



**UNIVERSITÀ CA' FOSCARI DI VENEZIA**

**CORSO METODOLOGICO CLIL (MIUR) 20 CFU**

**PROJECT WORK FINALE**

**TITOLO: A CRYPTOGRAPHIC JOURNEY  
FROM THE ANCIENT GREEKS TO THE WEB 2.0**

**Corsista: LUCA BATTISTIN**

**Tutor: MARA ZORDAN**

**Anno Accademico 2017/2018**

## Table of Contents

Foreword.....	3
Introduction.....	3
Activities.....	6
Lesson 1: Introduction to Cryptography.....	6
Lesson 2: From Vigenere to rotor machines.....	9
Lesson 3: The Enigma Machine.....	10
Lesson 4: Crypto challenge.....	13
Evaluation.....	15
Next Lessons.....	16
Cracking the Enigma machine.....	16
From Colossus to DES.....	16
Alice and Bob go public.....	18
Message Digest.....	19
https, PGP and TOR.....	19
Crypto Treasure Hunt.....	20
Further Development.....	20
Acknowledgements.....	20
Appendix1.....	21
Crypto Challenge:.....	21

## Foreword

The lessons designed in this paper are based on the Simon Singh's "The Code Book" [1] that I found in an intriguing second hand bookshop in Brighton a couple of years ago.

I hope that, through the activities described in this paper, some students might experience part of the sense of wonder I've found while reading it and might be inspired to deepen the concepts exposed reading this or other books related to the subject.

All the activities are designed for students of the fifth or the fourth year of a Computer Science Technical School (ITI ad indirizzo informatico) but they can be easily adapted for different schools and different years.

## Introduction

*CLIL, the abbreviation for Content and Language Integrated Learning, is an approach that has spread across Europe in response to increasing demands to improve students' foreign language competence. It integrates language with non-language content in a dual-focussed learning environment.[2]*

In other words it is a teaching methodology by which the learner acquires new contents through a foreign language and a foreign language through the contents<sup>1</sup>.

For me CLIL is a new perspective to look at the matter of my teaching and an opportunity to reconsider my role as a teacher.

Why this particular topic?

In a technical school (*ITI ad indirizzo informatico*) the 5<sup>th</sup> year Computer Science contents are rather complex and advanced. I've chosen a topic whose complexity allows to balance the effort to deal with it using a foreign language<sup>2</sup>.

Moreover, Computer science technology is changing quite rapidly, so that its teaching has to be updated every year: choosing an historical perspective allows me to reuse the material and the activities – with some slight adjustments - more than once.

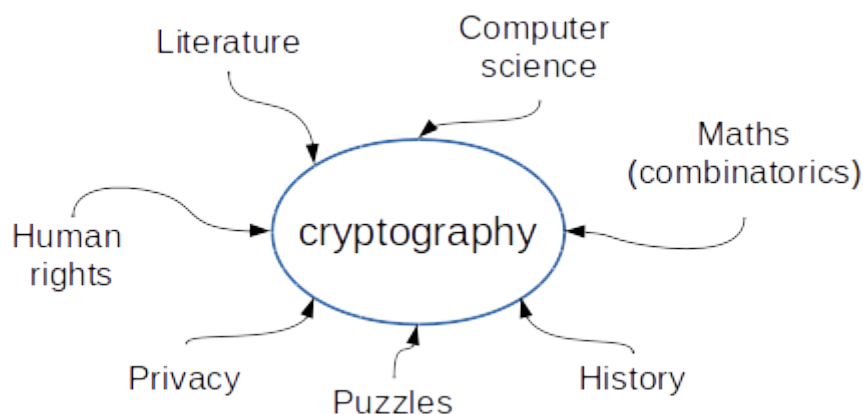
But first of all I've chosen CRYPTOGRAPHY because it is fun and it is a subject that is linked to many other disciplines from Literature to History ... Using Simon Singh's words : "*Cryptography is about mathematics, it's about science, it's about politics, it's*

---

1 In my experience I've seen students who were very good at computer science (the content) but rather weak in English improving their fluency and finding new motivations towards the foreign language because of their understanding of the subject and their capacity to explain to the fellow students some concepts or solve a problem. Vice versa, and even more often, I've seen students who were meeting difficulties in the subject finding themselves in a new leading role in the activities because of their good English level.

2 Marcella Menegale -How to promote productive skills - "Ideal CLIL materials must maintain LCD-CCD equilibrium".

*about privacy, it's about human, rights it's about technology... It's a whole mess of different things"[3]*



I asked the Maths teacher to work on the combinatorics of the Enigma machine and the History teacher to focus on the role of intelligence during World War II and the battle of the Atlantic in particular.

*"... An essential feature of a CLIL programme is that it be the result of continuous consultation between the content teacher and the foreign language teacher"[2]*

I asked the English teacher to help me with the language side of the activities: giving feedback to the students in order to enhance their written and oral production but also reading in class some part of "The Gold Bug" by E.A. Poe[4] and developing some lessons on the biography of Alan Turing before watching "The imitation game".

In designing the activities I've tried to keep in mind some theoretical frames like the Bloom taxonomy but also the advice professor Coonan gave us during the last lesson: "think how and when you learnt best". I learn when ...

