New world **New skills**

Computers and Codebreaking

PwC's Primary School Toolkit

pwc

Today's objectives

1. To know how to decrypt a message
2. To know what input, output and functions are
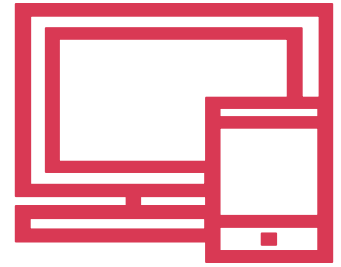3. To know how to encrypt using a Caesar cipher

What is a computer?

How do you decrypt a message in a secret code?

How do computers work?

What are inputs and outputs?

Can a computer imitate a human?
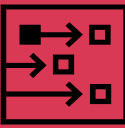
Discuss as a class

What is a computer?

Inputs

Computers need specific instructions in order to function properly.

These are known as **inputs** (E.g. pushing the 'on' button).

Inputs   **Outputs**

Outputs

When a computer then does something as a result of an **input**, this is called an **output** (e.g. the computer switches on).

Inputs   Outputs

Functions

Computers use **functions** to get things done. Humans create these functions for a computer to use. However, computers are not like humans and need much more specific instructions on how to do something.

Function - Turn on the computer
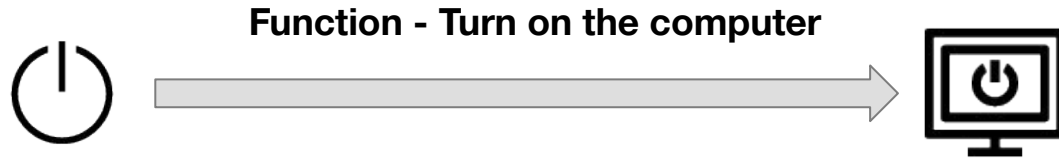
Activity: Computer Teacher

You are going to pretend your teacher is a computer.

Your task is to navigate your teacher across the room by giving them instructions on where to move.

"Move forwards 3 steps"

"Wrong way!"
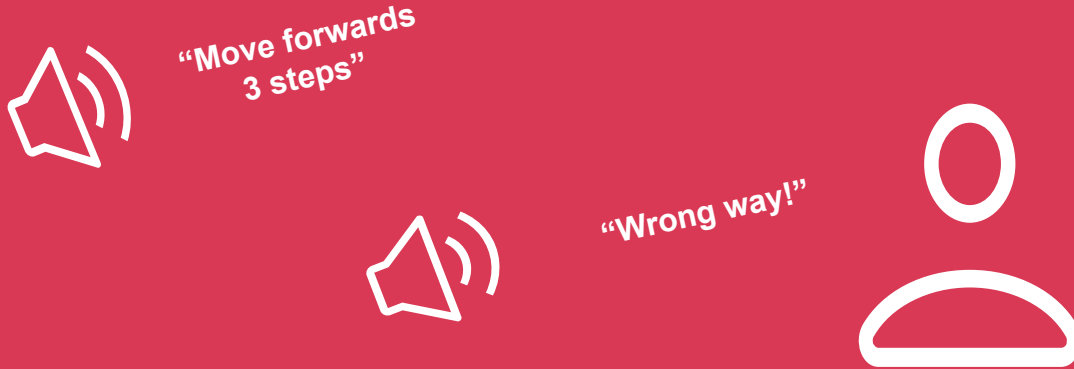
Tip: Computers are not like humans so make sure to be specific!
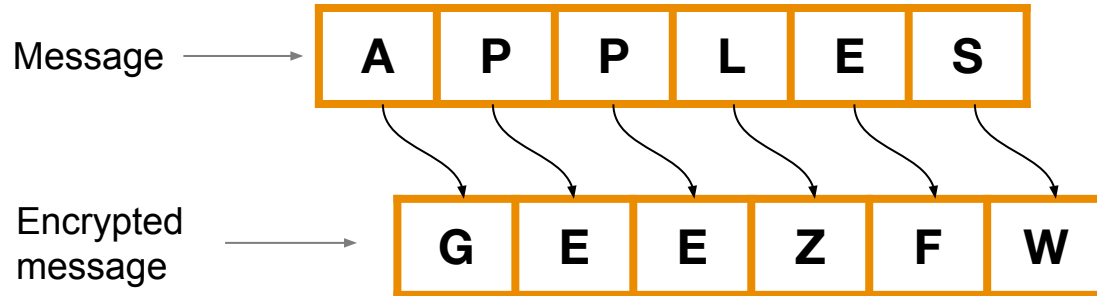
Codebreaking and Encryption

Have you ever wanted to send a secret message to someone?

If a message is written in code, we say that the message is **encrypted**.
If we wanted to find out what a secret message says, we would need to **crack the code!**

Codebreaking and Encryption

Message → | **A** | **P** | **P** | **L** | **E** | **S** |

Encrypted message → | **G** | **E** | **E** | **Z** | **F** | **W** |

The Caesar cipher

The Caesar cipher

- The Caesar cipher was used by an ancient Roman emperor called **Julius Caesar** when he wanted to send messages to his soldiers.

- Back then, there were no emails or post vans, so messages were hand-delivered by human messengers who ran on foot to make their deliveries.

- These messages would contain important military strategies so it was important that nobody else would be able to understand them without knowing how to crack the code.

Caesar Cipher

How to make a Caesar Cipher

To make a Caesar cipher, we need to give each letter of the alphabet a number.

So let's say:

- 'A' is 1
- 'B' is 2
- 'C' is 3 and so on, all the way to
- 'Z' is 26.

Now, we make the cipher by shifting each of these numbers by a fixed number.

Caesar Cipher

For our cipher, let's shift each letter by 2.

So we add 2 to each of these numbers:
– 1 + 2 = 3,
– 2 + 2 = 4 etc.

Instead of an 'A', we'll now write a 'C', because 'C' is two letters ahead of 'A' in the alphabet.
- 'B' becomes 'D'
- 'C' becomes 'E'
- 'D' becomes 'F' and so on.

Before Encryption	After Encryption
A (1)	C (3)
B (2)	D (4)
C (3)	E (5)
D (4)	F (6)
G (5)	I (7)
…	…

Activity: Caesar Cipher

Let's try **encrypting** the word 'Hello' using a Caesar cipher, moving each letter along by **two** places.

Extension: Can you come up with a code for the person next to you to try and break?

Activity: Caesar Cipher

Let's try **encrypting** the word 'Hello' using a Caesar cipher, moving each letter along by **two** places.

Answer
'H' becomes 'J'
'E' becomes 'G'
'L' becomes 'N'
'L' becomes 'N'
'O' becomes 'Q'

So 'Hello' in our new code would be written as '**JGNNQ**'.
Pretty good, right?

Extension: Can you come up with a code for the person next to you to try and break?

Wrap up and Reflection

In computing, what is an example of an output?

A: Shouting 'open!' at the computer

B: Pressing the On button

C: Selling a computer on eBay

Wrap up and Reflection

?

Who was Julius Caesar?

Wrap up and Reflection

How do you create a Caesar cipher?

Any questions?

?

pwc.co.uk