addition, they explain the process used to solve the activities through conversation in the group.

In free orientation, the fourth type of activity, visitors use their newly acquired knowledge and language to different investigations in order to perfect their knowledge about the topic.

Finally, in integration, the fifth and last type of activity, visitors should acquire an overall perspective of the contents and methods that have been worked on. They should know how to relate the new knowledge to other fields.

In order to move through the different phases of learning and evolve to the next level, different skills are developed: visual, verbal, pictorial, logical, and applied skills applied by Hoffer [26]. In addition, the use of technology and virtual learning environments has become in another skill. We consider that this last skill should be added to those previously mentioned [27,28]. The philosophy of "learning by doing" allows us to accustom a practice where educational innovation is constant and guarantees the development of the ability to create and develop mathematical logical thinking [29,30]. Therefore, we also consider necessary to complement the pictorial skill with the development of a dexterity in manipulative interaction with objects. In other words, to move from one level of mathematical thinking to the next, we must reach the previous level: visual, verbal, pictorial-manipulative, logical, applied and digital. The attainment of these skills provides us with a measure to evaluate learning.

The last phase of mathematical learning consists of the integration of the content worked with other fields of study. Likewise, the STEAM strategy consists of taking advantage of the common topics between the subjects: science, technology, art and mathematics, to develop an integrative approach to the teaching and learning process. Thus, we can consider STEAM not as a learning methodology but a strategy. One that encompasses technological tools, pedagogical perspectives and methodological perspectives that can contribute to troubleshooting [31].

We should consider that, for mathematics, this multidisciplinary strategy is addressed at the end of the learning process. Hence, it is necessary to be cautious when carrying out STEAM projects in which mathematical competences are developed subsidiarily after subjects in different contexts. Of course, assuming that this is enough for meaningful mathematical learning [32,33].

In this subsection we have seen how van Hiele's model presents a didactic of Mathematics based on experience. A student's progress to a higher level is made when the student has real learning experiences. One of the tasks of the teacher is to provide tasks that help the student progress.

In this work we present a proposal to develop workshops and activities based on the van Hiele model and show the proposal for a particular case: cryptography. For this,

in the following subsection we see the didactic uses of cryptography in the learning of mathematics in Section 2; the preliminaries to go on to present the objectives, research design and methodology in Section 3; in Section 4 the proposal of a cryptography workshop; and finally, in Sections 5 and 6, the discussion and conclusions, respectively.

1.2. Didactic Use of Cryptography for Mathematics Learning

Cryptography, algorithm, social networks and graphs, art, modelling... There are many current and everyday topics connected to mathematical knowledge. We could also use case studies in fictional situations as a way to develop the workshop meaningfully. They could act as medical examiners, sports analysts, expert witnesses, spies or mathematicians. We have chosen cryptography because it has been used for thousand years. In fact, nowadays, it is increasingly present in our daily lives, although we do not realize most of the time. For example, this happens when we pay with our credit or debit card by shopping on the Internet, when we log in to email or by using our digital signature, among many other examples. The protection of valuable information is a priority in today's society. Cyber-attacks on companies, governments and individuals have grown exponentially. Identity theft, fraud, extortion, malware, phishing, spam, spyware, trojans and viruses are just a tiny sample of this activity.

Cryptography is the art of creating secret messages and its technique's sophistication is directly related to scientific advancements. It comes from a branch of mathematics known as information theory. This branch studies the different techniques and algorithms to hide (encrypting) and reveal (decrypting) information considered useful. Cryptanalysis is the counterpart, which tries to break that encryption to retrieve the hidden information.

In every communication there is a: sender (who sends the message), receiver (who receives the message), code (set of signals or signs that make up the message), message (the information to be transmitted) and communication channel (the media by which the message is transferred). In our work, the message was encrypted and in its original encoding.

We divided approaches into two main blocks: classical and modern.

The former was called classical due to the techniques used. Character substitution and transposition operation were carried out. The encryption algorithms required a secret key that was not public.

The substitution method consisted of replacing one symbol with another. However, the transposition method only changed the order of the symbols that were part of the original text. One example of transposition would be the scytale and of substitution the Caesar code. In these cases, the strength of the encryption does not rely on the algorithm, but on the key.

Within modern cryptography we distinguish between private key cryptography and public key cryptography. Private key cryptosystems use the same key for encryption and decryption. This method has the advantage of being very efficient computationally but has the disadvantage of protecting each user's keys. The system becomes inefficient if we are in a network with a large number of users. Public key cryptosystems use two different but related keys, one for encryption and the other for decryption. Every user has a key pair: the private key is used for decryption and is not shared; but the public key is used for encryption and is shared with other users. This solves the key exchange problem, although the algorithms require more processing time.

Mathematics offers us the right tools to work with hidden information. This relationship gives rise to the didactic possibilities of cryptography in mathematics learning. Thanks to the analysis of the different encryption techniques and algorithms, we can present basic mathematical content such as matrices, prime numbers, interpolation and divisibility [34].

In the next section we introduce the notation, definitions and mathematical contents needed to develop the activities proposed in the didactic sequence. Contents include secondary school and the first-degree year of engineering branch. Basically, we address:

- Concepts on divisibility: prime and composite numbers, prime factors decomposition [35,36].
- Concepts about matrices: definition, type of matrices, operation with matrices and the inverse matrix [37].
- Polynomial interpolation: interpolation definition and Newton's formula [38].
- Basic modular arithmetic concepts: congruences, the Euclidean algorithm and Bézout's theorem [39].

In the following section we present the mathematical contents related to cryptography that appear in the development of the workshop. Next, we establish the objectives, design and methodology used for the study's development. In Section 4 we create the activities and, finally, we analyse the results and conclusions.

2. Preliminaries

As we mentioned in the introduction, cryptography is a branch of mathematics called information theory. During its development, it makes use of concepts and results from other mathematics branches such as algebra and numeral calculus, among others.

In this section we present the concepts and the results of the necessary understanding of the cryptography workshop introduced in Section 4. We start by introducing in Figure 1 the general communication diagram, regardless of the encryption method used to transmit the information.

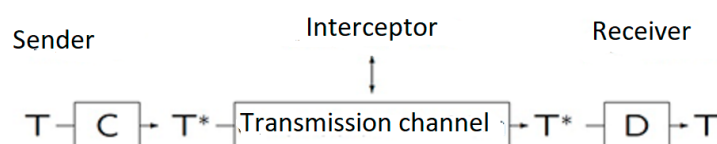


Figure 1. General scheme of transmission channel. T denotes the plain text (either natural language or reduced to a digit sequence for instant transcription). T^* : cryptogram, or coded text (unreadable to anyone who does not know D). C : encryption or coding function, known by the sender. D : decryption or decoding function, known by the receiver.

If we use the Semaphore flag signalling system as a code, C and D are on the table showing each position of the flag with the equivalence to the letter and number that it represents [40]. The same is true if we use Morse code or hieroglyphics [41–43].

If we encode with a classical transposition cryptography method such as the scytale, C and D are the cylinders of the same diameters [44].

In order to understand most private or public key cryptographic system ciphers, see the general diagram in Figure 2. One of the essential concepts to remember is prime integer and coprime integer numbers, as well as some basic results regarding these concepts such as: every positive integer greater than or equal to two is a prime number or is a product of prime numbers. This decomposition is unique, except for the order. The calculation of prime numbers whose product is equal to a given integer n is called the prime factor decomposition of n .