- my curiosity is aroused
- I can touch, build, manipulate something
- I can explain my thoughts and have a feedback
- the same topic is seen from different point of view
- I can see the human enterprise that has led to a particular achievement<sup>3</sup>
- the explanations are clear and use different languages (text, images, schemes, videos, etc.)
- There is redundancy but not mere repetition
- I can move and interact with others

<sup>3</sup> Some times scientific results, theorems or principles are exposed like timeless celestial objects descended on earth perfectly shaped, while they are usually the result of a great effort or even of a fierce battle against failure and mistakes... The student can be motivated by the awareness that his doubts, questions and mistakes are likely to have been encountered also by the greatest scientists.

- I can see some other paths through the subject that I might follow on my own

The **ICTs** can play a key role in CLIL if they are properly used. In designing these lessons I've relied heavily on the opportunities offered by different learning platforms (EdPuzzle, Socrative, Kahoot, the Khan Academy, TED) and in particular on the Marzotto's Moodle platform superbly managed by my fellow computer science teacher Riccardo Crosato<sup>4</sup>.

ICTs allow to prepare the activities for the students to be carried out almost independently from the teacher who, therefore, can shift from the frontal role of the actor to the more side role of the director or trainer. This does not mean that ICTs make the job of the teacher easier; on the contrary, it takes much longer to design and devise activities student-centered! But in my opinion they are more effective because the learner is more active and the teacher has a better understanding of the progress of the learning process.

Frontal lessons are not banned from this methodology: they still play an important role when a new subject has to be introduced or an extra explanation is needed (because the feedbacks show that something has been missed or misunderstood)

Among the many valuable tools (quiz, lesson, wiki, feedback, shared material) I want to mention the possibility of sharing an assessment with the language teacher so that the feedback for the student can come both from the content side (mine) and the language side (the language fellow teacher – Gabriella Zanrosso in this case).

There are at least three important drawbacks to face when using ICTs in class:

1. Sometimes they do not work the way we want or suppose they should. We need to test their functionality *before* entering the class and we always have to be ready with a B plan in case they are not available (because of a blackout or any other unpleasant event)
2. They can be a source of distraction. This can be avoided or at least minimized walking through the room (while helping them we can also check what the students are actually doing) or using a software to remotely control and monitor computers-lab<sup>5</sup>. Furthermore, an internal Moodle platform can be accessed without being connected to the Internet.
3. Every online activity leaves a digital trace on some server. The new GDPR warns us about being careful every time we give our data to a web company. Again, using an internally managed Moodle platform keeps this issue under control

Every time I use technologies I try to keep a certain balance between online and unplugged activities. For example, the fundamental algorithms of cryptography are

---

4 The Marzotto-Luzzatti Moodle platform is hosted on an internal blade server and administered by the head of the Computer Science department, Riccardo Crosato, so that we can have a complete control over its functioning and the data it contains. Beside that, the internal connectivity is very good thanks to the Gigabit ethernet.

5 One very good example is Veyon : <https://veyon.io/>

firstly introduced using a wooden cipher disk, a paper scytale and a paper Enigma Machine.

One of the main obstacles to the success of a CLIL activity is the reluctance of the students to talk in English. That is more than obvious since they are not used to it and they see no point in using a foreign language when it is so easy to communicate in Italian... *“Why should one make things more complicated than needed?!”*

To tackle this problem and win some embarrassment I try to use the experience of some of them who have been (or are going) abroad for the Erasmus+ project: I say to the class:

*«Let us pretend to be an international team of technicians coming from all over the world... This is something I have experienced myself both in my studies and in my job and it is what some of you has already experienced during the Erasmus+. It is, anyway, what might happen to all of you soon...*

*None of us is a native English speaker – my English is far from being perfect -, some of us are not fluent, but nevertheless we have to carry out a common task.*

*It is not essential to be accurate as long as we try our best to communicate and share our ideas; you won't be judged or evaluated about your level of English – though we'll ask the English teacher to give us some feedback in order to improve our accuracy and get rid of some mistakes...*

*My name is Luca, I'm from the Slovak Republic, where are you from?... »*

and so every student chooses a country and asks his partner where he comes from. I've found this trick to work pretty well with fourth and fifth year students. After a while the students get into the role playing and they even try to joke or argue in English.

## Activities

This project work is structured in 4 lessons, divided in activities for a total amount of 7 hours. The timing indicated for each activity is a downward approximation of what it took when I tried them for my tirocinio.

### Lesson 1: Introduction to Cryptography

Class : 5 <sup>th</sup> year	Level: A2-B1	Duration: 2 hours
Learning objectives:		
Content	Language	
<ul style="list-style-type: none"> <li>• General scheme of a secure communication</li> <li>• Basic concept of Cryptography and Cryptology</li> <li>• Mono alphabetic ciphers</li> </ul>	<ul style="list-style-type: none"> <li>• Acquiring new terminology</li> <li>• Practising fluency</li> <li>• passive forms</li> </ul>	

