MATH LEARNING THROUGH CLASSIC CRYPTOGRAPHY

M. Martínez-Muñoz[1]

[1] *Mechanical Engineering Area, Universidad de Alcalá (SPAIN)*

Abstract

The sure transmission of information has turned into a priority and increasing need. The codification and encryption is the protocol of the flow of information. Most of the university students have worse assimilation of the mathematical concepts in comparison with other subjects. In addition, the scientific language that is in use, together with the numerous formulae, generates lack of interest in the students. In this document, a multidisciplinary project is presented, Crypto Math, focused on cultivating the taste for the science, especially the mathematics, across the classic cryptography. Its principal aim is to discover encrypted tracks and secret codes by means of mathematical concepts.

Keywords: math and science learning, cryptography.

1 INTRODUCTION

The cryptography is the science that deals with the technologies to transform a flat text into a ciphered text.

From the Former Egypt, the man has had the need to conceal information for diverse reasons, not only military men. This has caused the appearance and development of technologies, increasingly complex, to encrypt information. The hieroglyphs, Spartan Escítala, coding of Polybus, Julio César, Atbash method, visual cryptography up to the machine Crux German in the Second World War, are methods of coding that are based on the application of mathematical concepts.

For example: counterfoils, graphs, coloration of maps, binary system, binary sum, permutations, combinations, prime numbers, greatest common divisor...

The Cryptography is a Science that, together with the Cryptanalysis and the Steganography, exists since the writing appeared. Along the history, the civilizations have had the need to conceal the information, supporting its integrity.

Crypto-Math is a workshop destined to a public of top studies, who by means of a gymkhana (using the most significant cryptographic as hieroglyphic methods, coding Polybus, coded of Julio César, Atbash, Crux and Albert i's Disc) with ciphered tracks, allows to discover a scientific mystery.

Crypto Math is a multidisciplinary activity directed to cultivating the taste for the science, especially the mathematics, across secret codes. The development of this idea tries to reach the following aims:

· To promote the spreading and the social communication of the mathematics.

· To stir into action the education of this science, incorporating active methodologies doing a tour for the history of the cryptography.

· To promote the innovative and enterprising spirit between the student body.

2 METHODOLOGY

Along the history and up to entered good the 20th century the cryptography was principally used in the areas diplomatically and militarily. The habitual use of the computers and the great quantity of information have done that the cryptography extends his horizons. Practically any company of average size meets obliged to use cryptography to protect his information. Not using her can be an object of industrial espionage.

The assaults of hackers are famous to all kinds of computers, including those of "companies" as big as the same Pentagon. Even the user of afoot would use great more cryptography if it was conscious of the assaults that his computer receives daily with intention of extracting information. The base of the modern cryptography is the classic cryptography, which has his foundations in mathematical concepts.

With Crypto-Math one tries to develop a new methodology of education - learning of the mathematics, principally in the University. By means of a series of tests encrypted with diverse technologies of encryption, the students solve cruxes. Initially, one explains the different methods of encryption, with his mathematical base, and the different malingerers who exist in the network. Later, they the gymkhana appears in order that they put into practice the acquired knowledge.

ESCAPE THE CITY OR GYMKHANA

The following game consists of realizing 5 tests distributed along 4 zones known about the city (Plaza of the Town hall, Park of the Concord, Palace of the Infantado and Plaza of Carmen). The tests will have to be realized in a certain order, for it, the resolution of a test will give a track to find the place in which to realize the following test.

All the participants will have Vigenère table. The first test will have as purpose that the participants familiarize themselves with the managing of Vigenère table that will have assigned them. In the polyalphabetic coding to a certain letter of a message they can correspond to him so many assignments like ciphered alphabets want to use. The insole of coding of Vigenère consists of a flat alphabet of n characters under which ciphered alphabets are distributed n, each of them displaced a letter to the left side.