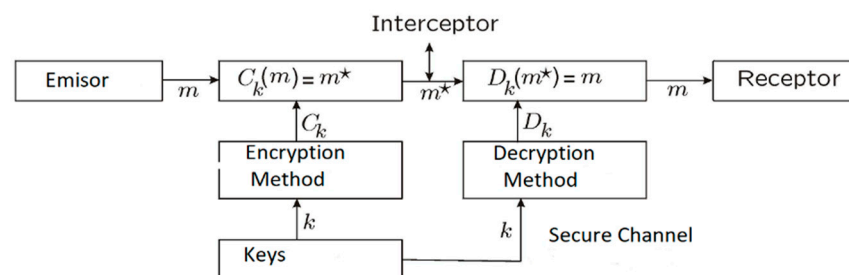


Figure 2. Cryptographic system. Where m denotes the message to be transmitted and m^* the encrypted message.

Congruence is the other fundamental concept. When n is an integer greater than one, given a and b , two integers, a is congruent to b module n and it can be denoted as $a \equiv b \pmod{n}$ if $a - b$ is a multiple of n . The activities in the next section show examples of their application in some cryptographic systems such as an RSA public key.

On the other hand, some of the essential tools in linear algebra useful to us are matrices. We consider that $A_{m \times n}$ denote a matrix of m rows and n columns. If $m = 1$ we affirm that A is a row matrix and if $n = 1$ we affirm that A is a column matrix. In the activity's development, we use classical matrix operations such as addition, product and the calculation of the inverse of a matrix. Any linear algebra book like [45] can be used to review all these operations. Furthermore, we use the solutions of linear equation systems for calculating the interpolation polynomial. The book [46] can be looked up to introduce the interpolation polynomials and how to obtain them.

To conclude this section, we consider that a cryptographic system or cryptosystem consists of five components: M , M^* , K , C and D are the set of all messages to be transmitted; M^* is the set of all encrypted messages; K is the set of keys to be used, that is to say, the parameters controlling the encryption and decryption processes; C is the set of all encryption methods:

$$C = \{C_k : M \rightarrow M^*, k \in K\} \quad (1)$$

D is the set of all decryption methods:

$$D = \{D_k : M^* \rightarrow M, k \in K\} \quad (2)$$

For a given key k , the transformation D_k is the inverse of C_k ; in other words,

$$D_k(C_k(m)) = m, \forall m \in M \quad (3)$$

3. Objectives, Research Design and Methodology

3.1. Objectives

Two objectives were set out in this work's development:

1. To introduce a proposal for science workshop design in a museum, based on van Hiele's mathematics learning model and the STEAM strategy.
2. To use this general proposal to design a scientific workshop for learning mathematics about cryptography.

3.2. Research Design and Methodology

Firstly, we developed a general proposal applicable in different museums, both for students and for the general public, and furthermore with the objective of learning a certain set of mathematical content.

In order to design the workshop format, we used the van Hiele model for the didactic part. To achieve this, we remembered that although van Hiele's model was initially relegated to basic level geometric questions, its original statement is general for mathematical reasoning. We followed the same line of the works developed in 1994, such as that of Llorens [15]; that is: to establish that in certain reasoning skills about a mathematical concept, there are levels that are detectable and whose properties coincide with those postulated by van Hiele [14].

Following this idea and, emphasizing the ideas that Pract [21] insisted in her doctoral thesis, a correct extension of the model first requires defining the descriptors of the levels.

On the other hand, if we remember the axes on which van Hiele's model is based, in addition to the thinking levels we had the student's competence, which we formulated through Hoffer's abilities, and the learning phases in which we considered the use of games and the STEAM strategy in the design of activities

We are aware that a STEAM project involves different subjects, multiple objectives and an expensive timeframe, whereas a workshop in a museum can cover a few activities in

50–60 min. We thought that the first thing to define would be: what is a STEAM workshop for a science museum?

As we have already mentioned, it is not advisable to turn a museum visit into a classroom extension. Therefore, we should programme activities that favour one or several phases of learning without losing the playful and non-formal components that characterise visits to these museums. Interactivity complements formal education, as a workshop does not have to focus on one topic or issue intensively or extensively. That is, it does not have to cover everything [47,48].

In order to identify strengths between van Hiele’s learning phases, Hoffer’s skills and STEAM project characteristics, as well as the conditions of the museum activity, in Table 1, we summarise them.

Table 1. Strengths of science workshop at museum, STEAM project and learning mathematics phases.

Science Workshop at the Museum	STEAM Project [30,31]	Learning Mathematics Phases (according to van Hiele’s Model)
Several pre-set activities with a topic that relates and contextualises them.	The starting point is a real, complex, and open situation, with social implications and very close to the visitors, which acts as a guiding thread for the action.	Type of activities: information, directed guidance, explicit, free guidance, and integration.
Low versatility to adapt the diversity of previous knowledge and short duration.	Well-structured activities are proposed, justifying each action and the relationship between them. These activities are addressed from the different perspectives of STEAM subjects, in order to favour their integration.	Skills to be developed in the activities: communicative, visual, pictorial-manipulative, logical, applied and digital.
No interaction related to the contents of workshop with visitors before or after the visit is planned at first.	Questions are posed in order to develop a research process with an important experimental part.	
The workshop contents may or may not be related to those studied at school.	Visitors participate in the process, starting from the very definition of the problem, in the evaluation and in the production of a final product.	
Funny (motivating), game and mathematics, learning by doing, active interaction and manipulation.	Encourages the visitors to develop creativity, critical thinking, scientific communication and peer-to-peer collaboration.	
Instructor–visitor communication becomes essential.	As transversal: gender perspective, development of SDG (sustainable development goal) values, digital competence and creation of scientific vocation are discussed.	
Scientifically rigorous.		

Therefore, a STEAM workshop for learning in a museum should bring together the features of the three aspects characterised in Table 1.

The STEAM workshop acquires a greater meaning for learning as part of a project. Therefore, a didactic intervention should be designed to introduce the contents of the workshop before, during and after the visit. This type of workshop would be the optimal one for achieving the learning objectives. However, the museum cannot attend exclusively to those groups that have prepared the visit didactically. It often occurs that in school visits to science museums and in the majority of family visits, no prior works are performed on

what is going to be developed in the workshop. For this reason, the workshop should have its own structure, one that allows it to be adapted to the different audience scenarios.

As a general proposal for the workshop in the museum, we consider the following indications:

1. The starting point is a real, complex and open situation, with social implications and very close to the visitors, which acts as a guiding thread for the action. Prior knowledge survey: the language and questions used in the workshops are adapted to the visitors' prior knowledge.
2. Information, directed guidance, explanation, free guidance, and integration (STEAM) activities developing the different communicative, visual, pictorial, logical, applied and digital skills. Presented in a motivational way, through different games or challenges, but scientifically rigorous.
3. Paying attention to the gender perspective, development of SDG (sustainable development goal) values, competence and creation of scientific vocation are discussed.
4. A final product and reflection are obtained.

Authors should discuss the results and how they can be interpreted from the perspective of previous studies and of the working hypotheses. The findings and their implications should be discussed in the broadest context possible. Future research directions may also be highlighted.

Once the general proposal had been set out, we proceeded to carry out the design for the particular case of cryptography. To do this, as we have mentioned, the first action we took was to make sure that the topic to be addressed could be developed according to the van Hiele model. In other words, first of all defined the descriptors of the first three levels that we address. See Table 2.

