Generalitat de Catalunya
Departament d'Educació

MASTER'S DEGREE
CLIL & FLE
CONTENT AND LANGUAGE INTEGRATED LEARNING - FOREIGN LANGUAGE EDUCATION

UAB
Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació

Let's discover secrets!

Institut Ramon Casas i Carbó
Patricia Tena Zaforas and Andrea Esteve Recatalà

Generació Plurilingüe (GEP)
Year 2
2019-2020

Els materials creats en el marc de la formació del programa GEP pertanyen a l'autor/a amb una llicència creative commons CC BY-NC-SA:

Reconeixement - No Comercial - Compartir Igual

Identification of the GEP project

Title	Let's discover secrets
Authorship	Patricia Tena Zaforas and Andrea Esteve Recatalà
School	Institut Ramon Casas i Carbó
Students' CEFR Level (A1, A2...)	A1
Grade	2nd ESO
Content area(s)	Maths, Geography, History, Science
Number of sessions (4, 6 or 9)	6 sessions
Teacher(s) involved	Patricia Tena Zaforas and Andrea Esteve Recatalà
Keywords	Cryptography, Key, Upper case, Lower case, Decode, Encode, Julius Caesar, Encryption, Vigenère cypher, Greatest Common Divisor (GCD), Analysis of frequency.

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

1. OUR PROJECT

Introduction:
Analysis of cryptography throughout the times.

Driving question:
How can you be a good spy?

Final product:

Poster's conference with mind maps (format chosen by students) that they decorate themselves hung in the high school corridors. The posters will have the shape of the UK countries and the mind-maps will be about the content about cryptography and English covered in the six sessions.

2. GOALS	2. HOW DO YOU KNOW STUDENTS ARE MAKING PROGRESS? (assessment criteria)
1. Encode and decode messages with main methods used throughout times.	1.1. Distinguish different encryption methods.
2. Define the evolution of cryptography from the military world in ancient times to daily life nowadays.	2.1. Create a mind map with the most relevant information about the evolution of cryptography covered in these sessions.

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya Departament d'Educació
MASTER'S DEGREE CLIL & FLE
LED
UAB Universitat Autònoma de Barcelona Facultat de Ciències de l'Educació

3. Be able to identify the maths involved in messages encryption.	3.1 Include in the mind map the mathematical elements that cryptography involves.

3. CURRICULUM CONNECTIONS
SPECIFIC COMPETENCES AND KEY CONTENTS

Subject-matter curriculum (Mathematical field)		Foreign language curriculum (Linguistic field)	
Specific Competences	**Key Contents**	**Specific Competences**	**Key Contents**
• Problems resolution dimension: **Competence 3**: Keep an attitude of research in front of a word problem rehearsing diverse strategies.	**Maths** 1. Analysis of frequency. 2. Greatest common number. **Geography** 1. UK flags.	o Oral dimension: - **Competence 2**. Plan and produce oral texts from diverse typology according to the communicative situation. - **Competence 3**. Choose interactive strategies in terms of communicative	1. Vocabulary related to cryptography. 2. Comprensió oral: global, literal i interpretativa. 3. Estratègies de comprensió oral. 4. Estratègies de producció oral. 5. Estratègies d'interacció oral. 6. Lectura en veu alta. 7. Comprensió escrita i interpretativa. 8. Cerca i gestió de la informació i la consulta

CC BY NC SA

- CC3: Calculation (mental, estimation, algorithmic with calculator). - CC5: Patterns, relations and functions. ● Reasoning and tests dimension: **Competence 6**: Employ the mathematical reasoning in non-mathematical surroundings. - CC13: Statistical sense. ● Connections dimension: **Competence 8**: Identify the mathematicians involved in the near and academic situations and look for situations that can be related		situation to initiate, keep and end the speech. o Reading dimension: - **Competence 4**. Apply comprehension strategies to obtain information and interpret written texts with a clear structure from daily life, means of communication and of the academic field. o Written dimension: - **Competence 7**. Plan written texts from diverse typology using elements from the communicative situation. o Literary dimension:	lingüística. 9. Estratègies de revisió, correcció, reparació i presentació. 10. Producció creativa. 11. Textos orals, escrits i audiovisuals.

BY NC SA

with specific mathematical ideas. - CC2: Proportional reasoning. - CC15: Statistical methods of analysis of data. Communication and representation dimension: - Competence 11. Employ the communication and the collaborative work to share and build knowledge from mathematical ideas. - CC1: Numeral sense and operations one. - CC6: Representation of functions: graphic, tables and formulas.		- **Competence 11.** Comprehend and consider literary texts (adapted or authentic). o Transversal, attitudinal, and plurilingual dimension: - Use non-verbal language.	

BY NC SA

4. 21st CENTURY COMPETENCES			
Collaboration	X	Information, media and technology	**X**
Communication	X	Leadership & Responsibility	**X**
Critical Thinking and Problem Solving	X	Initiative & Self-direction	**X**
Creativity & Innovation	X	Social & Cross-cultural	**X**
Others:			

5. KEY COMPETENCES			
Communicative, linguistic and audiovisual competence	X	Digital competence	X

CC BY NC SA

Mathematical competence	X	Social and civic competence	X
Interaction with the physical world competence	X	Learning to learn competence	X
Cultural & artistic competence	X	Personal initiative and entrepreneurship competence	X

6. CONTENT (Knowledge and Skills)	
CONTENT-RELATED KNOWLEDGE	**CONTENT-RELATED SKILLS**
1. Cryptography throughout history. 2. Methods for encoding and decoding messages. 3. Math's implication in cryptography (Analysis of frequency and Greatest Common Divisor).	1. Recognising different methods of encoding and decoding messages throughout history. 2. Analysing different methods of decrypting hidden messages. 3. Creating encoded messages and decode them. 4. Interacting in English with the colleagues while performing the task.

BY NC SA

	5. Developing their critical thinking.

7. REFERENCES

Khan, D. (1996) The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. New York. Scribner

Singh, S. (2000). Los códigos secretos. Madrid. Debate

Gómez J. (2010) Matemáticos, espías y piratas informáticos. Barcelona. RBA, S.A.

https://learnenglishkids.britishcouncil.org/reading-practice/the-uk
https://www.pinterest.com/pin/417568196675516822/

8. COMMENTS (optional)

As a final comment, it is worth mentioning that his project can be made so much more extensive since all the content is so wide that it's possible to cover it in depth.

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

9. ACKNOWLEDGEMENTS (optional)

It is important to acknowledge the presence on this project of the science teacher M. Àngels Alié Capdevila in session 5 for offering the support and collaboration on science needed to carry out the workshop.

Skills: R: reading , S:speaking, L: listening, W: writing, I: Interaction
Interaction: T-S: teacher-student, S-S: student-student, SG: small groups, WG: whole group, S-Expert, S-World
Assessment: PA: Peer assessment, SA: Self-assessment, TA: Teacher assessment, AT: Assessment tools

10. UNIT OVERVIEW

Session	Activities	Timing	Skills	Interaction	ICT	Assessment

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

1	**Activity 1**: Breakout	1h	R, S, L, I	T-S SG	Genially	TA
2	**Activity 2** - Initial explanation of cryptography	15 min	R, L	T-S WG	Ppt	
	Activity 3 - Have you understood what crypto is?	15 min	R, S, I	T-S SG		PA
	Activity 4 - Encode messages with Caesar Cipher: **4.1** How is it made? **4.2** Do you dare to try it on your own?	15 min	R, S, L, W, I	T-S S-S	Ppt	PA
	Activity 5 - Instructive text	15 min	R, L, S, W	Ind		TA
3	**Activity 6** - Arabian cryptanalyst **6.1** – Explanation:	10 min	R, L	T-S WG	Ppt	

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

	6.2 – Mathematical website: Thatquiz for the bar chart	15 min	R, S, L,	Ind	Thatquiz Google Drive	TA
	6.3 – Create a bar chart	15 min	R, S, I	S-S, SG		SA
	6.4. – Finally, students decode a message using the frequency analysis.	20 min	R, L, W, S, I	S-S, SG		SA
4	**Activity 7** - Vigenère cipher: **7.1.** Vigenère cipher explanation.	10 min	L, S	T-S WG	Ppt	
	7.2 - Encode a message with Vigenère cypher.	10 min	R, S, L, W, I	SG S-S		SA
	7.3 – Voicethread about Vigenère cypher.	15 min	R, S, L, W, I	S-S	Voicethr ead	PA
	Activity 8 – Greatest Common Divisor (GCD)	10 min	R, S, L, I	T-S	Ppt	

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

	8.1 – Babbage explanation					
	8.2 – Greatest Common divisor	15 min	R, W	Ind		PA
5	**Steganography and Invisible Ink Workshop: Explanation**	10 min	L	T-S S-S WG	Ppt	
	Activity 9: Secret messages with lemon juice	8 min	R, L, W	SG		TA
	Activity 10: Secret messages using milk	8 min	R, L, W	SG		TA
	Activity 11: Secret messages using vinegar	8 min	R, L, W	SG		TA
	Activity 12: Secret messages with sodium bicarbonate	8 min	R, L, W	SG		TA
	Activity 13: Think, discuss and share. How it works. Assessment: Checklist with activities from 8 until 12	18 min	S, L, I	SG		TA
6	**Reading Task: The UK**					

CC BY NC SA

	Activity 14: Reading Comprehension	5 min	R, S, L	T-S; S-S; WG	Genially	TA
	Activity 15: Reading comprehension: Survey Monkey	5' min	R, W,	Ind	Survey Monkey	TA
	Activity 16: Presentation poster's conference	20 min	R, S, L, W, I	S-S SG		TA
	Activity 17. Posters' conference	30 min	S, L, I	S-S S-WG		TA

11. SESSION PLANNING

SESSION 1: Activating session - Breakout

Objectives of the session: This session aims at approaching the notion of cryptography and encrypted messages. A brief insight is provided in this session by carrying out a breakout session. This session also has the following objectives: positive critical and creative thinking, cooperative learning, gamification, and learning based on challenges.

CC BY NC SA

Content-obligatory language for the session:

- Academic language. Keywords: Encode, decode, plain text, key, lower case, upper case, below, cylinder, plus, less, times, over.
- Instructional text (e.g. the clues for this breakout are instructions for the students to follow for obtaining the code of the box).
- Explanatory text (e.g. the story that there is behind the game of the breakout).
- Academic language: discursive connectors (i.e. present in the explanatory text, the main story of the breakout, so, moreover, etc).
- Grammar items determined by the tasks and topic: Imperative (i.e. instructions, sum up, multiply, etc).
- Grammar items determined by the tasks and topic: Past tenses (e.g. narration of the story: stole, entered the house, robbed, etc).
- Interactive strategies: (e.g. Language support: Where is it? We got it!, etc).

