Coding

Topic	Algorithms
Learning objectives	Know the different ways of coding and learn to decode
Age group	12-16 years (to be adapted in each country)
Estimated duration	45 min
Activities	Encrypt and decrypt
Related visits	Paris

Previous knowledge required

No particular prerequisites are required.

Step by step: the sequence in the classroom

Step 1: Introducing the topic

Short presentation of the heritage elements in this sequence

Cryptography is a science somewhere between mathematics and computer science but with very practical applications. Its aim is to protect information, usually by making it seem incomprehensible by mixing and transforming it according to a particular method.

There is also a cryptographic technique called Steganography, which is used to hide a message in seemingly innocuous text or images. These messages can be sent in the Untitled design-2.png

Untitled design-3.pngpublic domain without worrying about being intercepted or discovered, even accidentally.

A bit of history

- From 800 BC to 200 BC: The Spartans used scytales
- Around 600 BC: Nebuchadnezzar used shaved skulls
- Around 480 BC: Dematarus (Greek), isolated in Persia, uses wax tablets to warn his country of the plans of Xerxes (Persia)
- 100 BC / 44 BC: Caesar's cipher (alphabetical shift)
- 1st century: Appearance of invisible ink (organic fluids rich in carbon)
- 1580: Digit by substitution of symbols (Code nomenclature) - Mary Stuart
- 1586: Treatise on ciphers: Vigenère cipher
- 1930: Enigma machine
- Late 20th century: Appearance of public key encryption – RSA

Coding definition:

Cryptology: The science of cryptography and cryptanalysis.

Cryptography: Science of creating cryptograms.

Cryptanalysis: Science of analysing cryptograms with a view to decrypting them.

Cryptogram: Encrypted message.

Encrypt / Cipher / Crypt: Transform a text or piece of information by replacing the letters (or words to encode) in a script made up of predefined signs.

Decrypt / Decode: transform an encrypted message into a clear message that conforms to the original.

Decrypt: find the cipher used in the cryptogram.

Clear text: original message before encryption.

Ciphertext: text obtained after encryption.

Key: Element (word or number) that transforms the application of the encryption and/or decryption method.

Codes classification:

Substitution cipher: Crypto system in which each letter of the message is replaced by another character, but keeps its place in the message.

Transposition cipher: Crypto system in which each letter of the message remains unchanged, but is moved to another place in the message.

Mono alphabetic substitution: Substitution cipher where the encrypted alphabet remains the same throughout the encryption. Substitution by letters, symbols, digits or numbers, etc.

Poly-alphabetic substitution: Substitution cipher where the ciphered alphabet changes during the encryption. This change is carried out according to a key.

Nomenclature code: This type of cipher combines simple substitution (each letter is replaced by a symbol) and a repertory code (certain words are also replaced by a symbol, as well as disruptive symbols).

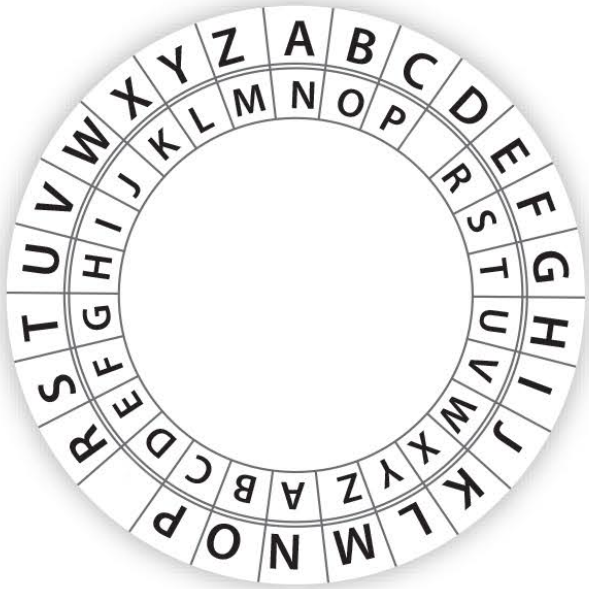
Step 2: Class activities

Example of the most known coding systems

1. Caesar's cipher or Cesar's code

For important communications to his army, Caesar encrypted his messages. What is known as Caesar's cipher (mono-alphabetic substitution) is a shifting of the letters of rank 4: to encrypt a message, **A becomes D**, **B becomes E**, **C becomes F**, etc.

To take all the letters of the alphabet into account, it is wiser to represent the alphabet on a wheel.



Credit Fermat Science

To decrypt the message

"DOHD MDFWD HVW"

so all you have to do is shift the letters in the other direction: D is decoded as A, E as B, etc.

The decoded message is then:

ALEA JACTA EST

Decrypt the following 3 messages:

WKH URPDQV

YLFWRUB

HPSHURU

2 The Vigenère cipher

The Vigenère cipher is a polyalphabetic subsitution algorithm.

Instead of circularly matching letters, each letter is now associated with another letter (in no fixed order or as a general rule).

For example :

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
F	Q	B	M	X	I	T	E	P	A	L	W	H	S	D	O	Z	K	V	G	R	C	N	Y	J	U

To encrypt the message

"TO BE OR NOT TO BE THAT IS THE QUESTION"

look at the correspondence and replace the letter E by the letter X, then the letter T by the letter G, then the letter R by the letter K...

The encrypted message is then:

"GD QX DK SDG GD QX GEFG PV GEX ZRXVPDS"

To decipher it, knowing the substitutions, we do the reverse operation.

Decrypt the following 3 messages:

HFGE PV IFSGF VGPB

OWFJ NPGE SRHQX KV

FSDGEXK PMXF IKDH HFGEV

3 The Porta cipher system

Porta was an Italian physicist and inventor of the first literal double-key system, i.e. the first cipher for which the alphabet changes with each letter.

This polyalphabetic system was extremely robust for its time, so much so that many consider Porta to be the "father of modern cryptography". Giovanni Della Porta invented his cipher system in 1563, and it was used successfully for three centuries.

Here is an example of the Porta encryption table:

AB	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
CD	a b c d e f g h i j k l m z n o p q r s t u v w x y
EF	a b c d e f g h i j k l m y z n o p q r s t u v w x
GH	a b c d e f g h i j k l m x y z n o p q r s t u v w
IJ	a b c d e f g h i j k l m w x y z n o p q r s t u v
KL	a b c d e f g h i j k l m v w x y z n o p q r s t u
MN	a b c d e f g h i j k l m u v w x y z n o p q r s t
OP	a b c d e f g h i j k l m t u v w x y z n o p q r s
QR	a b c d e f g h i j k l m s t u v w x y z n o p q r
ST	a b c d e f g h i j k l m r s t u v w x y z n o p q
UV	a b c d e f g h i j k l m q r s t u v w x y z n o p
WX	a b c d e f g h i j k l m p q r s t u v w x y z n o
YZ	a b c d e f g h i j k l m o p q r s t u v w x y z n

Credit photo – apprendre-en-ligne.net

To cipher using one of these alphabets, the letter opposite it in the table is chosen to replace the letter in the plaintext. For example, if you are encrypting using the alphabet AB, you will substitute a for n, b for o, q for d, and so on.

For example, if the keyword is **STEEL**, the alphabets S, T, E, E, L, S, T, E, E, L, etc. are used successively to encrypt the message. If we encrypt the phrase "**Porta cipher**" with the key **STEEL**, we obtain:

Clear	p	o	r	t	a	c	i	p	h	e	r
Key	**S**	**T**	**E**	**E**	**L**	**S**	**T**	**E**	**E**	**L**	**S**
Coded	L	K	G	I	V	T	Z	E	S	Z	A

The cipher porta was used by Queen Marie-Antoinette to modify and improve the cipher PORTA for use in her correspondence. In particular, she added the feature of encoding only every other letter.

Step 3: Homework and development ideas

How about a challenge? Pass coded messages to your classmates so that they can decipher them.

For example, choose a coding method and encrypt your message, then pass it on without giving away the method used.

Add a little suspense by giving a time limit or a reward.

You can also create your own decryption wheel, which is easy to find on the internet: https://www.youtube.com/watch?v=0Xuv58Uwu9o

Material needed for the tour

Pupils participating to the tour will need to have pencil, eraser and paper to find the right code.

VISIT MATH

Co-funded by the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Project code: 1-FR01-KA220-SCH-00027771

Learn more about Visit Math at: https://visitmath.eu

FERMAT SCIENCE
Une autre idée des maths

5th High School
Agrinio · Greece

ISTITUTO STATALE "E. MONTALE" PONTEDERA

LogoPsyCom

ZS 31

YuzuPulse