Table 2. Descriptors of the van Hiele levels I, II and III for cryptography.

Descriptors of the van Hiele Levels	
Level 1 Visualization	Distinguishes between encoding and encryption.
	Recognizes the different types of encryptions and the agents involved.
	Associates the names of the encryption devices with their images.
	Interprets sentences that describe classic encryption methods.
	Draws different codes and encryption devices, accurately labelling their parts.
Level 2 Analysis	Understands the form and meaning of the elements of a flowchart.
	Recognizes different variants in each type of encryption.
	Properly describes the elements of each classical and modern encryption system.
	Translates verbal information about encryption method properties to draw flowcharts.
	Understands the classification of encryption types according to their characteristics.
Level 3 Classification	Properly identifies the use of public and private keys.
	Recognizes the use of prime numbers and cryptography in different areas of everyday life.
	Understands the steps of an algorithm and relates them appropriately to the flowchart.
	Appropriately interprets the visual representation of an algorithm through its flowchart.
	Formulates precise definitions of the different methods presented.
Level 3 Classification	Is capable of building other encryptions based on the presented models.
	Understands the successive steps to encrypt or decrypt a message in classic and modern cryptography.
	Use the appropriate statements to develop an encryption or decryption algorithm.
Level 3 Classification	Is capable of solving problems from other areas of science and everyday life by applying cryptography.

With the van Hiele levels described and, taking into account the strengths established in Table 1 between visits to museums, STEAM projects and learning phases, we related the activities with the three axes of the model by van Hiele. For it, we divided the design and the development of the cryptography workshop into three blocks of activities, which are detailed in Table 3.

Table 3. Characteristics of the STEAM workshop.

Situation	Activity	Type	Concepts	Skills	Sessions
Pre-visit (classroom)	Everyone has secrets I	Information and directed guidance	Cryptology, coding, encryption	Communicative and visual	1 session
Pre-visit (classroom)	The challenge is deciphering it I	Information, directed guidance and explanation	Encryption and decryption by substitution and transposition, matrix definition, additive structure, divisibility criteria.	Communicative, visual, pictorial-manipulative, logical	1 session
Workshop at the museum	Everyone has secrets II	Information and directed guidance	Cryptology, coding, encryption	Communicative and visual	1 session
Workshop at the museum	The challenge is deciphering it II	Information, directed guidance and explanation	Encryption and decryption by substitution and transposition, matrix definition, addition and subtraction of matrices.	Communicative, visual, pictorial-manipulative, logical, and applied	
Workshop at the museum	Enigma machine	Information, directed guidance and explanation	Automatic encryption and decryption, additive structure	Communicative, visual, pictorial-manipulative, logical, and applied	
Post-visit (classroom)	The challenge is deciphering it III	Information, directed guidance, explanation, and free guidance	Row matrix, column matrix, square matrix, matrix multiplication, and inverse of a matrix.	Communicative, visual, and applied	1 session
Post-visit (classroom)	My secrets are yours	Information, directed guidance, explanation, and free guidance	Polynomial interpolation, linear equation systems, Cramer's method, Newton's method for quadratic interpolation and modular arithmetic.	Communicative, visual, and applied	1 session
Post-visit (classroom)	Prime numbers and their significance	Information, directed guidance, explanation, and free guidance	Public and private key, divisibility criteria, prime numbers, prime factor decomposition, integer powers, congruences, Euclid's algorithm, and Bexout's theorem.	Communicative, visual, and applied	1 session
Post-visit (classroom)	Everyone is encrypted	Information, targeted guidance and integration	DNA, living being code, nitrogenous basis, chromosomes, cell nucleus and genetics. Polynomials and Newton's binomial.	Communicative, visual, pictorial-manipulative, logical, and applied	1 session
Post-visit (classroom)	Steganography	Information, directed guidance, explanation, free guidance and integration	Algorithmics, mobile applications, digital photography and scratch	Communicative, visual, pictorial-manipulative, logical, applied and digital	2 sessions

With this present the cryptography workshop proposal in the next section.

4. Proposal for a Cryptography Workshop

This is the development of a complete project starting in the classroom, continuing in the museum and ending back in the classroom. In the case of a group of students who have not prepared for the visit or a non-school group, the museum workshop would be developed with the following activities: the challenge is deciphering it I, the challenge is deciphering it II and enigma machine.

The methodology of the different activities and some examples are set out below.

4.1. Activity 1: Everyone Has Secrets I

Methodology (activity development): After asking the group about the need to keep some information hidden, whether they know any method of encryption and the role of mathematics in achieving this. The mathematical content to be developed is mentioned and prior knowledge is probed. In pairs, they are asked to list situations where they think cryptography is used or a variety of situations are presented for discussion in small groups. In order to complete the activity, each group selects and discusses two news about cryptography, cybersecurity or bitcoins, among others.

In addition, in order to distinguish between coding and encryption concepts, it is possible to play a communication game with sign language. A member of the group takes out a card with the name of a cryptographic concept and communicates it to his or her classmates in sign language (the group will use the alphabet with finger positions). Other codes can be used: morse, flags or braille.

1. Small groups are set up and the sign code is provided.
2. Opinions on the current importance of cryptography are shared.
3. Different news is analysed by the students.
4. A recap or outline of the work done is made.

4.2. Activity 2: The Challenge Is Deciphering It I

Methodology: In this activity, participants are able to form working groups, which makes it possible to communicate solution strategies for each challenge. In addition, it is also possible to share the mathematical concepts used, analysing and socialising the solutions found in order to institutionalise the concepts learnt.

1. Small groups are created, encryption challenges are provided and discussed.
2. Simple types of encryptions by substitution and translation, such as scytale, Polybius and Caesar, are discussed. Matrix definition, additive structure and divisibility criteria are explained.
3. Message decryption with scytale and Polybius. Construction of a Caesar cipher wheel.
4. Opinions are shared on the strategies used to solve the challenges.
5. New challenge proposal by the students.
6. A recap or outline of the work completed is made.

Example: we recommend an activity with the scytale, where the receiver is provided with cylinders of various diameters. In this way, he or she can check that it is only possible to decrypt the message with the cylinder of the same diameter as the one used by the sender to encrypt. It would also be interesting to carry out an activity with the Caesar cipher. Figure 3 shows some secondary school students engaging in a MUDIC cryptography workshop named "Alan Turing". They are encrypting with the scytale, and in Figure 4 the constructed Caesar wheel is shown.



Figure 3. Students encrypting with the scytale.

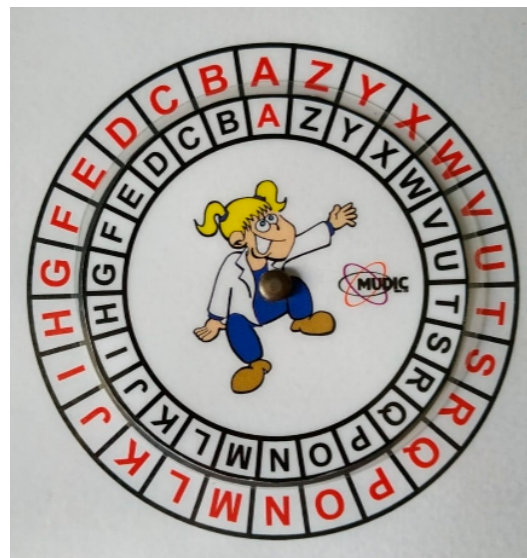


Figure 4. Caesar wheel designed at the MUDIC.