Activities

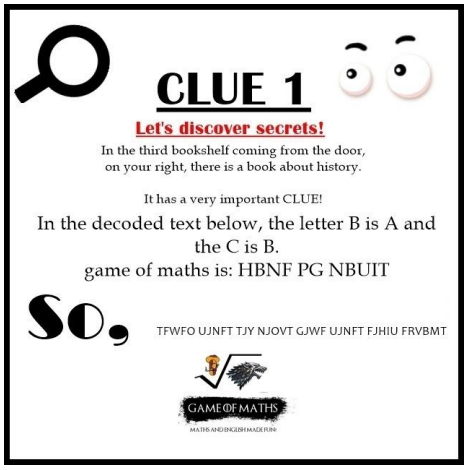
BY NC SA

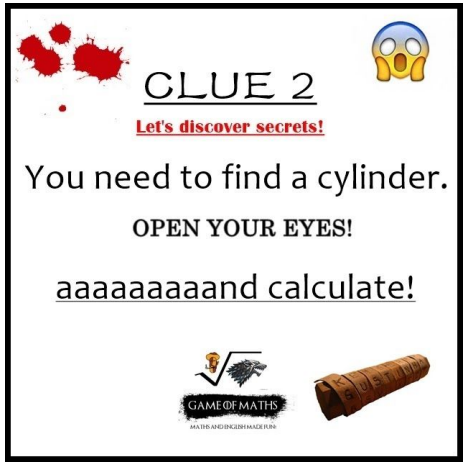
1.1	**Activity 1 - Breakout:** The aim of this breakout is introducing them to the concept of hiding messages, finding codes, and obtaining the key. These are the main objectives of cryptography. Therefore, this breakout is used as a metaphor for students to internalise the main objective of cryptography. Through this dynamic technique, students are hooked and in the mood of being good spies, which is the main idea of this project's driving question. The activity will be performed in the library where two groups will have to follow some clues. They are shown below:	1h	R, S, L, I	T-S SG	Ge niall y	TA

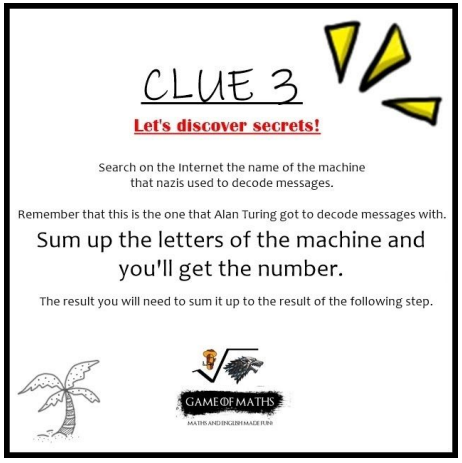
BY NC SA

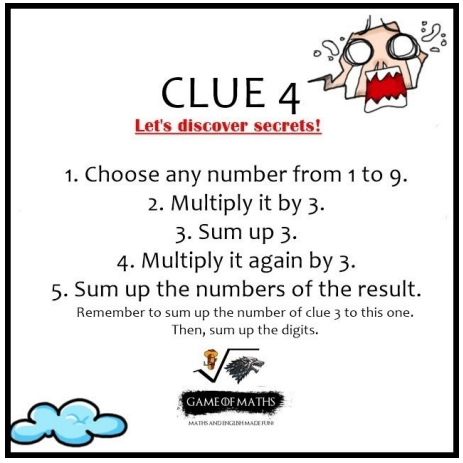
CLUE 1
Let's discover secrets!
In the third bookshelf coming from the door, on your right, there is a book about history.
It has a very important CLUE!
In the decoded text below, the letter B is A and the C is B.
game of maths is: HBNF PG NBUIT
So, GJWF QMVT UXP FRVBMT
GAME OF MATHS

CLUE 1
Let's discover secrets!
In the third bookshelf coming from the door, on your right, there is a book about history.
It has a very important CLUE!
In the decoded text below, the letter B is A and the C is B.
game of maths is: HBNF PG NBUIT
So, UISFF QMVT OJOF FRVBMT
GAME OF MATHS


CLUE 1
Let's discover secrets!
In the third bookshelf coming from the door, on your right, there is a book about history.
It has a very important CLUE!
In the decoded text below, the letter B is A and the C is B.
game of maths is: HBNF PG NBUIT
So, TFWFO UJNFT TJY NJOVT GJWF UJNFT FJHIU FRVBMT
GAME OF MATHS


CLUE 2
Let's discover secrets!
You need to find a cylinder.
OPEN YOUR EYES!
aaaaaaaaand calculate!
GAME OF MATHS


CLUE 3
Let's discover secrets!
Search on the Internet the name of the machine that nazis used to decode messages.
Remember that this is the one that Alan Turing got to decode messages with.
Sum up the letters of the machine and you'll get the number.
The result you will need to sum it up to the result of the following step.
GAME OF MATHS


CLUE 4
Let's discover secrets!
1. Choose any number from 1 to 9.
2. Multiply it by 3.
3. Sum up 3.
4. Multiply it again by 3.
5. Sum up the numbers of the result.
Remember to sum up the number of clue 3 to this one.
Then, sum up the digits.
GAME OF MATHS

BY NC SA

They are the steps to follow to find out the key for opening the lock of the boxes. Each group has to solve four clues. The clues contain cryptography methods used to decode messages throughout times.

Students will need to discover who the robber of the pearl necklace is. This pearl necklace is part of the materials of the breakout. It is shown below:

BY NC SA

The development of the breakout is explained deeply in the following section.

FURTHER EXPLANATION OF THE BREAKOUT ACTIVITY

The class is divided into two teams: A and B. There are two tables with a poster indicating which group this table belongs to. This title has the letter format with the "Game of Thrones" making reference to the "Game of Maths", which is the subject this breakout takes place in.

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya Departament d'Educació
MASTER'S DEGREE CLIL & FLE
UAB Universitat Autònoma de Barcelona Facultat de Ciències de l'Educació

There are two wooden boxes with a numbered lock with three digits. The guiding thread of the breakout is a robbery. Thus, by following all the clues, they can open the wooden boxes that will stay who the robber was and they will also find the collar of Elizabeth I of England.

In **"Clue 1"**, **TEAM A** has this coded message: **GJWF QMVT UXP FRVBMT,** which will correspond to the first number of the lock. The solution is: FIVE PLUS TWO EQUALS 7. Seven is the first number to unlock the box.

In **"Clue 1"**, **TEAM B** has this coded message: **UISFF QMVT OJOF FRVBMT,** which will correspond to the first number of the lock. The solution is: THREE PLUS NINE EQUALS, 12; 1+2= 3. Three is the first number to unlock the box.

In **"Clue 2",** it is the case of the "Spartan scytale", which you can see represented in the game in the following image. The image on the left is the official Spartan scytale and the image on the right represents the materials created by us making reference to the Spartan scytale. The idea of the Spartan scytale consists of rolling a tape on a cylinder and, by choosing the right one, they can read a hidden message. It also connects with the idea that Spartan Greeks used the inner part of their belts to hide messages.

BY NC SA

There is more than one cylinder (spray, aluminium roll, cylindrical roll) to emphasise the idea that the diameter is very important to decode the message since if the students choose the wrong cylinder it is not possible to read the message in the tape.

The other objects that are cylindrical are distractors since not all the cylinders correspond to the tapes, making the reading of the tape impossible to read, and impossible to decode.

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya Departament d'Educació
MASTER'S DEGREE CLIL & FLE
UAB Universitat Autònoma de Barcelona Facultat de Ciències de l'Educació

	Group A can read the message in a wide diameter cylinder (the round box). Group B can read the message by rolling up the tape to the little diameter aluminium cylinder. Group A has the following message: "Six times seven equals to". You must sum up the digits until there is only one. The solution is 6x7=42; 4+2= 6; 2nd digit of the lock: 6. Group B has the following message: "Five times seven equals". They should sum up the digitS, The solution is 5x7=35; 3+5=8; The second digit of the lock is 8. In **Clue 3**, it is the same one for the two groups. In this one, the students need to use the computer to find the name of the machine that the Nazis used in the II World War which Alan Turing achieved to crack the code with. They need to sum up the letters and they will obtain one number. The solution is 6 because the name is "Enigma". The number obtained will need to be sum up to the result in the following clue.					

BY NC SA

	In **Clue 4,** students need to choose a number from 1 to 9, then multiply it by 3, and sum 3. Then, multiply it again by 3 and sum up the digits of the result. In this case, it will always be 9. The solution is 6+9=15; 1+5 = 6. Therefore, the third digit is 6. The lock numbers are: - For GROUP A: 7 6 6 - For GROUP B: 3 8 6 Moreover, this is the main story of the breakout. The story will be shown in the screen, So, this text will be read by each student. This is the **explanatory text** part of the COL: A terrible event has happened! You could NEVER imagine what it is. A terrible crime was committed yesterday. Elizabeth I of England was robbed while she was out of her house. When she came back, she saw that her house was in a mess and her most precious barrel was EMPTY!! But, why was it the most precious one? What must she have in there? Wine? Money? Love letters?... So, who committed the crime? It was unknown. The only clue is that the person was wearing a red jumper at the time of the robbery. The problem is that the people who saw the crime, the					

CC BY NC SA

witnesses, were the servants and were told to lie UNLESS they will be killed. So, it is not possible to know anything through their words. Fortunately, nobody was killed in the robbery. But, be careful! Something can change.

So, **TODAY**, **YOU** are **HERE** to solve this mysterious event. WHO ROBBED WHAT?

Elizabeth I of England called you, the police, to investigate what happened exactly. You go there and see some footprints in the garden. There was one near the wall. The thief must have fallen and entered from there. Mmmm...interesting!

You've got some envelopes on the table with some clues that might help you. They will give you the answer to open the final box. Follow the steps of those envelopes and you would know WHAT has been robbed and WHO committed the crime.

DO NOT MISS ANY DETAILS! OPEN YOUR EYES! Be attentive!

Are you ready? 😎

The group who finds out the keys for unlocking the boxes will get stickers as a present. The stickers are previously designed by the teachers taking into consideration the subject within which the breakout has been developed. At the back of the stickers, there is the name of the

BY NC SA

robber. Thus, the stickers are employed as a metaphor of the prize obtained when a code is decoded and the spy gets a reward, normally, a message. In this case, the reward is the criminal, the person who committed the robbery. As the sessions are within the subject "Game of Maths", making reference to "Game of Thrones", the font of this famous series was downloaded so that everything is based on that particular topic. The stickers are these:

	The visuals aids are original by the teachers , authors of this project, and are shown using Genially ICT tool. They run as follows: https://view.genial.ly/5df7a5c6edd1f40f1e03fe15/presentation-breakout-gom					

BY NC SA

You could NEVER image what happened!

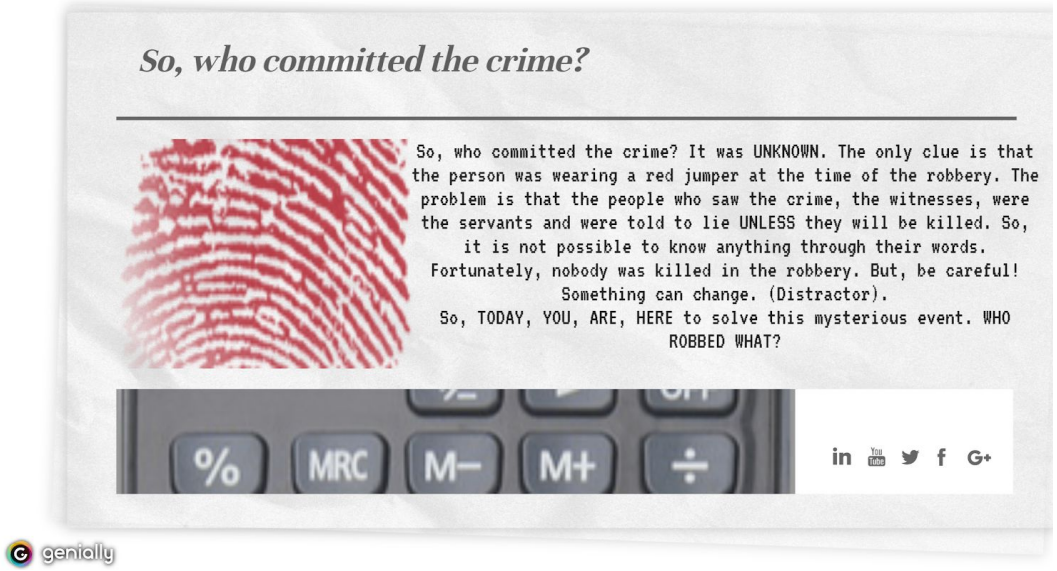
A terrible event has occured!

A terrible CRIME was committed yesterday. Elizabeth I of England was robbed? while she was out of her house.