- Transposition and substitution

### CLIL - Intro to Cryptography

- Intro to Cryptography  
926.9KB Caricato il 18/10/2018 20:01
- slide (Intro to Cryptography)  
1.2MB Caricato il 31/10/2018 18:55
- "The adventure of the dancing men" by A.C.Doyle
- The Gold Bug by E.A.Poe
- (CLIL) Running dictate : Introduction to Cryptography
- cryptographic quiz
- Homework

timing	Activity name	Short Description
10'	Intro to CLIL	Since it is the first CLIL lesson I clarify what CLIL stands for and why I think it is a good thing... I also introduce the "international technician team role play" described in the Introduction
25'	Intro to Cryptography	<p>It is partially frontal and partially a work-in-pairs activity. I introduce the subject showing a stripe of paper (big enough for everybody to be read) and say : <i>This is the subject of our lesson</i></p> <p style="text-align: center; font-weight: bold; font-size: 1.2em;">TNOPAHDFTPEECOHWRRGYOSYR!</p> <p><i>... can you read it?</i></p> <p>they are forced to spell it letter by letter since it is gibberish. <i>Can you understand it?... No?! Sure, you're not supposed to understand it because the message is meant to be unintelligible to anyone except the intended recipient who knows the key and the process to decrypt it...</i></p> <p><i>The process is "wrap the stripe of paper around a cylinder" and the key is the diameter of the cylinder...</i></p> <p>then I give every couple a copy of the message to try and decipher it. Then we move to the the Caesar cipher and to other example of monoalphabetic ciphers taken from A. C. Doyle[5] and E. A. Poe[4]</p> <p>See the slides "<a href="#"><i>L1_CLIL_Into_to_cryptography_2018</i></a>" in the Student Materials folder for more details</p>
25'	"Hide and seek" + kahoot quiz	It is a scaffolding activity where the basic terminology is acquired searching around the room the terms which match the definitions given by the teacher.

		See the “ <i>hide&amp;seek_term_definitions.pdf</i> ” file in the Student Material folder. A kahoot.com quiz follows in order to check the correct matching.
5’	break	If the weather is good the class can move outside for the next activity
25’	Running dictate and sorting paragraphs	It is a scaffolding activity where the students also practice some reading, writing and speaking skills <sup>6</sup> . They work in pairs : a runner and a writer. One student runs to the wall where a short paragraph (one for each couple), has been hung by the teacher and reads a bit of it; next he runs back to his partner and dictates him what he has just read. As soon as the writer has written the piece of sentence, the runner goes to the wall again and repeats the process till the end of the paragraph. Some “process language” is given to the students to help them interacting during the task <sup>7</sup> . At the end every couple writes its paragraphs on a shared doc (a wiki), and the entire class discuss how to sort them. all paragraphs are taken from “The Code Book”[1] by Simon Singh except the last which is taken from “Data and Goliath” by Bruce Schneier[6] See the “ <i>Running_dictate_01_bigfont.pdf</i> ” file in the Student Materials folder. Some “process language” is suggested to help the students interaction.
20’	Moodle quiz	It is a quiz to revise the basic terminology and concepts acquired during the activities and to practice some basic ciphering methods. Every question has a proper feedback so that the student can correct himself.
5’	Homework + a glimpse to Vigenere	write five questions about cryptography. They might be simple questions with a straightforward answer or more difficult ones concerning something you didn't fully understand or something that has aroused your curiosity.

6 I got the idea of the *running dictate* from Joe, my CLIL methodology teacher during a course in Brighton. I immediately liked it because it gives a touch of kinaesthetic learning to the activities that the students appreciated. It has to be accurately prepared (I laminated the paragraphs and pinned it on the courtyard wall: since the weather was nice we could play the activity outside). Anyway this activity may take longer than expected.

7 By “Process language” I mean simple phrases helpful to carry out the task; For example: “Can you repeat, please ?” ; “how do you spell that?” “Can you speak more slowly?” “Are you sure?.. You might need to read it again”.



		<p>Chose one or two of them and record your answer on an audio-file of about one minute. Upload both the text with the questions and the mp3 file on our Moodle platform</p> <p><i>Only the brave:</i> Answer the above questions recording a video of about 3 minutes or develop a software that encrypt and decrypt a message</p>
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Lesson 2: From Vigenere to rotor machines

It is a bridge lesson to introduce the Enigma machine and the flipped classroom methodology.

Class : 5 <sup>th</sup> year	Level: A2-B1	Duration: 1 hours
Learning objectives:		
Content:	Language:	
<ul style="list-style-type: none"> <li>• Polyalphabetic ciphers</li> <li>• Vigenere cipher</li> <li>• Encryption machines</li> </ul>	<ul style="list-style-type: none"> <li>• Acquiring new terminology</li> <li>• Practising fluency</li> <li>• sharing opinions</li> </ul>	

timing	Activity name	Short Description
10'	recap	Discussion of the (most interesting) questions asked by the students and uploaded on the Moodle platform <sup>8</sup>
20'	Vigenere and poly-alphabetic ciphers	Frontal explanation of the Vigenere cipher, starting from the Caesar cipher, using the wooden cipher disk. Exercises (in pairs): pen and paper deciphering some messages given by the teacher. From the wooden cipher disk to the rotor machines. see slide " <a href="#">L2_CLIL_Vigenere_2018</a> " in the Student Materials folder
15'	Definition loop (group activity)	It is a scaffolding activity to introduce some new important terminology: <i>«Divide into groups of six people. Each of you will receive an unmatching pair : term and definition. One member of the group reads his definition and (only) the person who has the matching term will answer "I got it! It's ...". In his turn this person will read his definition for another member to match, thus repeating the process</i>
















<sup>8</sup> Some of the questions uploaded by the students showed a deep interest in the matter and would have taken a longer time to be properly answered. So I asked them to be patient because some of the answers might come with the following activities

