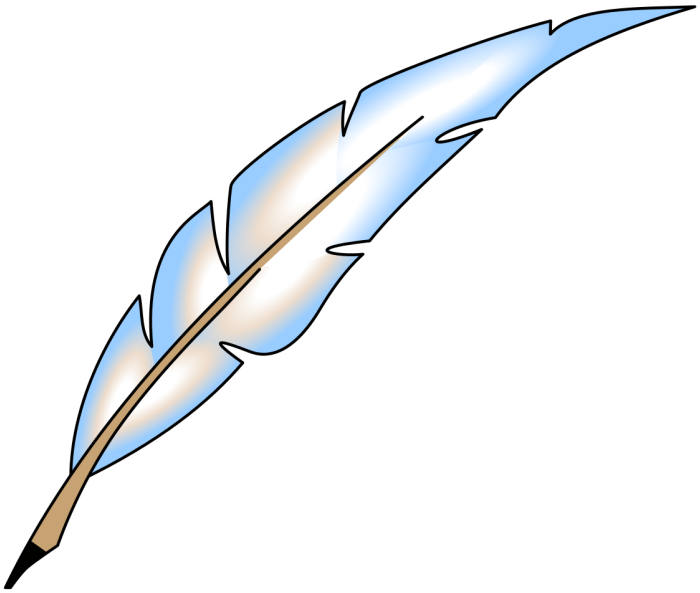
technocamps

Inspiring | Creative | Fun

Ysbrydoledig | Creadigol | Hwyl

The Codebreakers



Swansea University Prifysgol Abertawe

Cardiff University Prifysgol Caerdydd

Prifysgol Bangor University

Cardiff Metropolitan University | Prifysgol Metropolitan Caerdydd

i.t.wales www.itwales.com

Prifysgol Aberystwyth University

Prifysgol Glyndŵr University

University of South Wales Prifysgol De Cymru

Yn gweithio ar ran Llywodraeth Cymru

Working on behalf of the Welsh Government

Aims

- To learn how to use encryption to write secret messages.
- To learn how secret codes were used during WW1.
- To learn how to decrypt secret messages in three different ways.

Overview

In this workshop, we will be looking at a particular method of writing secret messages that no one else will understand! This method has been used for hundreds of years and we'll look at how secret codes were used during WW1.

We will learn how to write secret messages, how to work out what a secret message means using 3 methods, and finally we'll use these skills to help the war effort!

Key Words

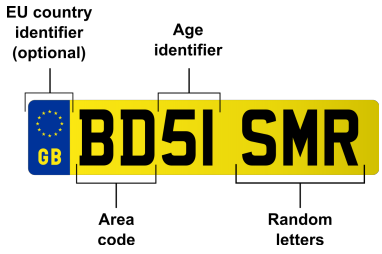
Encryption
Key
Cipher Wheel

Decryption
Code

Encryption – Using symbols, letters or numbers, or rearranging letters to disguise a message.
Decryption – Using a method to work out what a disguised message means, a lot of the time using a key.
Key – A key is a piece of information which is used to encrypt or decrypt a message. Like locking and unlocking a door, using a different key to unlock a door won't work, it must be the same. Even if we know how to open the lock, we still can't without the correct key.
Code – A code replaces words, phrases, or sentences with groups of letters or numbers.
Cipher Wheel – A wheel with letters or symbols which can be used to easily encrypt a message. The key is given by how much the wheel is turned.

Everyday Code

In our daily lives we see codes everywhere, but we may not realise it! Code is used in order to communicate information in a shorter or easier way. Car registration plates is one example, post codes, barcodes on items in shops, QR Codes for scanning, these are all examples of code we see around us.



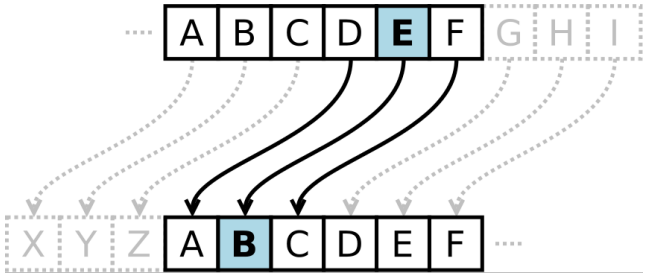
How can we hide a message?

Write a list in this box or fill out the spider diagram below:

The Caesar Cipher

The Caesar Cipher, also known as a shift cipher, is one of the oldest and simplest forms of encrypting a message.