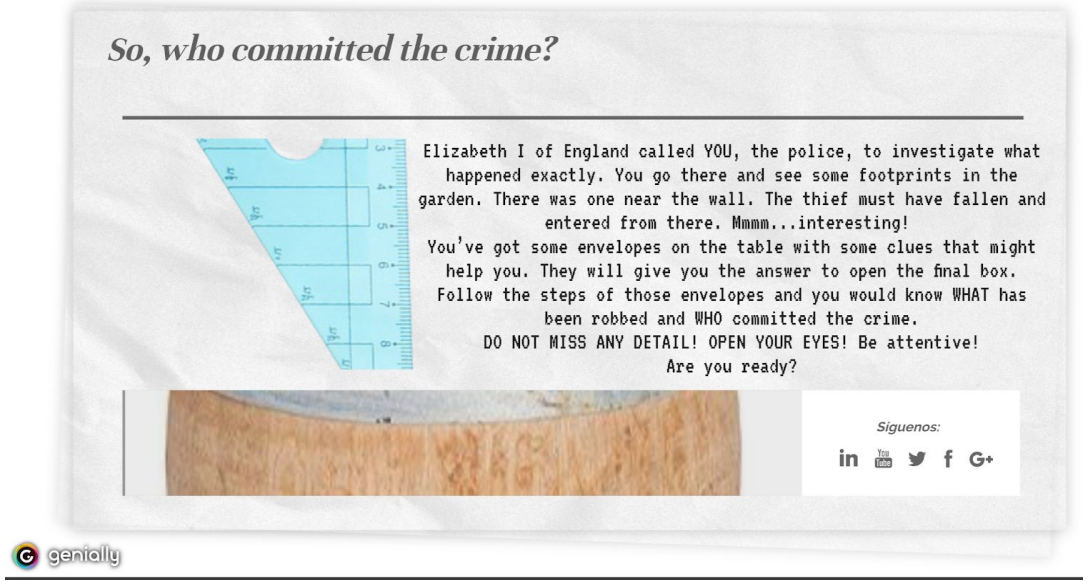
When she came back, she saw that her house was in a mess and her most precious barrel was EMPTY!! But, why was it the most precious one? What must she have in there? Wine? Money? Love letters?...

genially

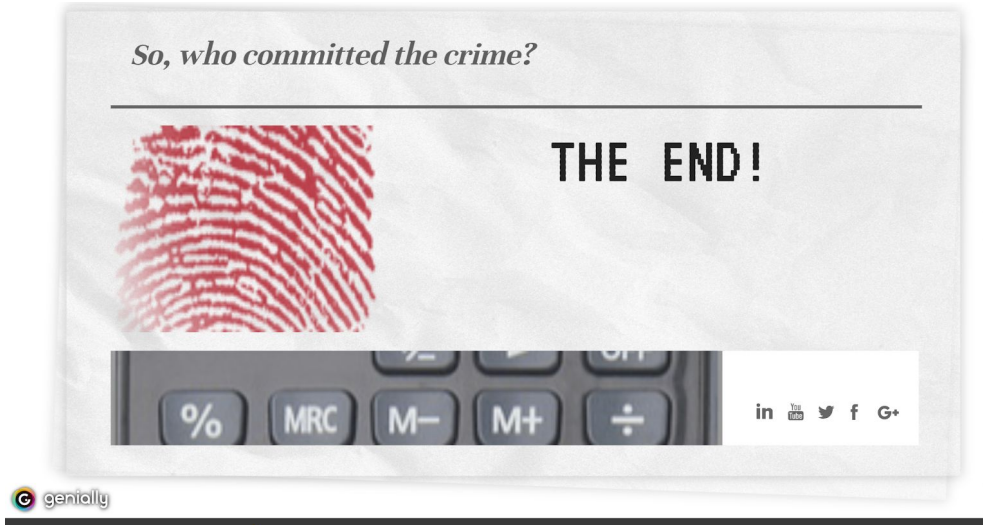
BY NC SA

	 So, who committed the crime? So, who committed the crime? It was UNKNOWN. The only clue is that the person was wearing a red jumper at the time of the robbery. The problem is that the people who saw the crime, the witnesses, were the servants and were told to lie UNLESS they will be killed. So, it is not possible to know anything through their words. Fortunately, nobody was killed in the robbery. But, be careful! Something can change. (Distractor). So, TODAY, YOU, ARE, HERE to solve this mysterious event. WHO ROBBED WHAT? % MRC M− M+ ÷ genially					

CC BY NC SA


So, who committed the crime?
Elizabeth I of England called YOU, the police, to investigate what happened exactly. You go there and see some footprints in the garden. There was one near the wall. The thief must have fallen and entered from there. Mmmm...interesting!
You've got some envelopes on the table with some clues that might help you. They will give you the answer to open the final box.
Follow the steps of those envelopes and you would know WHAT has been robbed and WHO committed the crime.
DO NOT MISS ANY DETAIL! OPEN YOUR EYES! Be attentive!
Are you ready?
Siguenos:
genially

BY NC SA



The entrance doors are decorated with "Game of Maths" breakout posters.

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

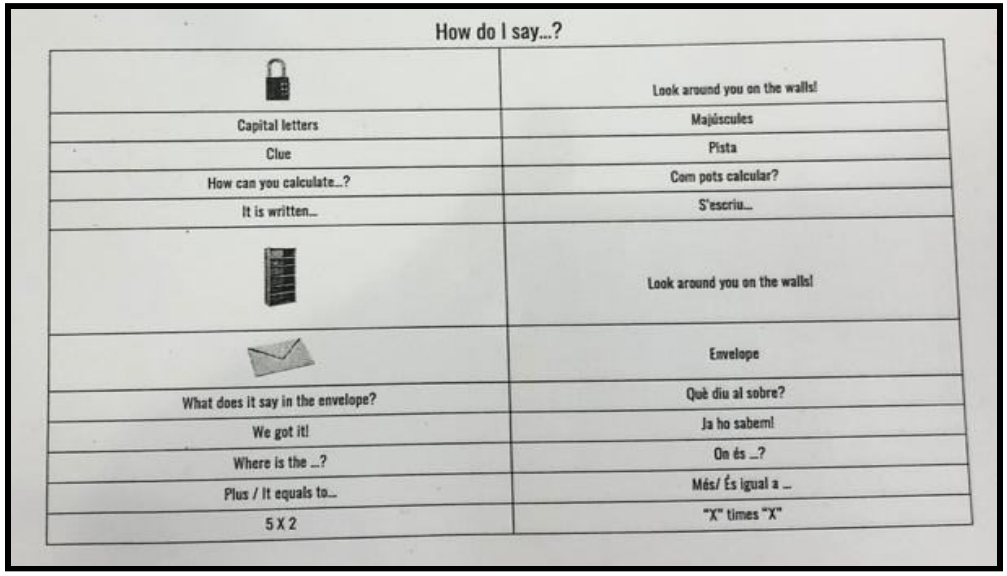
Generalitat de Catalunya
Departament d'Educació

MASTER'S DEGREE CLIL & FLE

LED

UAB
Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació

The students are helped to understand the activity by being provided with language support.

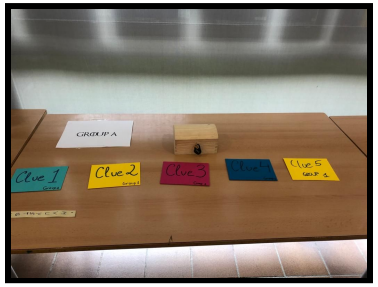


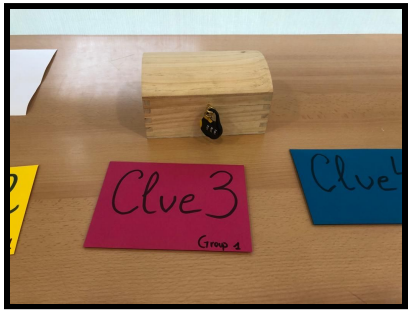
How do I say...?

	Look around you on the walls!
Capital letters	Majúscules
Clue	Pista
How can you calculate...?	Com pots calcular?
It is written...	S'escriu...
	Look around you on the walls!
	Envelope
What does it say in the envelope?	Què diu al sobre?
We got it!	Ja ho sabem!
Where is the ...?	On és ...?
Plus / It equals to...	Més/ És igual a ...
5 X 2	"X" times "X"

The distribution of the activity is done as follows:

BY NC SA





The teachers will be assessing using a checklist as a tool.

	Yes	No
Do they follow the rules easily?		
Do they speak in English when doing the activity?		
Do they realise that the words are hung on the walls?		
Have they solved the mathematical operations properly?		
Did they discover that the diameter is important for the clue?		
Do they realise that when they have a code of two ciphers they need to sum them up?		
Do they find a lot of interest in the activity?		
Do they find the correct code?		

BY NC SA

	Students will be exposed to the **driving question** in this moment of the project because they have carried out the breakout and they have a slight contact with spies. Therefore, they are presented with the question: **"How can you be a good spy"**?. It is an appropriate driving question because students will explore the methods in which the cryptography has helped the hiding of messages, and, therefore, the task of "future spies" throughout times. As we are covering a PBL project, it needs a **final product** which will be **a mind-map** covering all the details explained and worked on in class. This mind-map will also come **with the shape of the UK countries** since the UK is key in the development of cryptography through times. Moreover, as the vehicular language is English, students need to be aware where the country is located and how it is organised. Session 6 explains deeply the task: the creation of the mind-map poster as well as the presentation (with the language support). The PBL requires the student's voice and choice, then, they are the ones in charge of the format of the mind-map. The requirements are that the poster has the shape of the UK country that they are in charge of and the contents of the mind-map are a summary of all the content covered in the six sessions. The idea is that this mind-map (**whose format is decided by the group of students**) is a recap of all the content and the language that has been integrated in these six sessions. The teachers will give advice on the formats but they are the ones using their voice and choice. The format tips are the following ones: **video tutorial, hand-made, explanatory video, theatre play**, among others.					

CC BY NC SA

1.2	Materials: Two boxes, four cylinders of different diameter (e.g. aluminium roll, mosquito repeller spray, etc), envelopes, tape, a pearl necklace, Genially presentation with the story, Game of Maths stickers, projector, language support, and computer.					

SESSION 2: More than seven centuries of codification of Julius Caesar

Objectives of the session: This session aims at approaching the term of cryptography, encoding and decoding messages with the Caesar method in military ancient times.

Content-obligatory language for the session:

- Academic language (Keywords: Encode, decode, plain text, key, lower case, and uppercase).
- Descriptive text (e.g. explanation by the teacher the notion of Cryptography and the Julius Caesar ciphering).
- Instructive text (e.g. text stating the process and the steps needed to encode and decode a message following Julius Caesar method of cipher).
- Grammar items determined by the tasks and topic: (Imperatives needed to write the instructive text).

	Activities					

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

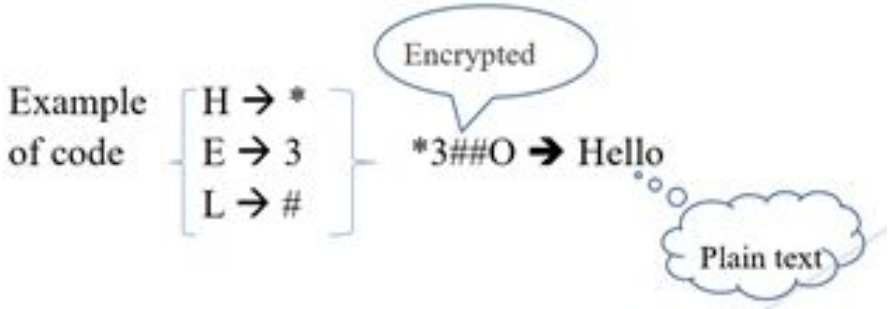
Generalitat de Catalunya Departament d'Educació
MASTER'S DEGREE CLIL & FLE
LED
UAB Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació

2.1	**Activity 2 - Initial explanation of cryptography**: Teachers present the notion "Cryptography" to the whole group with a PowerPoint presentation, previously prepared by the teachers, both content and form. The students read the content out loud and the teachers comment on them. ● Cryptography is the art of **hiding** messages. ● Cryptography is as **old** as writing. ● Historically, the **success of governments** and armies depended on: ○ The fact that **internal communications were secret**, and ○ To know **the communications** of the **enemies**. ● So that the enemy does not know your invasion plans, it is very important that he or she cannot understand the messages you send to your armies. But it is very interesting to know the enemy invasion plans. That is **why cryptography was born.** ● Currently, cryptography is widely used: ○ So that nobody can see our credit card information when we buy online. ○ So that nobody can access your email account. ○ For the ATM to transmit to our bank that we have taken money, ○ Among other cases. *Examples may arise from students*	15'	R, L	T-S WG	Ppt	

CC BY NC SA

- Governments are being interested, even today, in having their information known only to authorized people.