VIGENERE TABLE

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

Figure 1 - Vigenère table

The managing of the table is very simple. The table is composed of 26 rows x 26 columns and is the same for all the participants. Besides supplying the table them, there is supplied them the key word, which in this case is the word "SCIENCE". The resolution of the test will give them the ciphered message that they will have to decipher. And how do they decipher it? Let's imagine that the ciphered message that they obtain after the resolution of the first test is "PMTGWVO". They arrange it in such a way that they coincide, the first letter of the key word with the first letter of the ciphered code, with this case, C of SCIENCE with P of PMTGWVO and so on. Later, it is looked in the column of the letter C, the first position of the letter P and they obtain the first letter of the word that they are deciphering looking at the row in which they find, in this case, the letter N.

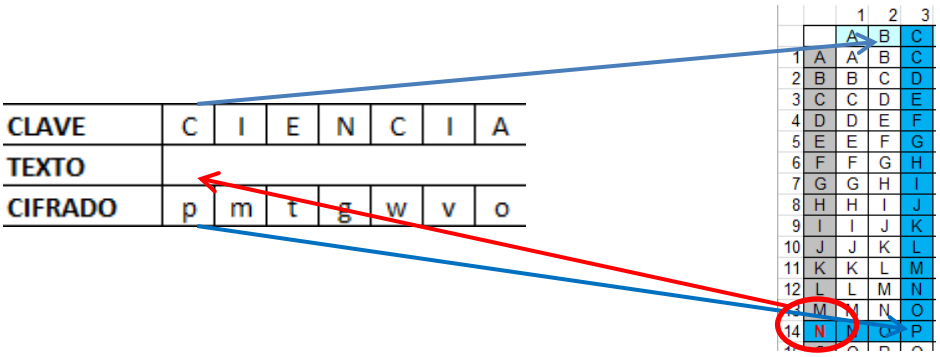

Figure 2 – Example

FIRST TEST

Since already we have commented previously, the purpose of this test consists of familiarizing with the managing of the table and the key of Vigenère. It will consist of solving a crossword answering to the questions that later they present:

1. Who did discover the three laws that dominate the orbits of the planets?
2. His equations describe how the electrical and magnetic fields are.
3. He explained the Brownian movement, the photoelectric effect and the special relativity.
4. He described the metaphor of the cat that one finds inside a box it can have died or not for the effect of a capsule of poison.
5. Who said that all the bodies attract between the force of the gravity and the intensity of this force declines with the square of the distance
6. He developed the electrical battery.
7. The effect of diminishing the tone of the siren of an ambulance on having gone on to our side was enunciated by the following man.
8. Password:

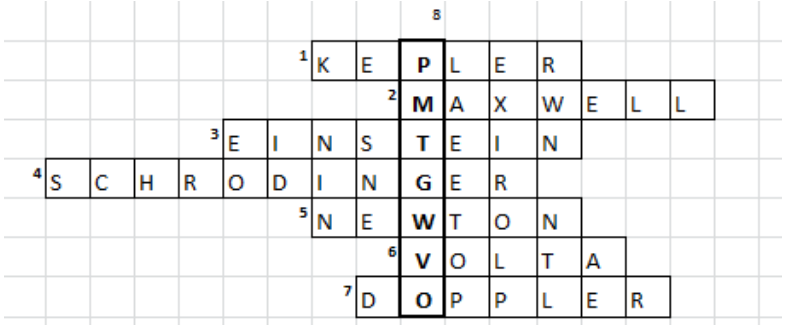

Figure 3 – Password

Depending on the age of the participants they might raise other questions.

Ultimately there is obtained a key encrypted word and thanks to the table they obtain the word for that they look: NEPTUNE. This word indicates the place which they have to approach to realize the second test. They have to approach the source of Neptune in the Plaza of Carmen.

SECOND TEST

Neptune is to 4.495 billion kilometers of the Sol, is the most remote planet, before it was Pluto, now considered as a dwarf planet. His revolution is very long: 165 years. The diameter of Neptune is approximately 49.500 kilometers, a bit less than the diameter than Uranus, but 4 times that of the Earth. His mass corresponds to 17 times the mass of the Earth. It is a gaseous planet, constituted in the main of hydrogen and helium.