4.3. Activity 3: *Everyone Has Secrets II*

Methodology: After asking the group about the need to keep some information hidden, whether they know any method of encryption and the role of mathematics in achieving this. The mathematical content to be developed is mentioned, and prior knowledge is probed. All this, in order to determine whether the group has already worked on the pre-visit. In order to distinguish between coding and encryption concepts, it is possible to play the communication game with flags. A member of the group takes out a card with the name of a cryptographic concept and communicates it to his or her classmates in flag language (the group will be provided the alphabet with the flag positions.)

1. Small groups are set up and the flag code is given out.
2. Opinions are shared on the strategies used to solve the challenges.
3. New challenge proposal by the students.
4. A recap or outline of the work completed is made.

4.4. Activity 4: *The Challenge Is Deciphering It II*

Methodology: In this activity, participants are able to form working groups, which will make it possible to communicate solutions strategies for each challenge. In addition, it is also possible to share the mathematical concepts used, analysing and socialising the solutions found in order to institutionalise the concepts learnt.

1. Small groups are created, encryption challenges are provided and discussed.

2. Commentary on the generalisation of substitution ciphers. Matrix definition, matrices addition and subtraction.
3. Educational escape code decryption to open a lock on a four-letter surprise chest.
4. Strategies used to solve the challenges are shared.
5. A recap or outline of the work completed is made.

The game development involves the preparation and opening of a chest with several padlocks with a four-letter key (it can also be numeric).

Colour cards are handed out to make pairs of groups. One of them encrypts the keys of the padlocks and hand over the chest, the encryption matrix, and the encrypted key of one of the padlocks. All this because the next encrypted key is the decrypted key obtained from the first padlock. This continues successively with the rest of the padlocks.

In order to encrypt, a four-letter key is chosen, transformed into a numeric key using Table 4 and becomes the elements of the key row matrix $A_{1 \times 4}$. This is encrypted by adding another given matrix $B_{1 \times 4}$, providing the output matrix $C_{1 \times 4}$. This is decrypted by subtracting the matrix $B_{1 \times 4}$.

Table 4. Equivalence of the letters of the alphabet in numbers.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Example: consider a chest and two padlocks.

Group1: encrypted.

The keys for the two padlocks are chosen: $A_1 = (F K B R)$ and $A_2 = (A V G L)$.

They are transformed into a numerical key: $A_1 = (6 11 2 18)$ and $A_2 = (1 22 7 12)$

We have as a key matrix: $A = A_1$

The encryption matrix is calculated by subtracting the row matrices: $B = A_2 - A_1 = (-5 11 5 - 6)$

The output matrix is calculated: $C = A + 2B = (6 11 2 18) + (-10 22 10 - 12) = (-4 33 12 6)$

The encrypted key C and the encryption matrix B are transferred to the other group.

Group2: decrypted.

Data: $C = (-4 33 12 6)$ y $B = (-5 11 5 - 6)$

The key $A_2 = C - B = (-4 33 12 6) - (-5 11 5 - 6) = (1 22 7 12) = (A V G L)$.

The key $A_1 = C - 2B = (-4 33 12 6) - (-10 22 10 - 12) = (6 11 2 18) = (F K B R)$.

4.5. Activity 5: Enigma Machine

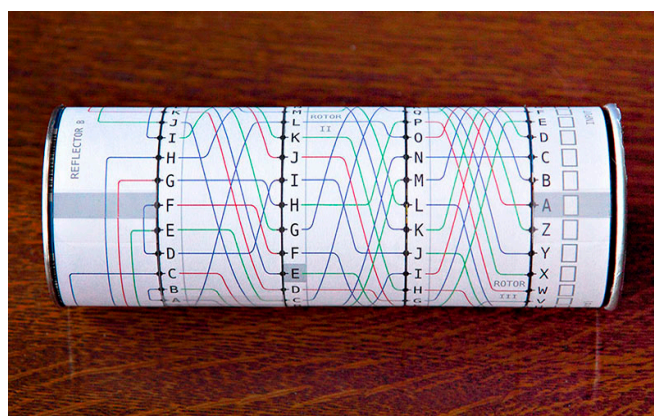
Methodology: In this activity, participants are able to form working groups which make it possible to communicate solution strategies for each challenge. In addition, it is also possible to share the mathematical concepts used, the definitions of input and output disc, rotors and reflector. All this by analysing and socialising the solutions found in order to institutionalise the concepts learnt.

1. Small groups are created, encryption challenges are provided and discussed.
2. Commentary on automatic cryptography and the enigma machine.
3. Construction, encryption and decryption of messages with an enigma machine recreation.
4. Strategies used to solve the challenges are shared.
5. A recap or outline of the work completed is made.

Example: we can work with two enigma machine simulators, depending on the level of the students. For secondary school students, we use the wheel shown in Figure 5a.



(a)



(b)

Figure 5. Enigma simulator. (a) Wheel enigma simulator of MUDIC. (b) Paper enigma machine for crisp tube.

For undergraduate students, we use the simulator in Figure 5b. The operation of the two simulators is practically the same and can be seen in [49].

4.6. Activity 6: The Challenge Is Deciphering it III

Methodology: In this activity, participants can form working groups, which makes it possible to communicate solutions strategies for each challenge. In addition, it is also possible to share the mathematical concepts used, analysing and socialising the solutions found in order to institutionalise the concepts learnt.

1. Small groups are created, encryption challenges are provided and discussed.
2. Commentary on the generalisation of substitution ciphers, row matrix, column matrix, square matrix, matrix multiplication and inverse of a matrix.
3. Educational escape code decryption to open a lock on a three-letter surprise chest.
4. Strategies used to solve the challenges are shared.
5. A recap or outline of the work completed is made.

Game development involves the preparation and opening of a chest with several padlocks with a three-letter key (it can also be numeric).

Colour cards are handed out to make pairs of groups. One of them encrypts the keys of the two padlocks and hands over the chest, together with the encrypted keys and the keys to the encryption matrix. This continues successively with the rest of the padlocks.

In order to encrypt, a three-letter key is chosen for each padlock and two natural numbers of the encryption matrices. The three letters are transformed into numbers using Table 3 and will be the elements of the key row matrix $A_{1 \times 3}$. This is encrypted by multiplying another given matrix $B_{3 \times 3}$, giving the output matrix $C_{1 \times 3}$. The matrix is decrypted by multiplying it by this matrix: $B_{3 \times 3}^{-1}$.

Example: consider a chest and two padlocks.

Group1: encrypted.

The keys for the two padlocks are chosen: $A_1 = (F K B)$, $A_2 = (A V G)$ and the encryption key $B = (12 \ 15)$.