- In short, science for message **encryption** is to put messages in code so they cannot be understood by people who do not want them to get the message.
- The idea is to put the messages in **code** so that they cannot be understood by people that we do not want to be understood:



Process:

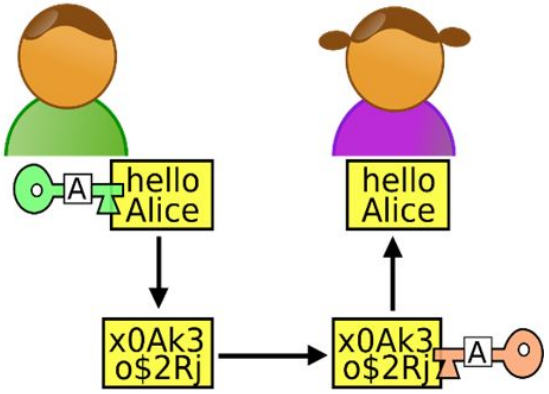
Alice (subject A) wants to send a message to Bob (subject B) without Eve (enemy) knowing the content of the message.

Alice encrypts or **encodes** the message with a password that only she and Bob know.

BY NC SA

Even if Eve intercepts the message as she doesn't know the password, she can't understand it.

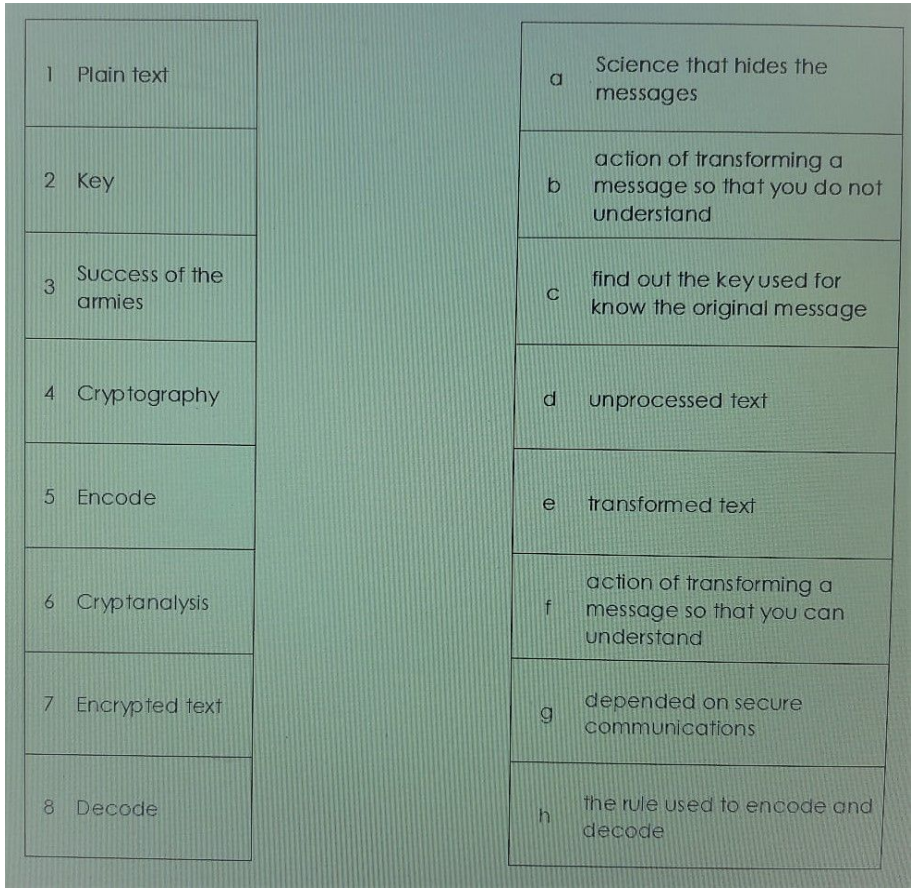
When Bob receives the message, he will **decode** it and know what information Alice transmits to him.



GLOSSARY:

- We call **plain text** to an unencrypted text, written in **lowercase**, for example, "hello".
- An **encrypted text** is the one that is encoded or encrypted, written in **uppercase**, in our example *3##O.
- The **key** is a short information necessary to encrypt and decrypt the algorithm.

BY NC SA

2.2	**Activity 3 - Have you understood what cryptography is?:** What is cryptography? Match the corresponding definitions with an arrow: 	15'	R, S, I	T-S SG		PA

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

BY NC SA

Generalitat de Catalunya
Departament d'Educació

MASTER'S DEGREE CLIL & FLE

UAB Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació

	These are the definitions learned in the previous explanation. They are specific vocabulary of cryptography (e.g. encode, decode, plain text, key, etc.) The assessment used in this activity will be peer-assessment. The tool employed is "Compare and contrast". This consists of the sharing experience of exchanging the document above with one colleague and the peers are the ones contrasting with the solutions. Teachers ask a student for the correct answer to question 1, then ask the whole group if they agree, after a few seconds of short discussion the teachers say the solution out loud and their peers contrast the right or wrong answers. Then, question 2, 3...Teachers observe if in any definition the error rate is too high to reinforce learning, if necessary, with new examples. The grouping by pairs will be done according to geographic proximity criteria, each with the partner next to them. Activity solution: 1-d; 2-h; 3-g; 4-a; 5-b; 6-c; 7-e; 8-f					
2.3	**Activity 4 - Encode messages with Caesar Cipher:** **4.1 How is it made?** Teachers show students how Julius Caesar would code with the example "**I love speak English**" with k = 1:	15'	R, S, L, W, I	T-S S-S	Ppt	PA

BY NC SA

- In the message we change the letters "A" for the letters "B", the "B" for "C", the "C" for "D", etc. And the "Z"? Well, the "Z" for the "A".
- Then we have an encrypted message in which the key would be "1" (**k = 1**), where "k" is the number of letters that move in the alphabet.
- So, "I love speak English" with k = 1 will be: "J MPWF TQFBL FOHMJTI"

Then, all together in the blackboard we codified **"If you can dream it, you can do it**" with k = 1 also. The encrypted text will be : "JG ZPV DBO ESFBN JU ZPV DBO EP JU".

Plain text	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
k = 1	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

4.2 Do you dare to try it on your own?

Translate and encode the following messages using the indicated displacements. The students must translate and codify:

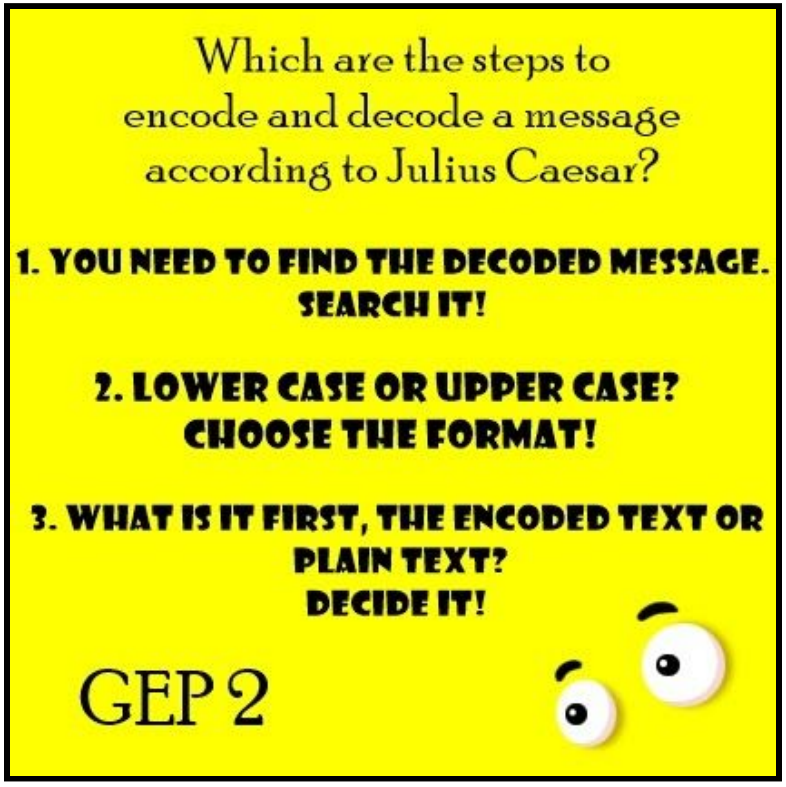
- "Start the day with a smile" (k=1),
- "Nobody finds its ways without getting lost several times" (k=2),

CC BY NC SA

	• "All you need is love" (k=3). First, students try to translate individually, then, into groups of four try to compare and reach an agreement. Then, they encode the sentence individually and finally compare it with their partners of the group. Students are formed the grouping with the "Card deck strategy". We will have prepared a deck with 24 cards because they are 24 students. The teachers will distribute a card faced down that all the students will have to discover at the same time and then get together without talking to their classmates following the same pattern (maybe they get together by objects, by numbers, by colours ...). The tool used to assess is "Compare and contrast". This technique is explained above. In this case, it consist to exchange the documents with those of the closest group. Teachers project the correct answers. Each group verify that their partner group has answered correctly.					
2.4	**Activity 5 - Instructive text** In this activity, students need to produce a brief written piece of text individually stating the steps they need to follow to encode and decode by using the Julius Caesar method. This way, they	15'	R, L, S, WI	Ind		TA

BY NC SA

need to write a text by using imperatives and practice this part of the English grammar. They will have a guiding document (being this card) as an example:



CC BY NC SA

After creating the instructive text, each student needs to read the text out loud and the teachers will be assessing both, the reading task as well as the oral reading of it. Therefore, students are also practising their oral production (speaking).

The assessment tool used to assess the instructive text as well as its reading orally is the following checklist:

CHECKLIST ASSESSMENT TOOL	👌	😈
Does the instructive text include the requirements from the guiding document (guiding card above)?		
Does the student include extra information that is not present in the card but is necessary to encode and decode using the Julius Caesar cipher method?		
Does the student use imperatives as it is necessary to include in the guiding document and in the instructive text?		
Does the student show that he or she has understood this method of cipher?		
Does the student show awareness in the English language?		
Does the student pronounce the main words related to cryptography properly?		

BY NC SA

	Does the student show important grammar mistakes in their writing?						
	Does the student show confidence to speak in public?						
	Does the student have eye contact and correct body gestures?						

SESSION 3: Al-Kindi and Arab cryptographers manage to break the Caesar Cipher.

Objectives of the session: This session aims at addressing the idea that the best cryptographic methods can be broken. That is what Cryptanalysts do. In this case we will see that with the **frequency analysis** that is a mathematical tool of the branch of statistics, Al-Kindi and the Arab cryptanalysts managed to break the Caesar's Cipher.

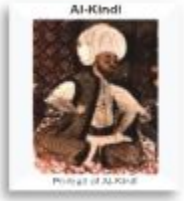
Content-obligatory language for the session:

- Academic language: Encode, decode, analysis of frequency, pain text, key, frequency of letter in the alphabet, and bar chart.

BY NC SA

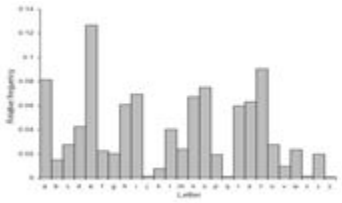
	- Text genre and typology: descriptive text (it is basically a mathematical session. So, it is very important that they understand the notions in order to do the mathematical operations. That is. the main idea is that they are exposed to descriptive texts.) - Interactive strategies (e.g. body language for the date of birth queue formation).					
	Activities					

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

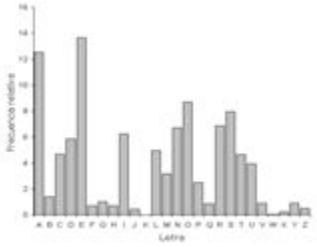
3.1	**Activity 6 - Arabian cryptanalyst** **6.1. Explanation:** Teachers explain to the students through a projected PowerPoint presentation that after ten centuries, the Arabian discover how to crack the code in Caesar Cipher. Students read the slides out loud and teachers make some comments and explanations on it.  · Al-Kindi analysed the letters of a message and discovered that some letters are used more than others. The letters "*a*" and "*l*" are the most frequent in Arabic while letters like "j" appear infrequently. This observation would be the first major advance towards cryptanalysis. • If we know the frequency with which the letters appear in a language it is much easier to know the key. In English (also in Catalan and Spanish) the vowels appear more than the consonants. Linguists have studied how often letters appear in languages.	10'	R, L	T-S WG	Ppt	

BY NC SA

- For example, the **frequency** table in **Bar Chart** format for English is:



- The letter most used in English is the ***e*** that appears almost 13% of times in a text.
- The **frequency** table in **Bar Chart** format for Spanish is:



- Compare the frequency of the letter "***a***" in English (8%) and in Spanish (more than 12%).