And to see the above mentioned influence we will realize a compass of paper. We will need a cavity, a thin paper or a cork, a needle or a nail and a magnet of those who sell in hardware stores, the magnets of the icebox are not in the habit of being it sufficiently powerful. To make the compass, the only thing that we need is to fill a water container, to rub a needle or a nail in a magnet during approximately 30 seconds, always in the same sense and later we stick it in a cork with a chunk of zeal or adhesive tape. Once stuck, we will put the cork in the water and immediately it will be orientated marking the north. We can replace the cork with a chunk of paper in which we cross the needle as if we were giving a point of seam.

The steel of the needle contains particles of iron orientated of random form. On having rubbed the magnet with the needle what we do is magnetize, or what is the same thing, to orientate the particles of iron of the needle in the same direction. The existing iron inside the Earth acts as a giant magnet and believes his magnetic field. The needle lines up with the magnetic field and acts as compass indicating in the direction north - South.

As soon as it is orientated in the correct direction, the participants will have to search in the direction that marks the needle something that are going to need for the following test. He had thought about the keys of a few padlocks that they will be in the following location. Close to the keys an encrypted code will appear. The encrypted code will be "MQSFMWCQVGBTLIC" and his translation will give the location of the third test “KIOSK CONCORDIA”

CLAVE	C	I	E	N	C	I	A	C	I	E	N	C	I	A	C
TEXTO	k	i	o	s	k	o	c	o	n	c	o	r	d	i	a
CIFRADO	m	q	s	f	m	w	c	q	v	g	b	t	l	i	c

Figure 4 – Example.

THIRD TEST

As soon as they come to the kiosk of the Concord, they will find a few boxes closed with a padlock. The key that they gathered in the second test will serve them to open the padlock and to see what exists inside the boxes. The first thing that they will find will be a phrase that it they will put in situation: “IF YOU WANT TO REALIZE THE FOLLOWING TEST, NEWTON HAS TO EXAMINE YOU “Isaac Newton was the first one in establishing a relation between the force, the mass and the acceleration in the shape of equation. Also it is famous for observing how they fall the apples of the trees.

Newton realized first observations, later it developed conceptual models of what it had observed and finally it expressed these models by means of the use of the mathematical language. And it ended up by enunciating those who today know themselves as Newton's Laws.

The terms of reference of the Newton's first law (law of the inertia) say “Any object preserves his condition of rest or his condition of movement to a constant speed and on line straight, until a clear force forces it to change condition ".

It is important to notice that the logic leads to us to thinking in the opposite direction, that is to say, the majority of the things about movement they finish stopping. The idea of that all the objects in movement have a natural trend to stop belongs to Aristotle. Newton had to come, 2000 years later to refuting him. Simply one tries to notice the perspicacity that Isaac Newton had to have to deduce that the natural condition of the movement consists of continuing actually in movement on line straight to a constant speed. The Newton's first law affirms that the only way of which something should change movement consists of applying a force to him.

To visualize of what it consists the first law the following material will be given to the participants: a glass of crystal, a strip of paper and a currency. One will ask them, with these materials how can we demonstrate the Newton's first law? The idea is that they put the currency on the edge of the glass and on the paper and withdraw the paper in such a way that the currency stays in touch with the glass in the same position in which we put it initially, that is to say, in the edge of the glass.

The correct resolution will do that there is given them the first part of the encrypted text "RIXVQ", whose translation is “PATIO".

Later they should give response to the following question why is mass a measure of the inertia? To understand it we are going to have two balls, a ball of Ping-Pong and a ball of football. If we apply the same clear force to both balls, the ball of Ping-Pong will move with facility whereas the ball of football will move slower. This is due to the fact that each one has a different mass and therefore a quantity of different inertia. Less mass, less inertia; more mass, more inertia.

And finally, they will realize a test that will go for name “THE MASS AND WEIGH ". The mass is not the same thing that the weight, the mass is a measure of the inertia and when we place a mass inside a gravitational field, we obtain the weight. If you were travelling to the Moon you would weigh more, would weigh less than in the Earth? And if you were travelling to Jupiter you would weigh more, would weigh less than in the Earth?