		<p><i>until the loop is complete.</i></p> <p><i>Let's see an example with a loop of four definitions: »</i>  see slide "<b>L2_CLIL_Vigenere_2018</b>" in the student materials</p>
15'	homework	<p>the file "<b>Flipped classroom activity: The Enigma Machine</b>" (see Student Materials folder) is shown on the whiteboard and explained. The beginning of the videos is shown (if there is time enough)... "<i>Remember to bring to school an empty Pringle tube !!!</i>"</p>

### Lesson 3: The Enigma Machine

Class : 5 <sup>th</sup> year	Level: A2-B1	Duration: 2 hours
Learning objectives:		
Content	Language	
<ul style="list-style-type: none"> <li>• The internal functioning of the Enigma machine</li> <li>• Key space and brute force attack</li> <li>• The key distribution problem</li> </ul>	<ul style="list-style-type: none"> <li>• Acquiring new terminology</li> <li>• Practising fluency</li> <li>• passive forms</li> <li>• conditional clauses</li> </ul>	

### CLIL - Intro to Cryptography - The Enigma Machine

-  (slides) CLIL Lesson: Vigenere   
152.4KB Uploaded 5/11/18, 20:38
-  Flipped classroom activity: The Enigma Machine   
24.3KB Uploaded 3/11/18, 15:24
-  Typescript of the Video by Simon Singh   
155.8KB Uploaded 22/10/18, 19:13
-  A deeper look inside the Enigma machine
-  How to build a paper enigma machine
-  upload here your mp3 file
-  Conditional clauses   
23.9KB Uploaded 8/11/18, 16:36
-  crypto challenge
-  quiz about cryptography
-  Z team - chat with the mysterious foreigner
-  Y team - chat with the mysterious foreigner
-  X team - chat with the mysterious foreigner
-  W team - chat with the mysterious foreigner
-  A team - chat with the mysterious foreigner
-  feedback on the CLIL activities

timing	Activity name	Short Description
10'	Question time	Questions asked by the students about what they have watched at home <sup>9</sup> .
40'	Building an Enigma paper machine (work in pairs)	Watch : <a href="https://youtu.be/z1ehM1pHrIU">https://youtu.be/z1ehM1pHrIU</a> and See also <a href="http://wiki.franklinheath.co.uk/index.php/Enigma/Paper_Enigma">http://wiki.franklinheath.co.uk/index.php/Enigma/Paper_Enigma</a> Following the instructions build a <b>paper Enigma machine</b> with: reflector B right rotor (the fastest) : <b>IV</b> middle rotor : <b>V</b> left rotor (the closer to the reflector) : <b>I</b> (we have been collecting empty pringles tubes just for this moment!) and decrypt the next message given by the teacher:

9 This activity helps introducing the lesson and recap the main ideas also for the students who had only run through the homework materials. The questions asked by the students were actually a sign of a deep reflection and allowed me to clarify how to calculate the combinations of the plugboard and to answer: "most of your doubts and curiosities will be satisfied in the next activities..."

		<p>initial letter orientation: <b>KAR</b> message : <b>OTGKVZ</b>  initial letter orientation: <b>LFG</b> message:  <b>JYZUMLMTFLZCNAERIUIZAHTZ</b></p> <p>Then encrypt a message and send it to another couple, after sharing a key (an initial setting). Check it with the simulator[7] : <a href="http://enigmaco.de/enigma/enigma.html">http://enigmaco.de/enigma/enigma.html</a></p>
15'	Running dictate	<p>Same kind of activity seen in lesson one. The paragraphs are related to the Enigma machine and can be read in the file "<i>Enigma_Running_dictate.pdf</i>" in the Student Material folder</p>
15'	Conditional clauses	<p>It is a reading activity where the students have to recognize the different conditional forms (zero, first, second and third) in sentences concerning the Enigma machine (they are taken from original texts – see the file "<i>Enigma_conditionalClauses</i>").</p> <p>Therefore, while revising the grammar, the activity helps preparing the next one.</p>
35'	Explain & record (team work of three students)	<p>It is mainly a <i>speaking</i> activity: the students have to record an audio file<sup>10</sup> according to the following instructions. They have some time to write down some notes and get ready. They can also check for pronunciation using[8] or other sites.</p> <p><b>Student A</b> explains to student B and C the following points: how the Enigma machine looks like, the basic constituent parts of the machine, How the rotors works and their internal wiring</p> <p><b>Student B</b>, using the incomplete scheme <i>Enigma_partial_scheme.pdf</i>, explains to student A and C the internal functioning of the machine; or, in other words, the path followed by the electrical signal to light up a letter when the operator press a key</p> <p><b>Student C</b> explains to student A and B how to calculate (approximately) the key space (the number of initial settings); what is they key distribution problem and what is a brute force attack. If you are working in couples, student A plays also the role of student B</p> <p>Note: record a <b>single mp3 file</b> with the three voices. Every member of the group uploads the same file on his moodle account.</p>

<sup>10</sup> I got the idea of using the smart phone to record the speeches from Annalisa Maule, while observing her "tirocinio" lessons. The audio file allows both the students and the teacher to understand what has been learned and how to improve it.

## Lesson 4: Crypto challenge

Class : 5 <sup>th</sup> year	Level: A2-B1	Duration: 2 hours
Learning objectives:		
Content	Language	
<ul style="list-style-type: none"> <li>• Testing</li> </ul>	<ul style="list-style-type: none"> <li>• Practising fluency</li> <li>• passive forms</li> </ul>	

timing	Activity name	Short Description
75'	Crypto challenge (team work; groups of four)	<p>This is a Multi task<sup>11</sup> activity. Every step involves concepts related to cryptography and involves different skill (listening, reading, writing, speaking). To get to the next step the team needs to solve the previous. The first team that complete all the tasks, get the special prize!! See the <b>appendix1</b> for more details.</p> <p>The <b>very first task</b> is to decipher the entering password: GIRMFY that has been encrypted with the paper enigma machine ...</p> <p>The <b>second is a listening task</b>. The audio file is taken from [10] and contains the answer to “<i>How many years would it take to break the code if we had ten men checking one setting a minute, twenty-four hours a day, seven days a week?</i>” (twenty million years)</p> <p>The <b>third, fourth and fifth tasks</b> are related to different deciphering methods but they also involve reading and problem solving skills.</p> <p>The <b>sixth task</b> is a writing/reading activity: the students have to ask questions to a mysterious entity<sup>12</sup> (a kind of oracle) that in fact is a machine : a web site where many questions and answers have been memorized. If they ask the right questions they get the password for the next step... Some questions or answers are encrypted.</p> <p>The <b>final task</b> is a writing-reading-speaking activity: the</p>

11 The term “task” has in this paper the meaning explained in [9] : “‘Task’ as a pedagogical construct currently occupies an important position in language teaching pedagogy together with associated movements of ‘discovery learning’ and ‘cooperative learning... *Some are done individually and others in groups, Some require the learners to draw on all their language and content knowledge to solve problems whereas others focus the attention of the pupil on discrete, isolated aspects*”

12 The mysterious entity (or oracle) is a simple server application with a data base where I have recorded several couples of questions and answers. Three questions have been (arbitrarily) chosen by me as “the right ones” so the relative answers give a piece of the password; the answers to other questions give some hint to guide the students toward the right ones. At this stage the web application is plain simple and its improvement might be a little project to develop with the students.

		team have to get the last password from a mysterious foreign person who is listening to a chat room (this person is an English teacher <sup>13</sup> or somebody from the international civil service). They have to agree on a place for the meeting (somewhere inside the school or just outside) but also to ask general questions in order to recognize him/her.
15'	feedback	It is an online form that allows the students to self-evaluate their achievements and the teacher to evaluate the effectiveness of the activities and decide some adjustments. See the file <i>Feedback_CLIL_activities.pdf</i> for more details
30'	Individual quiz	It is an online quiz about the learning objectives of the activities: basic terminology, general encryption scheme, monoalphabetic ciphers, Internal Enigma functioning, key space. There is also a question about conditional clauses. See <i>Quiz_about_cryptography.pdf</i> for more details

---

13 When I tried this activity during my tirocinio the role of the mysterious person was played by Elisabetta Cazzola and Anna Colla – splendid teachers of the splendid English department – who, while working on some projects in “sala insegnanti” were also listening to five different chat rooms – one for each team.

## Evaluation

The evaluation is meant to be an opportunity to challenge oneself and to receive a constructive feedback about what how a student has learnt.

Though it is a Content and Language integrated Evaluation (CLIE), it is mainly based on content. The quiz is structured in order to *Distinguish the linguistic aspects from the disciplinary content*<sup>14</sup>.

In order to evaluate both the output and the process of learning I've taken in account three different points of view:

- (35%) The score obtained in the crypto challenge (team work)
- (35%) The score obtained in the individual quiz on the basic terms and concepts
- (30%) The teachers<sup>15</sup> evaluation on the overall approach to the activities (using the following grid)

	0 none	30 inadequate	60 adequate	80 good	100 excellent
Quality of the homework and other assignments					
Involvement and contribution to the activities					
Effort to talk and interact in English all the time					

I avoided evaluating the oral production through an “interrogazione” because as Carmel Mary Coonan says: *“Content teachers are not normally trained for this challenge. In fact, although the interrogazione mentioned above is an oral format, it is only used for assessing content knowledge. The content teacher does not use it to assess the pupils from the point of view of oral language proficiency. Indeed the teachers do not know how to assess oral language. Also, having to assess both dimensions, brings to the fore another new problem that concerns the balance that content assessment and language assessment should have in the overall mark.[11]*

<sup>14</sup> Graziano Serraggiotto, slides from the Lesson, 04/10/2018

<sup>15</sup> The English teacher might help to evaluate some outputs like “the conditional clauses” and the mp3 audio file.

## Next Lessons

The journey has just begun... there are other astonishing battles between code-makers and codebreakers to explore. Let us see a brief summary of the steps we are going to follow even though they have not been fully developed as CLIL activities yet.

### Cracking the Enigma machine

The great struggle of Alan Turing and his fellow cryptanalysts at Bletchley Park to break the code that was supposed to be unbreakable (impregnable). Using both the Simon Singh's book and the Turing's nephew booklet (Demystifying the bombe)[12] we'll focus on some genial intuition of Alan Turing like the disentanglement of the scrambler unit and the plugboard searching for loops in a crib (a piece of ciphertext whose relative plaintext is known) and the design of the bombe...

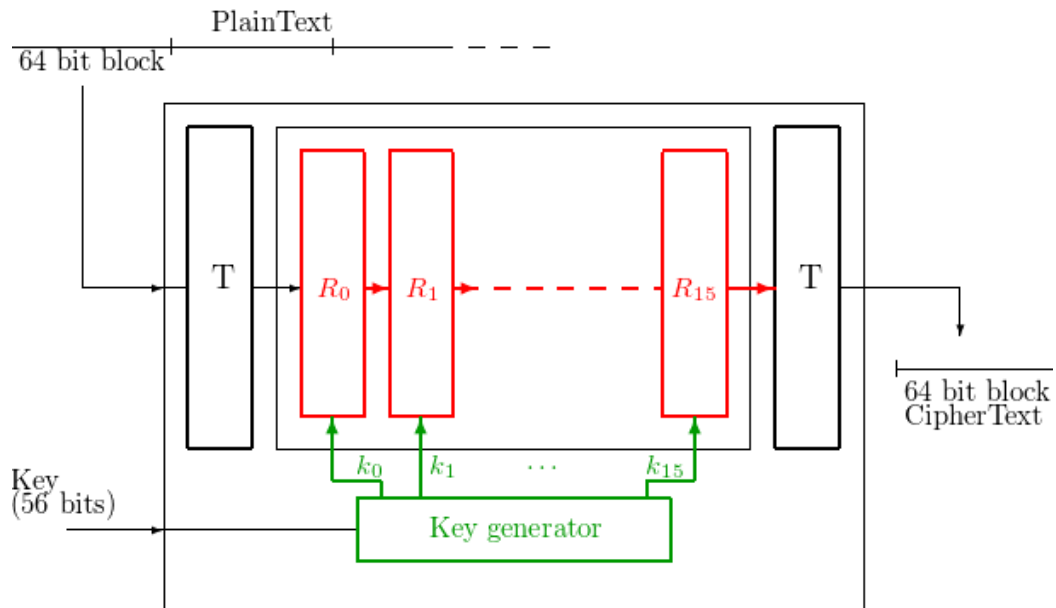
Discussing the movie "The imitation game" will help both understanding the unbelievable achievements of the crew at Bletchley Park and clearing some false ideas like the fact that Turing actually built the bombe.

### From Colossus to DES

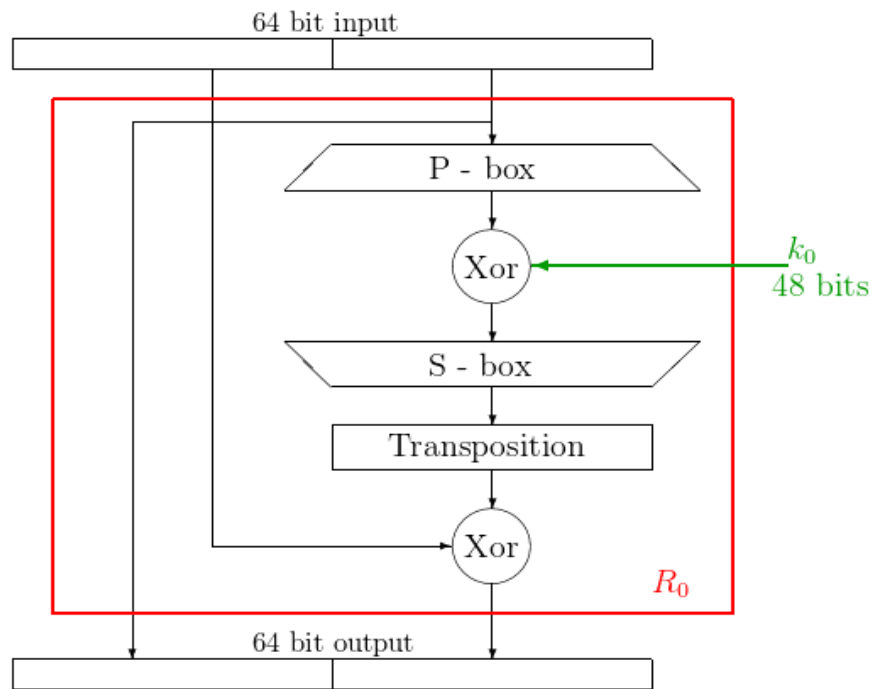
*"Drawing heavily on Alan Turing's concept of the universal machine, Max Newman, a Bletchley mathematician, designed a machine that was capable of adapting itself to different problems, what we would call a programmable computer"[1].* It was this new machine, named Colossus, that allowed the allies to read the code produced by an even stronger cipher machine, the Lorentz machine, used by Hitler to securely communicate with his higher commanders.

But if an electrical, highly sophisticated machine can break a code, a similar machine can also be used to devise a stronger cipher: using a computer we can easily implement a machine with tens of rotors and instead of ciphering each letter it can take a block of bits and scramble it in many different ways... The first international standard encryption algorithm was DES (Data Encryption Standard) whose internal functioning is shown in the following drawings:





Every single Round ( $R_n$ ) is the combination of three simple operations: substitutions (like the Caesar Cipher), transposition (like The scytale) and bitwise XOR between the block and the Key:



The strength of the cipher relies on the length of the key.

Somebody argued that the RSA lobbied the process of standardization in order to reduce the length of the key from 64 to 56 so that it would still be impregnable for everybody except the RSA itself that was the only agency on earth to dispose of the computational power needed by a brute force attack (the "Digital fortress" novel by Dan Brown[13] is entirely based on this assumption).

DES was publicly broken in 1998<sup>16</sup> and has been substituted by AES (Advanced Encryption Standard) which uses longer keys and blocks but whose internal algorithm still relies on the same basic mathematical functions used by DES.