BY NC SA

3.2	**6.2 Mathematical website: *Thatquiz* used for the bar chart** This is the time for students to learn how to make and interpret bar charts. Before they make one, we will warm up with the "Thatquiz" program: Open a text document with the title "Activity 4.2. - name and surname". Share it with the teachers. Type **https://www.thatquiz.org/** on the bar a) In "Concepts" select "Graphs" In "Length" select 10 In "Level" select 1 In "Feedback" select "On"	20'	R, L, W	T-S	That quiz and Google Drive	TA

BY NC SA

	Select "Bar" Select "How many" Select "Easier content" At the end, copy the screen and paste it into the document shared with the teachers. b) Repeat the previous activity changing the level to 2. Do not forget to copy and paste the final screen. c) Repeat the activity, selecting "Plot" (deselect "how many"). Remember the final screen copy. d) Repeat with "Plot" with level 3. Do not forget the screenshot copy. e) Perform the activity with the level you want, selecting "Normal Content". You can repeat several times and send the copy of the screen you prefer. So, students practice the bar chart using "Thatquiz", individually.					

BY NC SA

	Eventually, for the teachers to assess, students need to share the screenshots with the "Thatquiz" result. Teachers assess through the "Information gathering" tool checking the mail through Google Drive. It is important to mention that the website "Thatquiz" offers both the teachers and students the help of having feedback on the activities carried out. This material will be useful for teachers to assess their students.					

BY NC SA

3.3.

6.3 – Create a bar chart

15' | R, L, W, S, I | S-S, SG

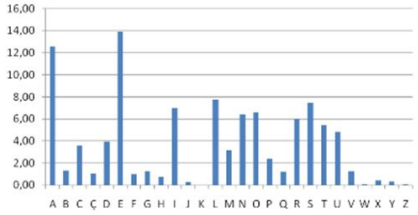
Then, in groups of four following the grouping strategy of "Date of Birth queue formation", they create a bar chart with the frequency of letters in Catalan. Here are the frequencies in percentages:

Lletra	A	B	C	Ç	D	E	F	G	H	I	J	K	L	M
%	12,55	1,32	3,60	1,06	3,94	13,89	1,00	1,28	0,72	6,99	0,30	0,00	7,74	3,16

Lletra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
%	6,40	6,58	2,39	1,2	5,99	7,43	5,44	4,84	1,25	0,01	0,45	0,35	0,05

Then, teachers show the solution, the group check if the answer is correct or wrong.

The activity **solution** is:



BY NC SA
Generalitat de Catalunya Departament d'Educació
MASTER'S DEGREE CLIL & FLE
UAB Universitat Autònoma de Barcelona Facultat de Ciències de l'Educació

3.4	**6.4. Finally, students decode a message using the frequency analysis.** In groups of four, following the grouping strategy of "Date of Birth queue formation", using the frequencies in English and with the help of your intuition, try to decrypt the following message encoded with Caesar's cipher: CP KFKQO JCU C FKHHGTGPV OGCPKPI VJCP KVU KPFKXKFWCN YQTFU HQT GZCORNG NGVVKPI VJG ECV QWV QH VJG DCI OGCPU TGXGCNKPI C UGETGV Then, teachers show the solution, the group checks if the answer is correct or wrong. The activity **solution** is:	15'	R, L, W, S, I	S-S, SG		SA

BY NC SA

	K = 2; There are 104 letters. In the message the letter that repeats the most is the "G" that appears 13 times (13/104 = 12.5%), then the C (12 times), the K and the V 10 times, etc. **The message is: *An idiom has a different meaning than its individual words. For example, letting the cat out of the bag means revealing a secret*.**					

	SESSION 4: Vigenère and the Greatest Common Divisor Objectives of the session: This session aims at encoding and decoding messages with the important cryptographic method known as Vigenere cypher. It also explores the idea of how to crack the code by using the Greatest Common Divisor (GCD).
	Content-obligatory language for the session: - Academic language: Decode, encode, key, Greatest common divisor. - Task management language items (e.g. Useful language and structures such as, "firstly, we need a table of Vigenère cypher", to record the podcast with the Voicethread ICT tool. - Interactive strategies (e.g. body language to group themselves using the cards).

BY NC SA

	Activities					
4.1	**Activity 7 - Vigenère cipher:** **7.1. Vigenère cipher explanation.** Teachers introduce the notion of "The Cypher de Vigenère" as students read aloud while others listen to the projected explanation: • The cryptanalysts attacked the ciphers through frequency analysis of the letters in a language. Therefore, they stopped being safe. • At the end of the 16th century, the Frenchman Blaise de Vigenère invented a new encryption. Well, it not was an own idea, but it is known as Vigenère Cipher. • He had examined the ideas of Italians Leon Alberti and Giovanni Porta and German Johannes Trithemius. They had worked to find a secure cryptographic method. • Vigenère created the following table where the alphabet is in rows and in columns:	10'	L	T-S WG	Ppt	

BY NC SA

	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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya
Departament d'Educació

MASTER'S DEGREE CLIL & FLE

UAB Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació

- We choose a keyword, for example: "**GAME**".
- The letters in the first row correspond to the unencrypted text.
- The first column corresponds to the letters of the keyword.
- We will mark the letters of the center for a message with the key “game".
- Let's code the phrase: "**See you at five**"
- The first letter of the message is encrypted with the code of the row where the first box is "g", the letter "s" in code "g" is the letter “y".
- The second letter with the code of the row where the first box is "a", and so on. When the rd is over it starts again.

Plain text:	s	e	e		y	o	u		a	t		f	i	v	e
Key: GAME	G	A	M		E	G	A		M	E		G	A	M	E
Coded text:	Y	E	Q		C	U	U		N	X		L	I	H	I

- Nobody will know that YEQ CUU NX LIHI is a proposal to see each other at five.
- Observe the letter “e” in Plain text. Now, observe in Coded text the “e” is “E”, “Q” and “I”.
    - **Now, The “Frequency Analysis” is no longer useful for decoding the message!!**

BY NC SA

	• We can see another example in the video: https://www.youtube.com/watch?v=SkJcmCaHqS0					
4.2	**7.2 - Encode a message with Vigenère cypher.** • In groups of six. • Search for a keyword. • Think and write a message. • Encode each one separately with the Vigenère Code. • Compare if you have stayed the same. • The grouping method used for this activity is "Card grouping" technique. The cards will reflect some ciphering methods. Students use body language to group: 	10 min	R, S, L, W	SG S-S		SA

CC BY NC SA

7.3 – Voicethread about Vigenère cypher.

Students will need to share, in a podcast created by them, the details of how they coded the messages using the Vigenère cypher. This will be done with Voicethread that they will need to listen to. The content of the Voicethread will be their own interpretation of the Vigenère cypher This is a guiding document for them to follow. It should include the following information. It is also a checklist for them to assess their own colleagues, as it is a peer-assessment tool.

CHECKLIST ASSESSMENT TOOL	😃	😓
Do you need a table in the Vigenère cypher with columns and rows?		
Do you need a keyword? Did you need to explain further?		
Do you need a plain text? Did you explain more?		
Do you use the keyword to modify the plain text?		
Did you encode a message with this cypher method?		
Did you find problems while pronouncing some words?		
Did you need further help from your colleagues in the group to construct sentences?		
Did you check any pronounciation before recording the Voicethread		

15’	R, S, L, W, I		Voicethread	

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya Departament d'Educació
MASTER'S DEGREE CLIL & FLE
LED
UAB Universitat Autònoma de Barcelona Facultat de Ciències de l'Educació

podcast?		
Do you have any positive comment about your colleagues performance? If so, which?		
Do you notice the pronunciation of a particular word wrongly? How can you improve it? Help your colleagues!		
Did they hesitate while producing their speech? Did they prepare properly?		

The grouping method used for this activity is "Card grouping" technique. The cards will reflect some ciphering methods. Students use body language to group:

BY NC SA

4.3	**Activity 8 – Greatest Common Divisor (GCD)** **8.1 – Babbage explanation** Teachers introduce the notion of how to crack "The Cypher de Vigenère" as students read aloud while others listen to the projected explanation: • The frequency analysis cannot be used to attack Vigenère encryption, since we do not know how long the key is, and each letter of the key will create different letter frequencies, since they are different codes. • In 1854, **Charles Babbage managed to attack him**. • He saw that, in very long messages, repetitions can be found. Some frequently used words separate with the same keys. See:	10 min	R, S, L, I	T-S	Ppt	

BY NC SA

YHXEK IGLXZ GUYEM EWLQZ RUYXG IFNED TCPRK
VIMEI YHAEJ XICED FYWWV YLLQR XXPBR MMWMM
EXTVR ZYFVV WCUSR GIYWV KOPMO SWZQG XUCIC
WMPYJ BUTWV RGPRP WXPGZ RWDIX SHDQV RXZRR
VUFRR PUBYR PWZWR IFAEJ XICGF RNPWK EUQMI
QUEMM EGPRK XIETV RMLRK IHWEZ QJZWJ MVTPZ
XUEHL RWZQG XUEKV XUYVR TCOTV VIGIK EKFMH
YYPPD ENPQR XCNIJ GIYGV RNCEZ EVLRJ HYWWT
MHNWV KIYWC MWZQL RCNER PJLWK SLBYV EFCED
ENSMY EPTEK VYDGV RNDUL ELLRK EHZYO ECDIC
TUDXF VPLLR ZYCHR GWPTK ELBYV IFXEK IGLXZ
GBLZZ EAFEE CUEMV WUTBZ GIXEH YYDXT ELCIX
EYWWV YAFEE CUWIJ TUEPC ECNSD IHNER GUXME
ELESK GIYXV RNAII SYWTR WNZVV WGLTV VXFXG
IFBYV EWLFR ZUOIM IOCIT VCOER PGLXV QUEMT
IMNSC XCAEI MZLVR IFQEM SLOIK SLYEI QYPPX SM

- .
- That allows to know how many letters is the key.
- It will be the **greatest common divisor** of the space between repetitions.
- And, by frequency analysis, find each of the codes.

BY NC SA

- In short, looking for repetitions in the encrypted text has allowed us to identify the length of the key, which turned out to be four letters. This allowed us to divide the encrypted text into four parts, each encoded according to a monoalphabetic substitution defined by a letter of the code.
- You should know that:
  - Babagge's great contribution was to decipher the indecipherable Vigenère Cypher. That was the biggest cryptanalytic leap since the ninth-century Arabs deciphered the Caesar cypher inventing the frequency analysis.
  - But more than 100 years passed until it was learned that Babbage had deciphered the Vigenère cypher. **Why?:**
    - Some say that Babagge forgot to publish his feat.
    - Others believe he wanted to publish it, but the British government asked him not to tell anyone because that way they would have an advantage in other wars that could come to win in the successive wars that were going on.
    - The latter is what has happened throughout history: **the achievements of the cryptanalysts have been kept secret for the benefit of national security.** If the enemy does not know that he can decrypt his messages, he will continue using the same coding and will have access to all the information he wants.

BY NC SA

	8.2 – Greatest Common divisor This activity consists of practicing the calculus and application of mathematical concepts known as Greatest Divisor Common. Students need to observe the repetition of words to decide if they need to apply the GCD to know the extension of the key word. Then, they need to answer some questions related to the mathematical field. • Do you know about Romeo and Juliet? It is a tragic love story. We will talk about them later. • Now, you have found a long love letter that Juliet wrote to Romeo. • The letter is coded and no one has been able to decipher. • You observe it carefully and verify that **there are two repetitions of words**. • One of the repetitions is given 30 letters away and the other 48 letters away. • You must answer: a. How many letters is the key composed of? b. Knowing that Juliet wrote it, what do you think could be the key? c. And if you discover that there is a repetition every 40, 56 and 72 letters d. How many letters is the key composed of?	15'	R, W	Ind		PA

BY NC SA

e. Knowing that Romeo and Juliet is a work of William Shakespeare, what do you think could be the key?

Solution activity 8.2. - Greatest Common divisor

One of the repetitions is given **30 letters** away and the other **48 letters** away.

a) How many letters is the key composed of?