The weight depends on the force of the gravity that it attracts to your mass. Our mass will be the same in all the sites, but in the Moon, the gravity is a 1/6 the gravity of earth for what we would weigh a sixth part of what indicates the scale in the Earth. But in Jupiter, a planet 318 times heavier that the Earth, our weight would be the equivalent to more than two times and average what we weigh in the Earth. If we had an elevator we might introduce a scale in the same one and rise and go down, in order that they saw since it changes the indicator of the scale depending on which it adds or reduces the acceleration of the elevator.

With the balls (the ideal thing would be 3, one of basket, other one of rubber of the size of a ball of handball and the ball of Ping-Pong) we might present the linear moment and they raise the challenge of if only we leave you touch the big ball might you do that the ball of Ping-Pong was ascending over the kiosk? The solution would happen for putting the ball of Ping-Pong on the ball of rubber and this one on the ball of basket and to give up them. The linear moment would enter game and would throw the ball of Ping-Pong to a considerable height.

In any case, it is the test that is; they would obtain the second part of the encrypted message. This second message would be "TEQVIF” that translated "LIONS". The complete message would be A COURT FROM LYON; they would have to go to the Palace of the Infantado to realizing the last test before returning to the Plaza of the Town hall.

FOURTH TEST

Light dispersion.

The rainbow is a special example of refraction: the light of the Sun turns aside on having crossed the drops of rain, but not all the colors are reflected of the same form, which does that on having gone out of the water drops, every color goes out separately and them we all could distinguish. Seven basic colors are distinguished in the spectrum: red, orange, yellow, green, blue, indigo and violet.

To check the dispersion of the light, we will need a black cardboard, a lantern and a CD without mask. The CDs act as networks of diffraction. A network of diffraction is an optical element with a regular boss, who divides the light and does that they travel in different directions. The CDs have some 700 lines/mm.

Once realized the experience and sight the dispersion on the CD, the colors will be identified and the participants will choose a color. The idea is that we have globes with the colors of the rainbow (7 globes minimum) and in one o more of them a key interferes and a message that THE BEGINNING puts “IS THE MOST IMPORTANT PART OF THE WORK (Plato) ". They should fall down in that they have to return to the Plaza of the Town hall. There they are waited by a box that will be opened by the key that they bring. Inside it would not be able say to you what to put, if a book, a key type key of the city. I think that there should be so many books, keys, etc … as participants, but I understand that it is going to be complicated.

A last comment, the globe that they choose we can say to them that they should puncture it or it is possible to ask them to try to cross with a needle of sewing or a stick of skewer and that they take it to him this way up to the square of the Town hall, in the latter case, the message should them give in hand as soon as they had crossed the globe.

The ends of the globe are of a darker colour because the rubber in these points is not so stretched like in the rest of the globe, which allows them a certain flexibility to be able to be deformed without managing to break. If we were puncturing in any other point of the globe with the same small stick, it would exploit to the instant.

3 CONCLUSIONS

This work has allowed us to know the impact of a game or gymkhana has in the process of teaching and learning. It is shown that the application of cryptography resources to represent information contributes to improving comprehensive learning of the physical concepts.

The project shows that the use of a visual methodology helps to fix and support for a long time the acquired knowledge.

REFERENCES

References [Arial, 10-point, left alignment, upper and lower case] should be cited according to the Bibliography and Citation Style https://iated.org/citation_guide

[1] Raúl Santiago, Alicia Díez, Luis Alberto Andía, “Flipped Classroom: 33 experiencias que ponen patas arriba el aprendizaje”, Outer Edu.

[2] C.J. Wnning, “Implementing inquiry-based instruction in the science classroom: A new model for solving the improvement-of-practice problem”, Journal of Physics Teacher, Education Online 2, 2005.

[3] Ian Abrahams, Michael J. Reiss & Rachael M. Sharpe (2013) The assessment of practical work in school science, Studies in Science Education, 49:2, 209-251, DOI: 10.1080/03057267.2013.858496