They are transformed into a numerical key with Table 3: $A_1 = (6 \ 11 \ 2)$ and $A_2 = (1 \ 22 \ 7)$

The encryption matrix is calculated for $b_1 = 12$, if b_1 is even: $B_1 = \begin{pmatrix} 1 & 1 & \frac{b_1}{2} \\ 0 & 1 & 0 \\ 2 & 1 & b_1 + 1 \end{pmatrix} =$

$$\begin{pmatrix} 1 & 1 & 6 \\ 0 & 1 & 0 \\ 2 & 1 & 13 \end{pmatrix}$$

The encryption matrix is calculated for $b_2 = 15$, if b_2 is odd: $B_2 = \begin{pmatrix} 1 & 1 & \frac{b_2-1}{2} \\ 0 & 1 & 0 \\ 2 & 1 & b_2 \end{pmatrix} =$

$$\begin{pmatrix} 1 & 1 & 7 \\ 0 & 1 & 0 \\ 2 & 1 & 15 \end{pmatrix}$$

The output matrix is calculated: $C_1 = A_1 \cdot B_1 = (6 \ 11 \ 2) \begin{pmatrix} 1 & 1 & 6 \\ 0 & 1 & 0 \\ 2 & 1 & 13 \end{pmatrix} =$

$$(10 \ 19 \ 62)$$

The output matrix is calculated: $C_2 = A_1 \cdot B_2 = (1 \ 22 \ 7) \begin{pmatrix} 1 & 1 & 7 \\ 0 & 1 & 0 \\ 2 & 1 & 15 \end{pmatrix} =$

$$(15 \ 30 \ 112)$$

The encrypted keys C_1 and C_2 , and the encryption matrix B are given to the other group.

Group2: decrypted.

Data: $C_1 = (10 \ 19 \ 62)$, $C_2 = (15 \ 30 \ 112)$ y $B = (12 \ 15)$.

The encryption matrix is calculated for $b_1 = 12$, if b_1 is even: $B_1 = \begin{pmatrix} 1 & 1 & \frac{b_1}{2} \\ 0 & 1 & 0 \\ 2 & 1 & b_1 + 1 \end{pmatrix} =$

$$\begin{pmatrix} 1 & 1 & 6 \\ 0 & 1 & 0 \\ 2 & 1 & 13 \end{pmatrix}$$

The encryption matrix is calculated for $b_2 = 15$, if b_2 is odd: $B_2 = \begin{pmatrix} 1 & 1 & \frac{b_2-1}{2} \\ 0 & 1 & 0 \\ 2 & 1 & b_2 \end{pmatrix} =$

$$\begin{pmatrix} 1 & 1 & 7 \\ 0 & 1 & 0 \\ 2 & 1 & 15 \end{pmatrix}$$

The inverse matrices are calculated: depending on the students' knowledge, it is possible to solve it by formula, by the Gauss–Jordan method or by a linear equation system.

$$B_1^{-1} = \frac{(Adj(B_1))^t}{|B_1|} = \begin{pmatrix} 13 & -7 & -6 \\ 0 & 1 & 0 \\ -2 & 1 & 1 \end{pmatrix} B_2^{-1} = \frac{(Adj(B_2))^t}{|B_2|} = \begin{pmatrix} 15 & -8 & -7 \\ 0 & 1 & 0 \\ -2 & 1 & 1 \end{pmatrix}$$

The key $A_1 = C_1 \cdot B_1^{-1} = (10 \ 19 \ 62) \begin{pmatrix} 13 & -7 & -6 \\ 0 & 1 & 0 \\ -2 & 1 & 1 \end{pmatrix} = (6 \ 11 \ 2) = (F \ K \ B)$

The key $A_1 = C_1 \cdot B_1^{-1} = (15 \ 30 \ 112) \begin{pmatrix} 15 & -8 & -6 \\ 0 & 1 & 0 \\ -2 & 1 & 1 \end{pmatrix} = (1 \ 22 \ 7) =$

$$(A \ V \ G)$$

4.7. Activity 7: My Secrets Are Yours

Methodology: In this activity, participants can form working groups, which makes it possible to communicate solutions strategies for each challenge. In addition, it is also possible to share the mathematical concepts used, analysing and socialising the solutions found in order to institutionalise the concepts learnt.

1. Small groups are created, encryption challenges are provided and discussed.

2. Commentary on the division of secrets and Parakh secret-sharing scheme [50]. Polynomial interpolation, linear equation systems, Cramer's method, Newton's method for quadratic interpolation and modular arithmetic.
3. Educational escape code decryption to open a lock on a four-letter surprise chest.
4. Strategies used to solve the challenges are shared.
5. A recap or outline of the work completed is made.

The game development would involve the preparation and opening of a chest with a padlock with a three-letter key (it can also be numeric). The idea is that a secret is not in just a person's hands, but that several people are involved. Furthermore, the secret can only be recovered when a certain number of people come together. Colour hands with encryptions are handed out to make a group of three pairs to solve the challenge.

For the encryption, a three-letter key is chosen for the padlock, transformed into numbers using Table 3. The interpolation polynomial is calculated with the points of ordinates 0, 1 and 2, and the abscissae the numbers of the key. The polynomial is then evaluated at different values (3, 4, 5...) and distributed on the different cards.

In order to decrypt the key, they must find second degree interpolation polynomial defined by the encryptions. Then, they must evaluate it at the values 0, 1 and 2, obtaining the key.

Example: consider a chest and a padlock.

Encryption: a key is chosen for the padlock: $A_1 = (F K B)$ and then is transformed into a numerical key with Table 3: $A_1 = (6 \ 11 \ 2)$.

The interpolation polynomial is calculated with the points (0,6), (1,11) and (2,2). It can be performed with Newton's method or with the general parabolic form, solving the resultant equation system. A demonstration of the first method follows below.

We define the polynomial of second degree $y = p + m(x - x_1) + n(x - x_1)(x - x_2)$ as passing through the indicated points:

$$\begin{cases} (0,6) \rightarrow 6 = p + m(0 - 0) + n(0 - 0)(0 - 1) \rightarrow p = 6 \\ (1,11) \rightarrow 11 = p + m(1 - 0) + n(1 - 0)(1 - 1) \rightarrow p + m = 11 \\ (2,2) \rightarrow 2 = p + m(2 - 0) + n(2 - 0)(2 - 1) \rightarrow p + 2m + 2n = 2 \end{cases}$$

The result is a linear equation system that is easy to solve: $p = 6$, $m = 5$ y $n = -7$.

The parabola sought is $y = p + m(x - x_1) + n(x - x_1)(x - x_2) = 6 + 5x - 7x(x - 1) = -7x^2 + 12x + 6$.

We evaluate the polynomial obtained in 3, 4, 5... depending on how many we need.

$$\begin{cases} x = 3 \rightarrow -7 \cdot 3^2 + 12 \cdot 3 + 6 = -21 \rightarrow (3, -21) \\ x = 4 \rightarrow -7 \cdot 4^2 + 12 \cdot 4 + 6 = -58 \rightarrow (4, -58) \\ x = 5 \rightarrow -7 \cdot 5^2 + 12 \cdot 5 + 6 = -109 \rightarrow (5, -109) \dots \end{cases}$$

The pairs are provided with cards with the points obtained and meet in pairs, three by three, to solve the challenge.

Decryption:

Data: three cards with the points (3, -21), (4, -58) and (5, -109).

The interpolation polynomial is calculated with the points (3, -21), (4, -58) and (5, -109). It can be performed with Newton's method or with the general parabolic form, solving the resultant equation system. A demonstration of the second method follows below.