It is a type of substitution cipher where each letter in the original message (which in cryptography is called the plaintext) is replaced with a letter corresponding to a certain number of letters shifted up or down in the alphabet.



Julius Caesar (after whom the cipher is named) used this by shifting the letters in the alphabet by 3 places, so D becomes A, and E becomes B and so on. This meant that no one could quickly read messages that they weren't supposed to if they only had a quick glance.

Encrypting using the Caesar Cipher

At this point you should have a very useful Cipher Wheel to help you encrypt your message. If not, you can find a digital copy in the Scratch Game at http://bit.ly/CipherWheel or a printable version at https://bit.ly/technocampsTWF

1. Encrypt "The White Feather" using a Caesar Shift of 3.

T H E W H I T E F E A T H E R

2. Encrypt your teacher's surname with a shift of 3.

3. Encrypt someone's name from your school using a shift of either 3 or 4.

Decrypting using the Caesar Cipher

Now that you're an expert in encryption, try using decryption to read the secret messages below:

1. L W U L H G. L U H D O O B W U L H G.

2. L G R Q R W Z D Q W B R X U Z D U.

3. L ' P V X U U R X Q G H G E B J K R V W V.

4. (Hint: This may not be a shift of 3!)
Q M P I W X S K S F I J S V I M W P I I T

What do you think this has to do with WWI?

Can you think of any connection between what we've looked at so far and The Great War?

How could a codebook help with decrypting secret messages?

Are there any disadvantages to using a codebook?

Another example of codes used, this time during WWII, were broadcast on French radio shows from London. To most these look like meaningless (and rather silly) messages. What do you think they might really mean?

Clementine will find a basket of eggs at her door.

Jean has a big moustache.

Methods of Decryption

In terms of ciphers, the Caesar Cipher (a form of substitution cipher) is one of the simplest, meaning it is rarely used anymore. A computer could break a cipher shifted message very quickly. There are a few different ways to do this and we will explore a few of them below.

First of all, is breaking a code by knowing the key. Look at the note below and see if you can work out how to decrypt it.

(7)

APT

P OHCL H ZLJYLA
SLA'Z TLLA
KHU

Now what about if we don't have the key? Is there anything else that can help us? Try this note below. (Hint: What letter might the 'M' on its own be? Can we work out a key from this?)

M PMOI WEVEL,
FYX HSR'X XIPP
LIV M WEMH WS.

Extension Task: Frequency Analysis

Frequency analysis is the term for looking at the letters or symbols to see which one appears most. In the English language, the letter that appears most often is the letter "E". This means that by tallying up the letters and seeing which appears the most, then setting the key so that it matches up with the letter "E" we can find the key.

EWWLEWGMLKAVWLZ

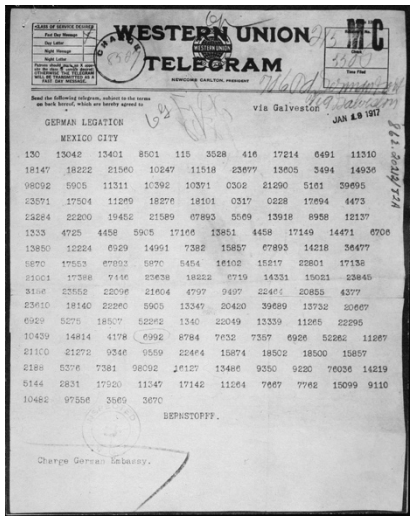
WYSLWLZAKWNWFAFY

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

What does the message say? Key : _____

Room 40 And The Zimmerman Telegram

During the First World War, codes, ciphers and cryptography had become vital in ensuring that communications were kept secret. Due to this, codebreaking also played a vital role in the war effort on both sides. The British set up a group of people whose role was to decrypt German codes. This was important work which led to important German information being stolen and used to their advantage. This group were known as "Room 40" and one particular breakthrough led to the USA joining the War effort.



The Zimmerman Telegram

The Zimmerman Telegram was an encrypted message sent in 1917, by Germany to Mexico, trying to convince them to join their side and go to war with the USA if they allied with Great Britain. The message however, was intercepted by the British before it crossed the Atlantic to the USA and on to Mexico. It was then decoded by the men and women of Room 40. The British then had to pretend that one of their spies had stolen the telegram as they didn't want the USA to know they were intercepting all of their communications! The USA weren't too happy about the Telegram and joined the War effort in 1917, while the British didn't let them know they were eavesdropping on their messages for many years after!

Use the space here to decipher the messages given to you!

Message A:

Message B:

Message C:

Message D:

Message E: