The Caesar cipher	Season	03
	Episode	09
	Time frame	1 period

Prerequisites : Concepts of cryptography.

Objectives :
- Discover a simple encryption algorithm.
- Practise the encryption and decryption processes.

Materials :
- *Beamer about the Caesar cipher.*
- *Lesson about the Caesar cipher.*

1 – How the Caesar cipher works 15 mins

The teacher explains, with a beamer, the history of the Caesar cipher and how it works.

2 – Coding and decoding a short message 20 mins

Each student encodes a simple question that he will send to another student, who will decode the question using the key indicated by the sender, and then send back an encrypted answer.

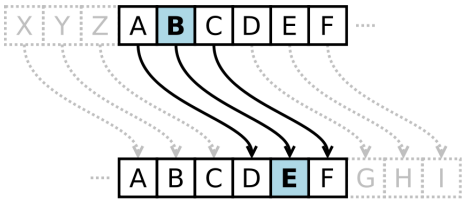
3 – Breaking the code 20 mins

Working in pairs, students try to decrypt some message without knowing the key.

According to Suetonius, a historian in the Roman Empire, Julius Caesar used a simple code to preserve the secrecy of some messages.

> "If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others."

Any encryption technique in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet has become known as a *Caesar cipher*.



An example

v	e	n	i	v	i	d	i	v	i	c	i
Y	H	Q	L	Y	L	G	L	Y	L	F	L

The implementation chain of a cipher