$y = ax^2 + bx + c$ as it passes through the points indicated:

$$\begin{cases} (3, -21) \rightarrow -21 = a \cdot 3^2 + b \cdot 3 + c \rightarrow 9a + 3b + c = -21 \\ (4, -58) \rightarrow -58 = a \cdot 4^2 + b \cdot 4 + c \rightarrow 16a + 4b + c = -58 \\ (5, -109) \rightarrow -109 = a \cdot 5^2 + b \cdot 5 + c \rightarrow 25a + 5b + c = -109 \end{cases}$$

We solve this system using Cramer's method:

$$a = \frac{\begin{vmatrix} -21 & 3 & 1 \\ -58 & 4 & 1 \\ -109 & 5 & 1 \end{vmatrix}}{\begin{vmatrix} 9 & 3 & 1 \\ 16 & 4 & 1 \\ 25 & 5 & 1 \end{vmatrix}} = \frac{14}{-2} = -7, \quad b = \frac{\begin{vmatrix} 9 & -21 & 1 \\ 16 & -58 & 1 \\ 25 & -109 & 1 \end{vmatrix}}{\begin{vmatrix} 9 & 3 & 1 \\ 16 & 4 & 1 \\ 25 & 5 & 1 \end{vmatrix}} = \frac{-24}{-2} = 12 \text{ and } c = \frac{\begin{vmatrix} 9 & 3 & -21 \\ 16 & 4 & -58 \\ 25 & 5 & -109 \end{vmatrix}}{\begin{vmatrix} 9 & 3 & 1 \\ 16 & 4 & 1 \\ 25 & 5 & 1 \end{vmatrix}} = \frac{-12}{-2} = 6$$

The parabola sought is $y = -7x^2 + 12x + 6$.

We evaluate the polynomial obtained in 0, 1, and 2, we obtain the key (6 11 2) = (F K B).

4.8. Activity 8: Prime Numbers and Their Significance

Methodology: In this activity, participants can form working groups, which makes it possible to communicate the results of the research. In addition, it is also possible to share the mathematical concepts used, analysing and socialising the solutions found in order to institutionalise the concepts learnt.

1. Small groups are created, activity objectives are provided and discussed.
2. Commentary on RSA encryption, public and private key, divisibility criteria, prime numbers, prime factor decomposition, integer powers, congruences, Euclid's algorithm and Bexout's theorem.
3. Investigation of the need to use very large prime numbers.
4. The products obtained in the different studies are shared through presentations, panels and exhibitions.
5. A recap or outline of the work completed is made.

Students are asked to investigate RSA encryption and the purpose of public and private keys. If we want to send a message, this is sent transformed into a large number P ; this message is encrypted as $c = P^m \pmod{n}$, where m is the public key. The message is decrypted by calculating $P = c^d \pmod{n}$, where d is the private key. The cipher is correct if numbers m and d verify that $d \cdot m \pmod{s} = 1$. The Bezout theorem is used to calculate these modular inverses. The number n , which is the modulus of both keys, is the product of two primes p and q and $s = (p - 1)(q - 1)$ of similar length [51,52].

Note that for the time being, no formula or procedure has been found to deduce prime numbers. In general, the more cases (more prime numbers produced) the formulae cover, the more computationally inefficient they are. If anyone tries to decode the message, he or she has to find out j , without knowing s . This comes down to knowing $p - 1$ and $q - 1$ otherwise p and q . For this, he or she has to factor n , which is difficult for very large prime numbers.

Example:

First, students conduct an example of encryption/decryption with RSA.

They use small and illustrative numbers compared to those handled by the algorithm. The public key is (m, n) . The private key is (d, n) . Taking $m = 13$, $d = 37$ and

$$n = 5 \cdot 11 = 55.$$

The encryption function is: $\text{encrypt}(P) = Pm \pmod{n} = P13 \pmod{55}$. Where P is the non-encrypted text.

The decryption function is: $\text{decrypt}(c) = cd \pmod{n} = c37 \pmod{55}$. Where c is the encrypted text.

In order to encrypt, if the value of the non-encrypt text is 38, we calculate: $\text{encrypt}(38) = 3813 \pmod{55} = 48$.

In order to decrypt, if the value of the encrypt text is 48, we calculate: $\text{decrypt}(48) = 4837 \pmod{55} = 38$.

We can carry out a second activity with the last year of secondary school and first year degree students. In this activity, they learn about a real application of the RSA public key cryptographic system: the distributed signature scheme of Tal Rabin (Israel, 1962) [53,54], one of the most significant women in modern cryptography [55–57]. This second activity also aims to address a reality that we are aware needs to be changed: the gender gap present in the STEAM field. For this purpose, we take into account the following causes of the problem: gender stereotypes because the STEM sector continues to be perceived as eminently masculine; predominantly male professional environments which, according to many professionals in the sector, are not exactly inclusive, where sexism and harassment continue to persist; as well as the scarcity of female role models, since when we talk about science and technology, the enormous majority of the references heard by girls are male [58].

Therefore, the activity also aims to highlight the huge legacy of women in the field of STEM in general. This project enables us to showcase the women who have contributed to cryptology's development throughout history. To achieve this, we set up groups. Then, they are invited to search on the Internet for women who have contributed to cryptology's development throughout history. They can be supplied with some addresses such as [59] and they can develop a classification of periods. Finally, Tal Rabin's distributed signature system is introduced.

4.9. Activity 9: Everyone Is Encrypted

Methodology: In this activity, participants can form working groups, which makes it possible to communicate the laboratory materials and techniques. In addition, it is also possible to share the mathematical concepts used, analysing and socialising the solutions found in order to institutionalise the concepts learnt.

1. Small groups are created, activity objectives are provided and discussed.
2. Commentary on DNA, living being code, nitrogenous basis, chromosomes, cell nucleus and genetics [60].
3. Vegetal DNA extraction and analysis of plant hybridisation analysis.
4. The strategies used for DNA extraction and Mendel's mathematical reasoning are shared, in addition to polynomials and Newton's binomial.
5. A recap or outline of the work completed is made.

4.10. Activity 10: Steganography

Methodology: In this activity, participants can form working groups, which makes it possible to communicate programming strategies for encryption and decryption algorithms, and the use of steganography. In addition, it is also possible to share the mathematical concepts used, analysing and socialising the solutions found in order to institutionalise the concepts learnt.

1. Small groups are created, activity objectives are provided and discussed.
2. Commentary on algorithmics, mobile applications, digital photography and scratch.
3. Programming encryption and decryption algorithms for Polybius and Caesar with scratch [61], as well as the use of steganography to hide messages in photographs.
4. Strategies used to program algorithms are shared.
5. A recap or outline of the work completed is made.

5. Discussion

This paper presented the design of a general workshop for learning mathematics. Moreover, this proposal has been used to design a scientific workshop for a science museum in order to learn mathematics through cryptography.

The didactic conception of work is based on van Hiele's educational model. We have chosen an educational model to provide a global explanation of learning and we have chosen van Hiele's model specifically because in the museum we are able to experience the importance of language, both when it comes to communicating and teaching science. In

addition, despite being an idea raised by van Hiele in the middle of last century, today it is one of the pillars of educational innovation at a general level: that the student learns from their own experience.

For the didactic procedure, ten activities were programmed combining the characteristics of science museums, STEAM projects and mathematics learning.

Our greatest challenge has been to generate activities adapted to the established requirements simultaneously in their three aspects. Moreover, the educational level, the mathematical content and the language to be used must be adapted to each audience. According to our experience, as in the museum and in secondary school and university, the activities presented here can be adapted not only for the general public, but also for secondary school students and first-year engineering students. In addition, it is important to introduce activities in these types of workshops and projects that bring us closer to inclusive education. It is also necessary to contribute to reducing the gender gap in STEM degrees.

A further difficulty is the design of a STEAM workshop for mathematics learning, able to operate independently, and as part of a wider STEAM project.

Finally, it is important to highlight that dealing with some cryptographic concepts is not easy. The reasons for this are the didactic and epistemological issues raised by these concept introductions in secondary education. However, its introduction in the first year of computer engineering is much easier.

6. Conclusions

The extension of van Hiele's geometric reasoning model to other fields of mathematics education involves an adaptation of Hoffer's skills to the mathematical concept being learned. Therefore, we found it interesting to add digital and manipulative abilities for learning mathematics. In addition, the development of all these skills can be used to assess learning.

We may conclude that, as many studies show, it is a learning opportunity for teachers to design the museum visit as a part of a didactic intervention with their students based on STEAM strategy, starting and ending in the classroom.

It is interesting to complement the museum's workshops with STEAM activities pre- and post-visit, providing feedback from visitors' and teachers' opinions in order to update them.

Although a museum is not a school, and can welcome teacher's suggestions, it is not a substitute for laboratory practice or mathematics lessons. Some mathematical content can naturally be worked on better in relation to other disciplines, while others are more difficult to contextualise. When mathematics appears as a subsidiary of another subject it is easier. For example, applied mathematics have a more procedural aspect. Therefore, we must take care of the whole learning process. The interdisciplinary role of mathematics is on the last level of the pathway and not an unjustified intermediate step.

Museums and educational institutions should seek spaces for socialisation and discussion with teachers from other areas and institutions. We do this in order to favour the design of other didactic interventions with STEAM strategy, involving teachers and museum education managers.

Furthermore, we would also like to point out the significance of training, both for teachers and museum staff, regarding the implementation strategies of these types of activities and the importance of the language to be used. A mathematical concept achieves its meaning only for people who can understand and relate to it.

An active involvement in the proposed activities enables the exchange of different knowledge levels, results in a transformation of the students' skills and improves their motivational conditions.

We cannot consider this work as a completed process. In fact, science workshops can continue to be designed with activities that favour the learning of enriched mathematical concepts with the STEAM strategy. In addition, it would be interesting to design a research to evaluate the effectiveness of the proposal presented by implementing the same workshop

at different educational levels, as well as in order to study the results and implications. Moreover, it would be interesting to use Table 3 of the workshop activity design to develop a proposal to assess student learning.

Author Contributions: All authors declare they have equally contributed to the preparation of the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the internal funding of the Department of Statistics, Mathematics and Informatics and the Research Institute Centre for Operational Research.

Conflicts of Interest: The authors declare that they have no conflict of interest.

References

1. Hein, G.E. *Learning in the Museum*; Routledge: London, UK, 1998.
2. Falk, J.H.; Dierking, L.D. *The Museum. Experience Revisited*; Left Coast Press: Walnut Creek, CA, USA, 2013.
3. Allen, S. Designs for Learning: Studying Science Museum Exhibits that do More Than Entertain. *Sci. Educ.* **2004**, *88*, 17–33. [CrossRef]
4. Faria, C.; Guilherme, E.; Gaspar, R.; Boaventura, D. History of science and Science Museums: An enriching partnership for elementary school science. *Sci. Educ.* **2015**, *24*, 983–1000. [CrossRef]
5. Anderson, D.; Lucas, K.B.; Ginns, I.S. Theoretical perspectives on learning in an informal setting. *J. Res. Sci. Teach.* **2003**, *40*, 177–199. [CrossRef]
6. Guisasola, J.; Morentín, M. Primary and Secondary Teachers' Ideas on School Visits to Science Centres in the Basque Country. *Int. J. Sci. Math. Educ.* **2015**, *13*, 191–214. Available online: <https://link.springer.com/article/10.1007/s10763-013-9481-1> (accessed on 15 November 2022).
7. Koch, F.D.; Dirsch-Weigand, A.; Awolin, M.; Pinkelman, R.J.; Hampe, M.J. Motivating first-year university students by interdisciplinary study projects. *Eur. J. Eng. Educ.* **2017**, *42*, 1–15. [CrossRef]
8. Aravind, V.R. Inexpensive physics toys for demonstrations and hands-on learning. *Lat. Am. J. Phys. Educ.* **2015**, *9*, 10.
9. Warren, S.; Dondlinger, M.J.; Stein, R.; Barab, S. Educational Game as Supplemental Learning Tool: Benefits, Challenges, and Tensions Arising from Use in an Elementary School Classroom. *J. Interact. Learn. Res.* **2009**, *20*, 487–505. Available online: <https://www.learntechlib.org/primary/p/28349/> (accessed on 15 November 2022).
10. Aguilos, V.; Fuchs, K. The Perceived Usefulness of Gamified E-Learning: A Study of Undergraduate Students With Implications for Higher Education. *Front. Educ.* **2002**, *7*, 945536. [CrossRef]
11. Campos, H.; Moreira, R. Games as an educational resource in the teaching and learning of mathematics: An educational experiment in Portuguese middle schools. *Int. J. Sci. Math. Educ. Sci. Technol.* **2016**, *47*, 463–474. [CrossRef]
12. Cheung, S.Y.; Ng, K.Y. Application of the Educational Game to Enhance Student Learning. *Front. Educ.* **2021**, *6*, 623793. [CrossRef]
13. Edo, M.; Baeza, M.; Deulofeu, J.; Badillo, E. Estudio del paralelismo entre las fases de resolución de un juego y las fases de resolución de un problema. *Unión* **2008**, *14*, 61–75.
14. van Hiele, P.M. *Structure and Insight: A Theory of Mathematics Education*; Academic Press: New York, NY, USA, 1986.
15. Llorens, J.L. Aplicación del modelo de Van Hiele al Concepto de Aproximación local. Ph.D. Thesis, Universidad Politécnica de Valencia, Valencia, Spain, 1994.
16. Campillo, P. La Noción de Continuidad Desde la óptica del Modelo de Van Hiele. Ph.D. Thesis, Universidad Politécnica de Valencia, Valencia, Spain, 1999.
17. de la Torre, A.F. Modelización del Espacio y el Tiempo: Su Estudio vía el Modelo de Van Hiele. Ph.D. Thesis, Universidad Politécnica de Valencia, Valencia, Spain, 2000.
18. Esteban, P.V. Estudio Comparativo del Concepto de Aproximación Local vía del Modelo de Van Hiele. Ph.D. Thesis, Universidad Politécnica de Valencia, Valencia, Spain, 2000.
19. Jaramillo, C.M. La Noción de Serie Convergente Desde la óptica de los Niveles de Van Hiele. Ph.D. Thesis, Universidad Politécnica de Valencia, Valencia, Spain, 2000.
20. Navarro, M.A. Un estudio de la Convergencia Encuadrado en el Modelo Educativo de Van Hiele y su Correspondiente Propuesta Metodológica. Ph.D. Thesis, Universidad de Sevilla, Sevilla, Spain, 2002.
21. Prat, M. Extensión del Modelo de van Hiele al Concepto de área. Ph.D. Thesis, Universidad Politécnica de Valencia, Valencia, Spain, 2015.
22. Dreyfus, T.; Thompson, P.W. Microworlds and van Hiele levels. In Proceedings of the Ninth International Conference for the Psychology of Mathematics Education, Utrecht, The Netherlands, 22–29 July 1985; Volume 1, pp. 5–11.