30	2	48	2
15	3	24	2
5	5	12	2
1		6	2
		3	3
		1	

$30 = 2 \cdot 3 \cdot 5$
$48 = 2^4 \cdot 3$

$M.C.D.(30, 48) = 2 \cdot 3 = 6$

b) Knowing that Juliet wrote it, what do you think could be the key?

Any word in English with six letters, perhaps JULIET

BY NC SA

c) And if you discover that there is a repetition every 40, 56 and 72 letters.

40	2	56	2	72	2
20	2	28	2	36	2
10	2	14	2	18	2
5	5	7	7	9	3
1		1		3	3
				1	

$$40 = 2^3 \cdot 5$$
$$56 = 2^3 \cdot 7$$
$$72 = 2^3 \cdot 3^2$$

$$M.C.D.(40, 56, 72) = 2^3$$

d) How many letters is the key composed of? **8 LETTERS**

e) Knowing that Romeo and Juliet is a work of William Shakespeare, what do you think could be the key?

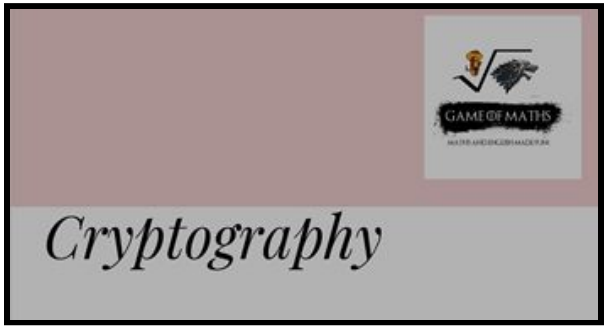
Any word in English with EIGHT letters,

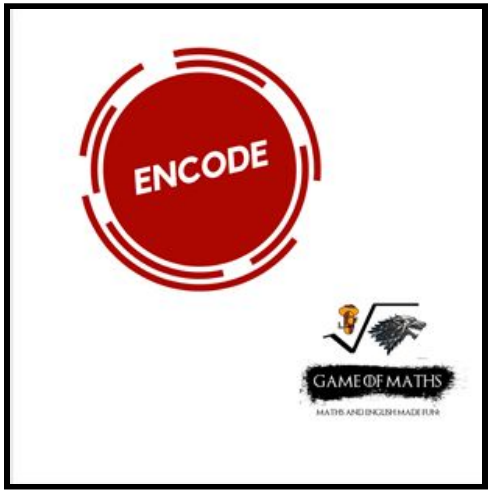
perhaps Shakespeare – Shakespr (8 letters)

Teachers will project the solutions for the activity and, through peer-assessment with the tool "Contrast and compare", previously explained above, they will need to check if they did a good job.

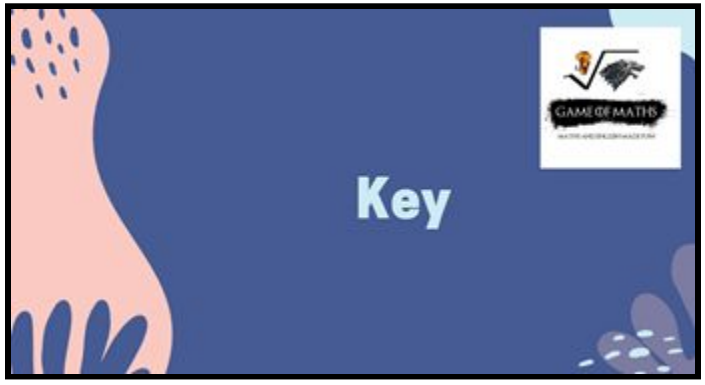
BY NC SA

The grouping method used for this activity is "Card grouping" technique. The cards will reflect specific vocabulary of this project.





BY NC SA



Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya
Departament d'Educació

MASTER'S DEGREE CLIL & FLE

UAB Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya
Departament d'Educació

MASTER'S DEGREE CLIL & FLE

UAB Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació

SESSION 5: Steganography and Invisible Ink

Objectives of the session: The main aim of this session is to discover what steganography is and experiment it with an invisible ink workshop.

Content-obligatory language for the session:

- Academic language: specific vocabulary (e.g. cotton bud, vinegar, sodium, milk, heat, language support included) and discursive connectors (e.g. **first**, you heat it with baking soda, **then,** you change the element).
- Genres and text typologies: Explanatory text (e.g. explanation of the experiment) and instructive text (e.g. step to follow to carry out the experiment by combining milk, vinegar, etc).
- Grammar items determined by the task: 3rd person singular (e.g. when you take the vinegar to the heat, i**t burns out** and the **ink is visible**).
- Task management language items (e.g. first, you use the vinegar. In this case, this goes here because…)
- Interactive strategies (e.g. body language, language support, role of gestures when taking turns when discussing in public, courtesy, etc).

Activities

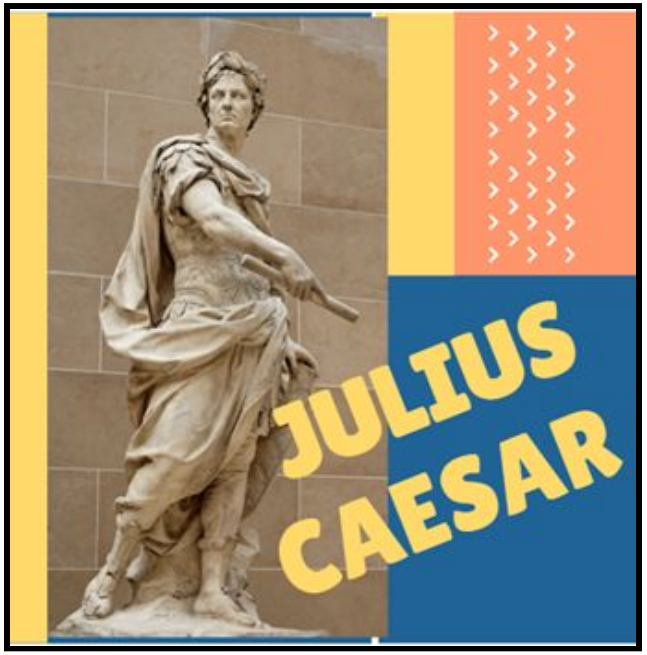
Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya Departament d'Educació
MASTER'S DEGREE CLIL & FLE
LED
UAB Universitat Autònoma de Barcelona Facultat de Ciències de l'Educació

	1. Steganography and Invisible Ink Workshop: Explanation. In this activity, the students need to make invisible ink with their own group. Before that, students need to be grouped in the way that is explained below. They need to try with different components being vinegar, baking soda, lemon, etc., and teachers are guiding the whole activity by giving them language support and discussing strategies (scaffolding) to make their own discussion of the experiment at the end of the session very profitable. Students are grouped forming four groups of six. As a grouping technique, they take a card of the following ones:	10'	L	T-S WG	Ppt	

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/



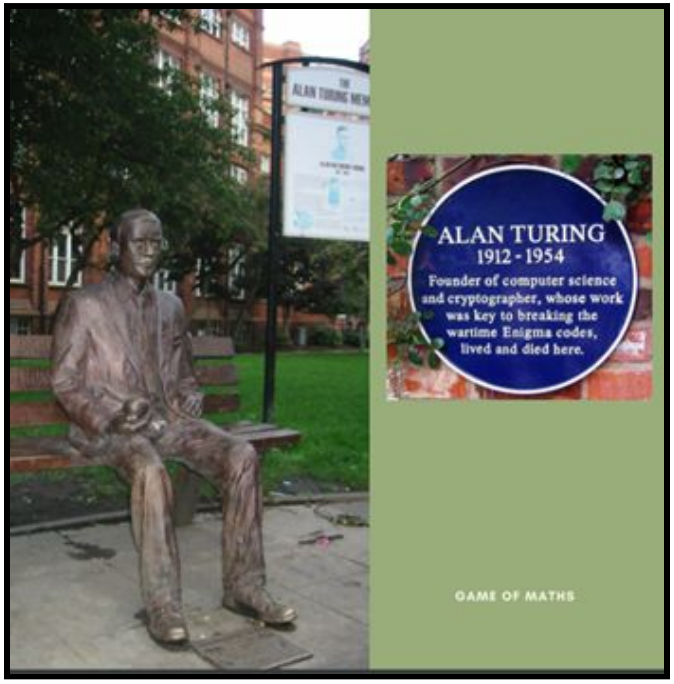
Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya
Departament d'Educació

MASTER'S DEGREE
CLIL & FLE

UAB
Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació



The experiment will be carried out the following way:

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya
Departament d'Educació

MASTER'S DEGREE CLIL & FLE

UAB Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació

Cryptography
4.1. Steganography – Invisible ink

Materials: what you'll need

- Half a lemon
- Water
- Spoon
- Cotton bud
- White paper
- Lamp or a heater

Cryptography
4.1. Steganography – Invisible ink

Procedure: what do you have to do?

Squeeze some lemon juice into the bowl and add a few drops of water

Mix the water and lemon juice with the spoon

Dip the cotton bud into the mixture and write a message onto the white paper

Wait for the juice to dry so it becomes completely invisible

When you are ready to read your secret message or show it to someone else, heat the paper by holding it close to a light or a heater.

Cryptography
4.1. Steganography – Invisible ink

2. Make invisible ink using milk

Milk is an effective and readily available form of invisible ink. Milk can be used tuo reveal secret messages.

Materials: what you'll need

- Milk
- Cotton bud
- White paper
- Lamp or a heater

Cryptography
4.1. Steganography – Invisible ink

Procedure: what do you have to do?

Put some milk into a bowl

Dip the cotton bud into the milk and write a message onto the white paper

Let it dry and watch how it disappears.

Heat the paper by holding it close to a light or a heater

CC BY NC SA

Cryptography
4.1. Steganography – Invisible ink

3. Make invisible ink with vinegar

Vinegar is a proper form of invisible ink.

Materials: what you'll need

- Two tablespoons of vinegar
- Water
- Cotton bud
- White paper
- Lamp or a heater

Cryptography
4.1. Steganography – Invisible ink

Procedure: what do you have to do?

Mix the vinegar with a few drops of water in a bowl

Dip the cotton bud into the mixture and write a message onto the white paper

Wait for it to dry and watch how it disappears.

Bring the paper close to a heated bulb or a heater and see your words appear gradually on the white paper.

Cryptography
4.1. Steganography – Invisible ink

4. Secret messages with sodium bicarbonate

Sodium bicarbonate can react chemically with some substances like lemon juice to reveal a secret message.

Materials: what you'll need

- Sodium bicarbonate or baking soda
- White paper
- Cotton bud
- Lemon juice
- Water
- Teaspoons

Cryptography
4.1. Steganography – Invisible ink

Procedure: what do you have to do?

- Combine approximately 1 teaspoons of sodium bicarbonate with 3 teaspoons of water.
- Dip the cotton bud into the mixture and write a message onto the white paper
- Write a message onto the white paper
- Let it dry an brush any excess sodium bicarbonate off the paper
- To reveal the secret message, spray lemon juice on the message.

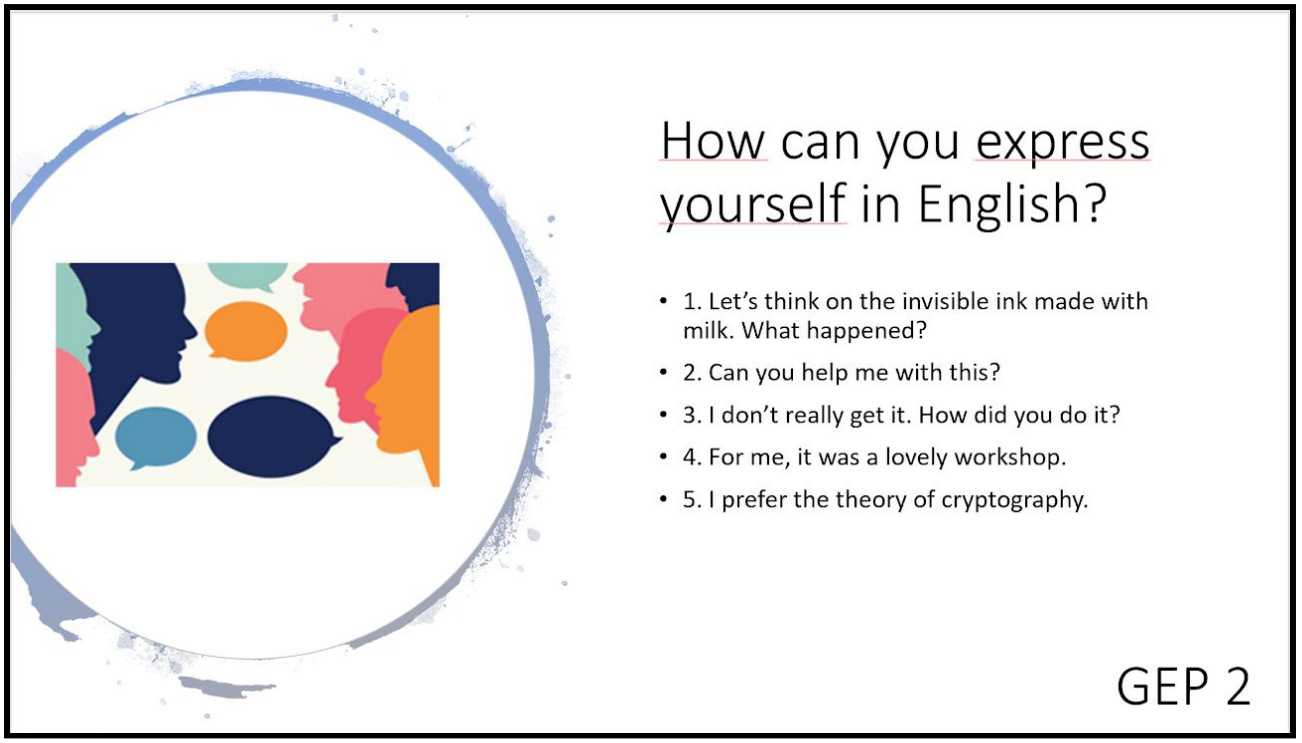
CC BY NC SA

	All the students will do the activities below. However, they will do it in groups so that they have their own perception of the experiment. They need to maintain a conversation in English. Therefore, they have the language support below so that they have a scaffolding. After doing the experiment with all the groups, they will need to discuss what happened in the session by sharing their own opinions on it. The following language support helps them with it. As for the discussion task, these are the materials given to students to discuss together and share their own opinions about the experiment. It needs to be mentioned that all materials used in this project are original from the authors of it.					

BY NC SA

Learn how to express your ideas!
• 1. I reckon it is…
• I really loved the workshop ☺
• 2. I couldn't agree more with you/ I couldn't disagree more with you.
• 3. What happened with the "vinegar"?
• 4. What does "cotton bud" mean?
• 5. I don't know how you see the ink.
• 6. I don't see much difference.
• 7. Are you joking? It's absolutely different.
GEP 2

BY NC SA



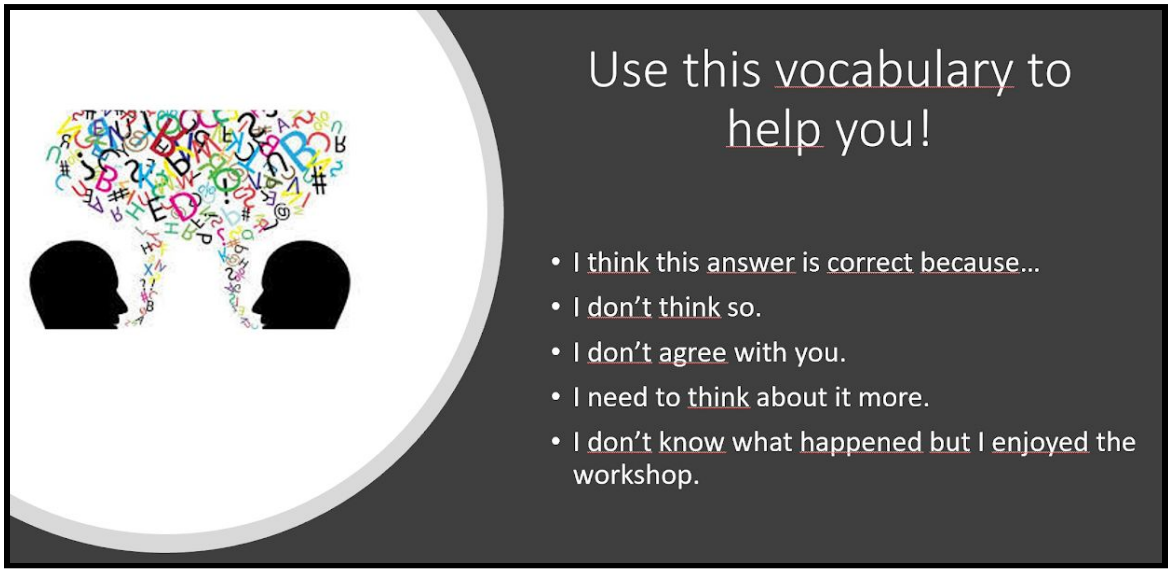
Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya
Departament d'Educació

MASTER'S DEGREE CLIL & FLE

UAB Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació



Eventually, the following document is used to assess the students. The assessment tool is a checklist.

BY NC SA

	Yes	No
Did they take care of the materials employed?		
Were they careful with the heat?		
Could they wait until the ink was visible?		
Could they interact in English following our instructions?		
Could they internalise the main point of the practical session?		
Could they follow the instructions to do the mixtures?		
Do they need further guidance in terms of English?		

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

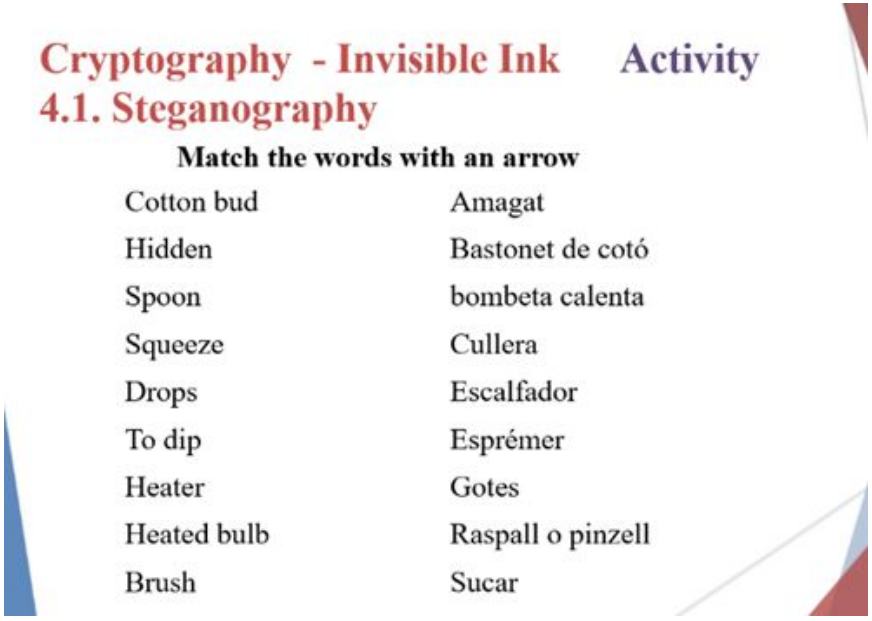
5.1	**Activity 9. Secret messages with lemon juice.** 	8'	R,L, W	SG		TA

CC BY NC SA

5.2	**Activity 10. Secret messages using milk.**	8'	R,L, W	SG		TA
5.3	**Activity 11. Secret messages using vinegar.**	8'	R,L, W	SG		TA
5.4	**Activity 12. Secret messages with sodium bicarbonate**.	8'	R,L, W	SG		TA
5.5	**Activity 13. Think, discuss and share. How it works.**	18'	S,L, I	SG		TA
	The activity consists of making invisible ink by writing messages that will be able to be read once they approach, to the heat the different components mentioned above. The activity will be made in group but every group will try all the components: milk, vinegar, baking soda, and lemon.					
	Finally, they will discuss each group of six members to find out why this happens. After the discussion, we will share it with the rest of the class. The following language support is given to the students in order to understand the experiment. The language support is given in a way of a					

BY NC SA

matching activity so that they are familiarised with it already. Once they are aware of the words, they can start the experiment with the different materials: milk, vinegar, baking soda, etc.



Cryptography - Invisible Ink Activity

4.1. Steganography

Match the words with an arrow

Cotton bud	Amagat
Hidden	Bastonet de cotó
Spoon	bombeta calenta
Squeeze	Cullera
Drops	Escalfador
To dip	Esprémer
Heater	Gotes
Heated bulb	Raspall o pinzell
Brush	Sucar

Teachers will guide the students to see that the oxidation of the carbon molecules from the diluted lemon juice (or other substances) that are absorbed by the paper are not noticeable

BY NC SA

	until the paper is exposed to heat, which causes some of the chemical bonds to break down, freeing the carbon. At the end of the experiments, the students will need to discuss what they think about the session and how they think the invisible ink is seen after being heated. The results of the experiment will be shared having the help of the language support below. The discussion language support given has already been shown above. Eventually, the assessment checklist has already been covered as well.					

SESSION 6: Presentation Poster Conference (Assessment)

Objectives of the session: The objective of the session is recapping all the important information about cryptography and create a poster of them. They will be shown as a poster conference. The audience is, firstly, the rest of the class and then, the rest of students of the high school. As we are dealing with a PBL, and one of the main functions of it is to be public and open to everybody, the posters will be hung on the walls so that the rest of the groups can be active in it.

BY NC SA

	Content-obligatory language for the session: - Explanatory text and audio (e.g. Genially interactive image), complementary texts. - Task management strategies (e.g. grouping through cards) - Interactive strategies (e.g. oral presentation- support).					
	Activities.					
6.1	**Activity 14. Reading Task:** UK geography. The activity will consist of reading individually a text regarding UK geography. As the UK has been a crucial point in the path of cryptography, it is important that students locate where it is and what parts the country has. That is why it is combined in this project. The text is extracted from the BBC and you can find the link in the reference section. However, it has been adapted using the ICT tool "Genially" by creating two interactive images. The image is the same one in both cases. However, the information that it includes is not the same. They have complementary information which both students will need to do the mind-map. The interactive images also contain the clips of the pronunciation of certain words that are difficult to produce.	5'	R, S, L	T-S S-S WG	Ge niall y	TA

CC BY NC SA

The reading task runs as follows:

- **In the pre-reading task**: Each student is given one card. They are shown below:

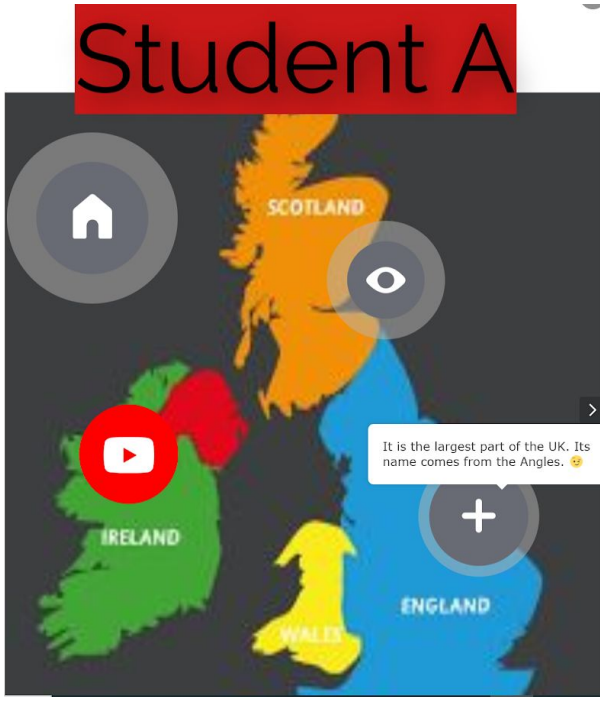
-

Each card corresponds to an interactive image created by Genially in which the information of the reading appears. However, the information of student A and student B are complementary, because it is a complementary text, and, therefore, complementary images.

BY NC SA

	The information they have initially (without being shared with their partner) is necessary to respond to the survey monkey activity following this one. In the interactive image (in A or in B, there is information about the UK countries and also some reference and voice clips to the pronunciation of certain difficult words). - **In the while-reading task:** Students need to read and listen to the information in the interactive image, each one, their corresponding image. - **Interactive image Student A:**					

BY NC SA



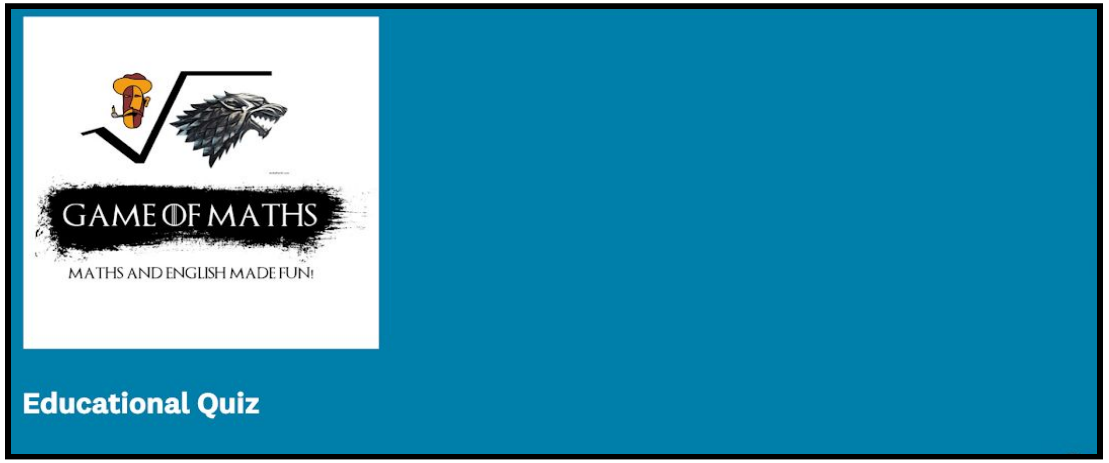
- **Interactive image Student B:**

BY NC SA

The link to have access to these two interactive images is: https://view.genial.ly/5e73ae73d77ff6169072aab6/interactive-image-imagen-interactiva

- **In the post-reading task:** Students need to share the information in the two interactive images and add more for carrying out the mind-map.

BY NC SA

6.2	**Activity - 15. Reading comprehension: Survey Monkey.** It consists of the individual comprehension of the different information in the interactive image. The authors are the BBC British council writers. However, the teachers of this project have modified the text and grade it so that it contains more information about the countries. The survey is shown below: 	5'	R, W	Ind	Survey Monkey	TA

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

2. Elizabeth's father, King Henry VIII, had six wives.

- ○ True
- ○ False

3. Elizabeth was very clever.

- ○ True
- ○ False

4. Elizabeth became queen after her brother died.

- ○ True
- ○ False

5. Elizabeth sent explorers sailing around the world.

- ○ True
- ○ False

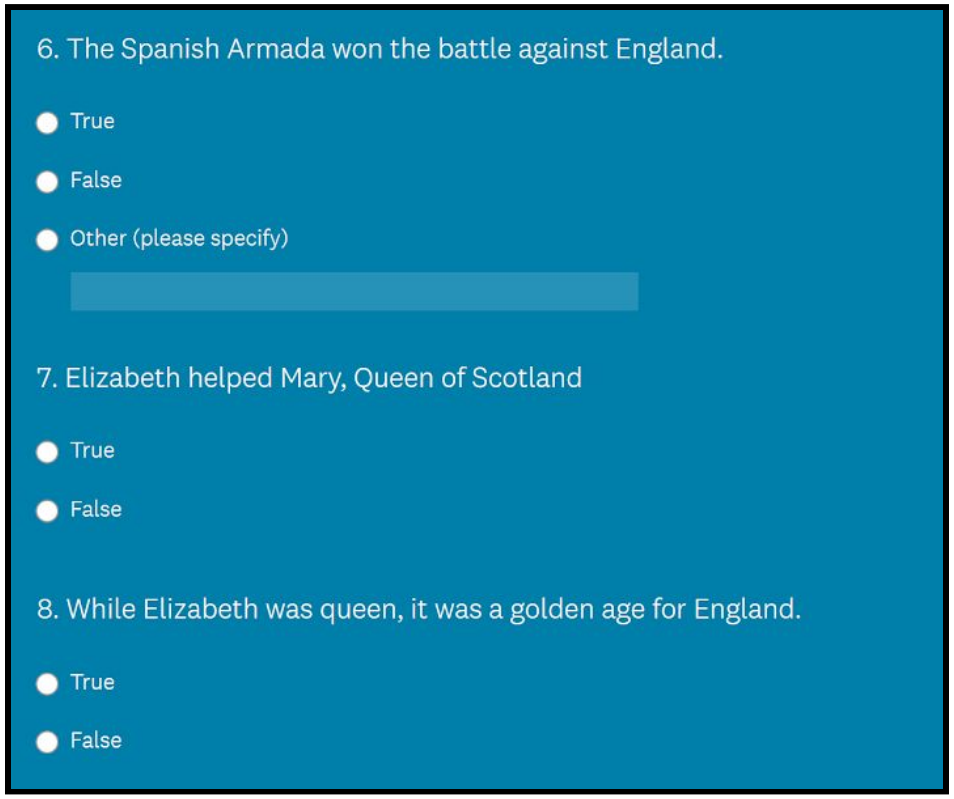
Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

CC BY NC SA

Generalitat de Catalunya
Departament d'Educació

MASTER'S DEGREE CLIL & FLE

UAB Universitat Autònoma de Barcelona
Facultat de Ciències de l'Educació



Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

	9. James I, Mary's son, became king when Elizabeth died. ○ True ○ False 10. Elizabeth is Mary's sister. Mary is Queen of Scotland. ○ True ○ False This activity will be assessed by the teachers, having a look at the results of the survey monkey ICT tool.					
6.3	**Activity 16. Presentation poster creation**. This activity is one of the core of PBL. Students need to create a poster following the guidelines of the teachers. They need to create a mind-map with all the cryptography content covered in class. The important thing is that they make a summary of the main points of cryptography as well as the new English vocabulary covered in this project. The artistic part of it is that the poster needs to be in the shape of a UK region (present in Activity 13). These mind-maps are created in groups formed by card group formation used in session 2.	20'	R, S, L, W, I	S-S SG		TA

BY NC SA

The assessment tool is the following rubric.

INDICATORS	NA	AS	AN	AE
CONTENT OF THE MIND-MAP	It doesn't cover the concepts dealt with in class about cryptography. It just shows the shape of the country and an undetailed mind-map.	It includes some of the most important concepts covered in the class about cryptography. The mind-map shows relevant facts of the sessions but it is not a complete piece.	It includes the most important concepts covered in the class about cryptography details.The mind-map shows relevant facts of the sessions but it is a rather complete piece.	It includes all the concepts covered in the class about cryptography. The mind-map shows relevant facts of the sessions but it is a very complete work.
LANGUAGE IN THE POSTER	The poster does not contain all the terms from the high-level English vocabulary covered in the sessions related to cryptography.	The poster contains some of the terms from the high-level English vocabulary covered in the sessions related	The poster contains nearly of the terms from the high-level English vocabulary covered in the sessions related	The poster contains all the terms from the high-level English vocabulary covered in the sessions related

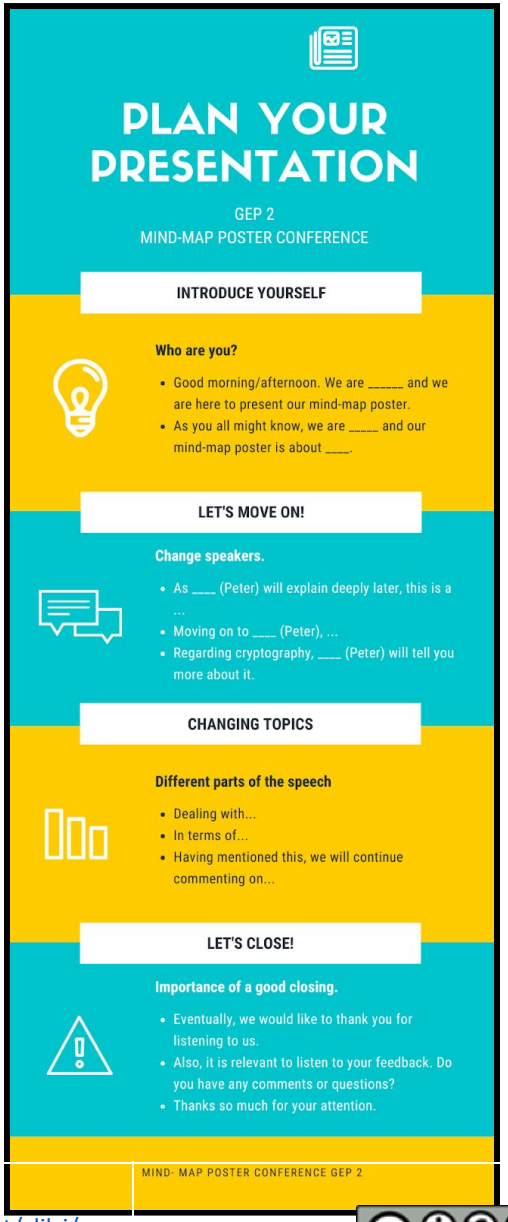
CC BY NC SA

	PRESENTATION	**The presentation is prepared according to the language support provided and the students read the speech prepared. The idea was not to read anything at all and perform freely.**	**to cryptography. The presentation is prepared according to the language support provided and the students do not read the card while performing. It is a satisfactory oral speech.**	**to cryptography. The presentation is prepared according to the language support provided and the students read partly the card while performing. It is an successful oral speech.**	**to cryptography. The presentation is prepared according to the language support provided and the students do not read the card while performing. It is an excellent oral speech.**					
	GROUP WORK	**The organisation of the group is not very stable. They need extra help for carrying out the task.**	**The group works cooperatively showing a problem-solving attitude having a lack of English use.**	**The group works cooperatively with some distractions during the process. They use English as a vehicular language.**	**The group works cooperatively showing a problem-solving attitude. The language they use is English.**					

CC BY NC SA

6.5	**Activity 17. Posters' conference**. It consists of the main part of the PBL. As it is the final product of this project and the posters' conference is open to everybody in the high school. Therefore, it consists of two important parts. Firstly, there is one presentation made in class in front of their peers. There is another part in which the posters are hung on the walls as the final product of the 6 sessions. As a matter of fact, activities 15 and 16 are correlated as they are the poster creation and the succeeding poster presentation. Students are offered with a language support card to prepare for the presentation in front of the class. This card has been prepared by the teachers carrying out this project by using the platform called "Canva" and it is an infographic.	30'	S, L, I	S-S		TA

BY NC SA



Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

BY NC SA

	They can rehearse but it is not allowed to have a look at the vocabulary while reading. This presentation will be assessed taking the rubric above.					

Teaching Materials Checklist

SELF-ASSESSMENT CHECKLIST

CLIL-PBL Project - Teaching materials	YES OR NO?
The teaching materials are **visually attractive** and **well-organized**.	Yes
The teaching materials are **self-explanatory** and **ready-to-use.**	Yes
All activities and teaching materials are **original** and **created** by the course participant.	Yes (Mind-map inspired on Pinterest)

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/

Any resource in any format (including videos, images, texts from the Internet), that is not original, is respectful of copyright and its **sources** are **cited**.	Yes
Students are presented with **multimodal** and **varied** input (spoken, written, visual, hands-on…).	Yes
Input is presented at the right **cognitive level**.	Yes
Input is presented at the right **language level.**	Yes
Students are **helped** in some way to **understand and process the input presented.**	Yes
Visuals are used to support comprehension.	Yes
Students are presented with **good questions** (explicit, implicit and referential) that help them process input and that challenge them not only to understand, but to think, create...	Yes
There are **opportunities for significant linguistic output** (the students produce communicative "products", speak, write, interact…).	Yes

BY NC SA

Support is provided to help students read, write, speak and interact.	Yes
A variety of **collaborative and cooperative learning strategies** are used throughout the sessions.	Yes
Activities facilitate **inquiry and reflection** and promote the role of the teacher as a facilitator/coach.	Yes
Task instructions are short, concise, **clear** and **comprehensible** to the students. Activities are written using an **appropriate level of language**.	Yes
The teaching materials are written in **accurate English**. There are **no mistakes at all**.	Yes

Template adapted from CLIL-SI 2015.
More information at: http://grupsderecerca.uab.cat/clilsi/