## Alice and Bob go public

If the modern computer did help in devising very strong symmetric ciphers the key distribution problem still lay unsolved at the mid of the seventies. As it has already been underlined, the strength of a symmetric cipher rely on the secrecy of the key and in order for it to be shared between sender and receiver the only secure way was to meet in person. During WWII, for instance, every month a booklet with the initial Enigma settings of each day was delivered to every enigma operator but, using Singh words:

*"... And we may be in the North African Network (Rommel in his troops) and everyone in Rommel's Network would have one of these bits of paper and we wake up in the morning we'd say right it's the fourth of June and we'd set up our machine according to that fourth of June recipe ... But that bit of paper has to be biked across the desert and the guy delivering it may be incompetent, he may be a double agent, he may lose it and this is known as the key distribution problem and it's expensive time-consuming and risky..."[3]*

Imagine the web today if every time you send an email, purchase online or log in any social network, you should first meet with somebody to agree on a secret key... Though the solution of the key distribution problem was something desired by everyone, from the governments to the business men, only very few scientist were working on it since it was considered to be an unsolvable problem. It was an unconventional mathematician and computer scientist, Whitfield Diffie who, working with Martin Hellman and Ralph Merkle, first found a solution to the key distribution problem in 1976<sup>17</sup>

---

16 The Electronic Frontier Foundation (EFF) built in 1998 "Deep Crack" a machine to perform a brute force search of the Data Encryption Standard cipher's key space. Deep Crack costed less than \$250,000 and took less than 56 hours work to decrypt the message.

17 But in 1976 it was revealed that James H. Ellis,[4] Clifford Cocks, and Malcolm J. Williamson of GCHQ, the British signals intelligence agency, had previously, in 1969 shown how public-key cryptography could be achieved

We'll see the details of the Diffie-Hellman-Key-exchange protocol and of the RSA (Rivest Shamir Adleman) protocol. They both uses modular arithmetic...

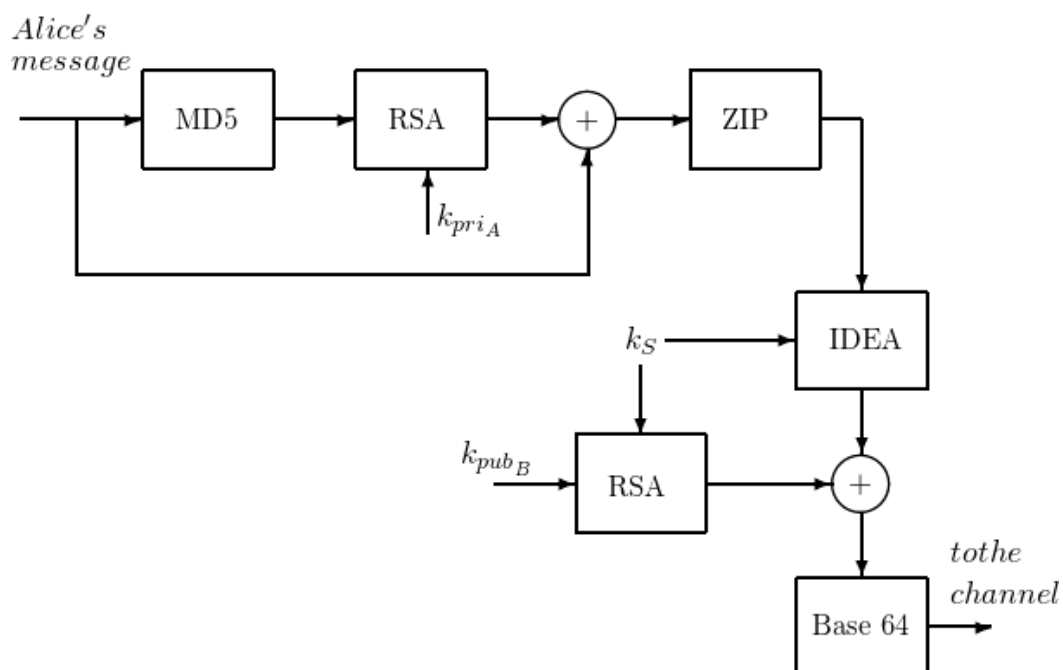
## Message Digest

Beside symmetric and asymmetric encryption algorithms, modern cryptography needs the digital “fingerprints” (or message digest) of a file. This is achieved by using a particular family of cryptographic functions, called HASH functions, that have five main properties:

- it is *deterministic* so the same message always results in the same message digest
- it is quick to compute the message digest for any given message (*computationally efficient*)
- it is infeasible to generate a message from its hash value except by trying all possible messages (*irreversibility*)
- a small change to a message should change the output so extensively that the new hash value appears uncorrelated with the old message digest (*avalanche effect*)
- it is infeasible to find two different messages with the same hash value (*collision resistant*)

## https, PGP and TOR

Hyper Text Markup Protocol Secure (https), Pretty Good Privacy (pgp) and The Onion Routing (TOR) are some of the most famous cryptographic systems used in everyday life. They use the three kind of modern cryptographic algorithms (symmetric, asymmetric and hash) to implement secure protocols of communication.



## Crypto Treasure Hunt

This is the final activity of the Unit. It is similar to the crypto challenge, but bigger: it takes a much longer time and it requires more hacking skills since it involves both ancient and modern cryptography.