23. Crowley, M.L. The van Hiele Model of the Development of Geometric Thought. In *Learning and Teaching Geometry, K-12, 1987 Yearbook of the National Council of Teachers of Mathematics*; Lindquist, M.M., Ed.; National Council of Teachers of Mathematics: Reston, VA, USA, 1987; pp. 1–16.
24. Jaime, A.; Gutiérrez, A. Una propuesta de fundamentación para la enseñanza de la geometría: El modelo de van Hiele. *Teor. Práct. Educ. Mat.* **1990**, 295–398. Available online: www.uv.es/angel.gutierrez/archivos1/textospdf/JaiGut90.pdf (accessed on 15 November 2022).
25. Jaime, A. Aportaciones a la Interpretación y Aplicación del Modelo de Van Hiele: La Enseñanza de las Isometrías del Plano. La evaluación del Nivel de Razonamiento. Doctoral Thesis, Departamento de Didáctica de la Matemática, Universidad de Valencia, Valencia, Spain, 1993.
26. Hoffer, A. Geometry is more than proof. *Math. Teach.* **1981**, 74, 11–18. [CrossRef]
27. Izzati, F.; Kusmanto, H.; Toheri, T. Pengaruh Penerapan Teori Van Hiele Berbantuan Software Wingeom Terhadap Kemampuan Penalaran Matematika Siswa pada Materi Geometri. *Inf. Technol. Eng. J.* **2016**, 2, 19–25. [CrossRef]
28. Theran, E. Pensamiento Geométrico, Teoría de Van Hiele y Tecnologías Computacionales. *Comput. Electr. Sci. Theory Appl.* **2021**, 2, 39–50. [CrossRef]
29. DuFour, R.; DuFour, R.; Eaker, R.; Many, T. *Learning by Doing. A Handbook for Professional Learning Communities at WorkTM*; Solution Tree: Bloomington, IN, USA, 2006.
30. Fernández, R.A. La enseñanza y aprendizaje de las matemáticas por medio del laboratorio 'Rurashpa Yachakuy. aprende haciendo'. *Mamakuna Rev. Divulg. Exp. Pedag.* **2018**, 8, 68–75.
31. Zollman, A. Learning for STEM literacy: STEM literacy for learning. *Sch. Sci. Math.* **2012**, 112, 12–19. [CrossRef]
32. Clavel, J.G.; Méndez, I.; Crespo, F.J.G. Are Teacher Characteristics and Teaching Practices Associated with Student Performance? *TIMMS Policy Brief* **2016**, 11, 1–8.
33. Domènech-Casalk, J.; Lope, S.; Mora, L. Qué proyectos STEM diseña y qué dificultades expresa el profesorado de secundaria sobre Aprendizaje Basado en Proyectos. *Rev. Eureka Sobre Enseñ. Divulg. Cienc.* **2019**, 16, 2203. [CrossRef]
34. Hoffstein, J. An Introduction to Cryptography. In *An Introduction to Mathematical Cryptography*; Springer: New York, NY, USA, 2008. [CrossRef]
35. Barton, D. *Cambridge Lower Secondary. Complete Mathematics 8*, 2nd ed.; Oxford University Press: Oxford, UK, 2021.
36. Barton, D. *Cambridge Lower Secondary. Complete Mathematics 9*, 2nd ed.; Oxford University Press: Oxford, UK, 2021.
37. McKelvey, L.; Crozier, M. *Cambridge International AS and A Level Mathematics. Further Mathematics Coursebook*; Cambridge University Press & Assessment: Cambridge, UK, 2019.
38. Rayner, D.; Bettison, I.; Taylor, M. *Complete Mathematic for Cambridge IGCSE*, 5th ed.; Oxford University Press: Oxford, UK, 2018.
39. Koblitz, N. *A Course in Number Theory and Cryptography*, 2nd ed.; Springer: New York, NY, USA, 1994.
40. Semaphore Flag Signaling System. Available online: <https://www.anbg.gov.au/flags/semaphore.html> (accessed on 11 September 2022).
41. Carron, L.P. *Morse Code: The Essential Language*, 2nd ed.; American Radio Relay League: Newington, CT, USA, 1991.
42. N8_ModPublisher. *Morse Code Book. For kids. Learn and Practice*; Independently Published: Chicago, IL, USA, 2021.
43. Fascinating Facts about Hieroglyphics. Available online: <https://www.natgeokids.com/uk/discover/history/egypt/hieroglyphics-uncovered/> (accessed on 11 September 2022).
44. La Escitla. Available online: <http://www.ugr.es/~janillos/textos/pdf/2010/EXPO-1.Criptografia/02a22.htm> (accessed on 11 September 2022).
45. Strang, G. *Introduction to Linear Algebra*, 5th ed.; Wellesley Cambridge Press: Wellesley, MA, USA, 2021.
46. Philips, G.M. *Interpolation and Approximation by Polynomials*; Springer: New York, NY, USA, 2011.
47. Wagensberg, J. The “total” museum, a tool for social change. *Hist. Cienc. Saude. Manguinhos.* **2005**, 12, 309–321. [CrossRef]
48. Drioli, A. Contemporary aesthetic forms and scientific museology (Italian original version). *JCOM J. Sci. Commun.* **2006**, 5, 1–10. [CrossRef]
49. Enigma/Paper Enigma. Available online: http://wiki.franklinheath.co.uk/index.php/Enigma/Paper_Enigma (accessed on 17 September 2022).
50. Parakh, A.; Subhash, K. Space efficient secret sharing. *Inf. Sci.* **2011**, 181, 335–341. [CrossRef]
51. Mao, W. *Modern Cryptography: Theory and Practice*; Pearson Education: Bengaluru, India, 2003.
52. Trappe, W. *Introduction to Cryptography with Coding Theory*; Pearson Education: Bengaluru, India, 2006.
53. Gennaro, R.; Jarecki, S.; Krawczyk, H.; Rabin, T. Robust and Efficient Sharing of RSA Functions. *CRYPTO'96* **1996**, v, 157–172.
54. Gennaro, R.; Rabin, T.; Krawczyk, H. RSA-Based Undeniable Signatures. *J. Cryptol.* **2000**, 13, 397–416. [CrossRef]
55. Center of Excellence for Women & Technology. Available online: <https://womenandtech.indiana.edu/programs/cybersecurity/profiles-current-trailblazers/rabin.html> (accessed on 20 September 2022).
56. Forbes, Tal Rabin. Available online: <https://www.forbes.com/profile/tal-rabin/?sh=52ac941f131b> (accessed on 22 September 2022).
57. Tal Rabin on the History and Future of Women in Data Science. Available online: <https://blog.seas.upenn.edu/tal-rabin-on-the-history-and-future-of-women-in-data-science/> (accessed on 22 September 2022).
58. Swafford, M.; Anderson, R. Addressing the Gender Gap: Women's Perceived Barriers to Pursuing STEM Careers. *J. Res. Tech. Careers* **2020**, 4, 61–74. [CrossRef]

59. Celebrating Female Cryptologic Pioneers During National Women's History Month & All Year Long! Available online: <https://cryptologicfoundation.org/what-we-do/stimulate/women-in-cryptology.html> (accessed on 25 September 2022).
60. Teicher, A. Mendel's use of mathematical modelling: Ratios, predictions and the appeal to tradition. *Hist. Philos. Life Sci.* **2014**, *36*, 187–208. Available online: <http://www.jstor.org/stable/44471280> (accessed on 15 November 2022). [[CrossRef](#)] [[PubMed](#)]
61. Esteve-Romero, A. Arqueología Informática: Implementación de Sistemas Clásicos de Cifrado en Scratch. Doctoral Dissertation, Escola Tècnica Superior d'Enginyeria Informàtica, Universitat Politècnica de Valencia, Valencia, Spain, 2019. Available online: <https://riunet.upv.es/handle/10251/124727> (accessed on 15 November 2022).