An example of this activity can be found following the next link:

<https://www.youtube.com/watch?v=SKR-KRo4iUs>

## Further Development

A stimulating project<sup>18</sup> I would like to propose to the fourth year student is to develop a series of encrypted messages using different methods of increasing difficulty (some of them devised by the students). The messages should lead to an actual “treasure” hidden somewhere (probably on the WWW) and should be disseminated in a short video, made by the students<sup>19</sup>, telling a cryptographic story.

## Acknowledgements

During this course I’ve had the privilege of meeting some very good teachers from whom I have learnt a lot. In particular I’d like to thank Annalisa Maule, Roberto Lorenzin and Mara Meneghini who shared with me the “tirocinio” experience.

I am also grateful to Gabriella Zanrosso, Franco Perin and Francesca Benetti, my fellow teachers at ITI Marzotto, for helping me developing the didactic unit from different points of view.

Nothing of what is written on these pages would have any sense without the students. I wish to express my gratitude for the gorgeous girls and boys of the fourth and fifth years in Computer Science at ITI Marzotto: they have accepted my CLIL proposal in a very positive way, giving most valuable feedbacks and showing a high capacity of learning, despite my flaws both in contents and in language.

Thanks to Laura Filotto, Elisabetta Cazzola, Gabriella Zanrosso and Laura Camposilvan for revising most of the material. Their annotations and suggestions have been very precious.

For keeping our Moodle platform updated and very performing – and for being always a shining example – I’m grateful to Riccardo Crosato so as I’m grateful to Mattia Bedani for sharing the everyday effort of giving the students a good education: without him I couldn’t have carried on both this course and the many other projects of our computer science department.

---

18 The idea for this activity comes from the short movie “The Thomas Beale Cipher” [14], kindly reported to me by tutor Elena Borsetto

19 Some students already have very good skills in video making. Three of them, for instance, made a promotional video for a school project: [https://www.iisvaldagno.it/wp/wp-content/uploads/2018/10/LinuxDay2018\\_lr.mp4](https://www.iisvaldagno.it/wp/wp-content/uploads/2018/10/LinuxDay2018_lr.mp4)

Finally, my greatest thanks is for Mirka, my wife, and for Giacomo, Elia and Lorenzo, my sons, because most of the time invested in this course has been stolen from the time I own them: they patiently waited for dad while he was in “writing mode”.

## Appendix1

### Crypto Challenge:

The very first task (step 0) is to decipher the entering password: GIRMFY  
It has been encrypted with the paper enigma machine and the following settings:  
left rotor: I letter T  
middle rotor: V letter E  
right rotor: IV letter R

crypto challenge

crypto challenge is a password protected lesson.

Please enter the password:


step 1

crypto challenge

You have earned 0 point(s) out of 0 point(s) thus far.

*How many years would it take to break the Enigma code if you had ten men checking one setting a minute, twenty-four hours a day, seven days a week?"*

Listen to the audio file and answer using less than seven words (do not use digits).



Your answer

step 2



## step 5

You have earned 4 point(s) out of 4 point(s) thus far.

The right question(s)

to get the password you have to ask the right question(s) to a mysterious person using the next form:

<http://10.10.3.103/~docentei/oracolo.php>

You can ask as many questions as you wish, but only the right one(s) will give you the password.



## final step

## crypto challenge

You have earned 5 point(s) out of 5 point(s) thus far.

meet the mysterious one

The last password is known only by a mysterious person that can be contacted using the chat room:

"? Team - chat with the mysterious foreigner"


Use it to make arrangements to meet him/her and to understand how to recognize him/her

Your answer

Submit

the magic words are squeamish ossifrage

*Response:*



Congratulations!!

Get your special prize... Ask your teacher (If you dare)

By the way...

The text "**The Magic Words are Squeamish Ossifrage**" was the solution to a challenge ciphertext posed by the inventors of the RSA cipher in 1977

## Bibliography

- 1: Simon Singh, The Code Book, 1999
- 2: Carmel Mary Coonan, Teresina Barbero and others, PERSPECTIVES, 2012
- 3: Simon Singh, The Enigma Machine Explained, 2013, [https://youtu.be/ASfAPOiq\\_eQ](https://youtu.be/ASfAPOiq_eQ)
- 4: Edgar A. Poe, The Gold Bug, [http://users.telenet.be/d.rijmenants/the\\_gold\\_bug.pdf](http://users.telenet.be/d.rijmenants/the_gold_bug.pdf)
- 5: Arthur Conan Doyle, The Adventure of the Dancing Men, , <https://sherlock-holm.es/stories/pdf/a4/1-sided/danc.pdf>
- 6: Bruce Schneier, Data and Goliath, 2015
- 7: Enigma Co., Online Enigma Simulator, <http://enigmaco.de/enigma/enigma.html>
- 8: Reverso Context, <https://context.reverso.net/>
- 9: Carmel Mary Coonan, Taking the matter to Task, 2008
- 10: Jacquie Bloese, The Imitation Game - Adapted, 2015
- 11: Carmel Mary Coonan, CLIL In (Language) Teacher Training, 2011
- 12: Dermot Turing, Demystifying the Bombe, 2015
- 13: Dan Brown, Digital Fortress, 1998
- 14: polymix, Award Winning Animation Short Film: The Thomas Beale Cipher, 2011, <https://www.youtube.com/watch?v=sKMxtfMSPTM>