Year 6 to 7 - Encryption

Bishop Challoner

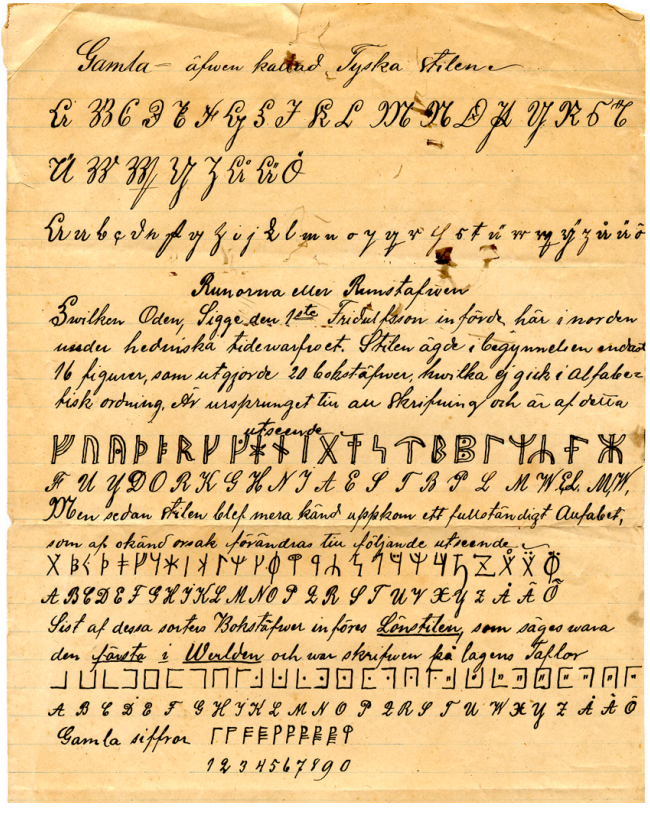
Computer Science Department

Learning Intentions

- To know how computers keep our personal and private information safe.
- To understand how messages can be encrypted so that no one can read them.
- To be able to encrypt your own message using code breaking techniques.

But First… A History Lesson

- Encrypting messages did not start with a computer.
- For centuries people have wanted to keep the contents of their messages secret from others so that people do not read them.



Notice that at the top of the gravestone, there is the symbol of a pair of compasses, one of the symbols of the Freemasons. The inscription appears to read "Thomas Brierley joined the group in July 16th 1785",


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

Activity 1 - PigPen Decode

- The PigPen cipher is a very old (1531!) cipherer that can be used to encrypt messages. Your job is to decode the following messages using your wipeboards.


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


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


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


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

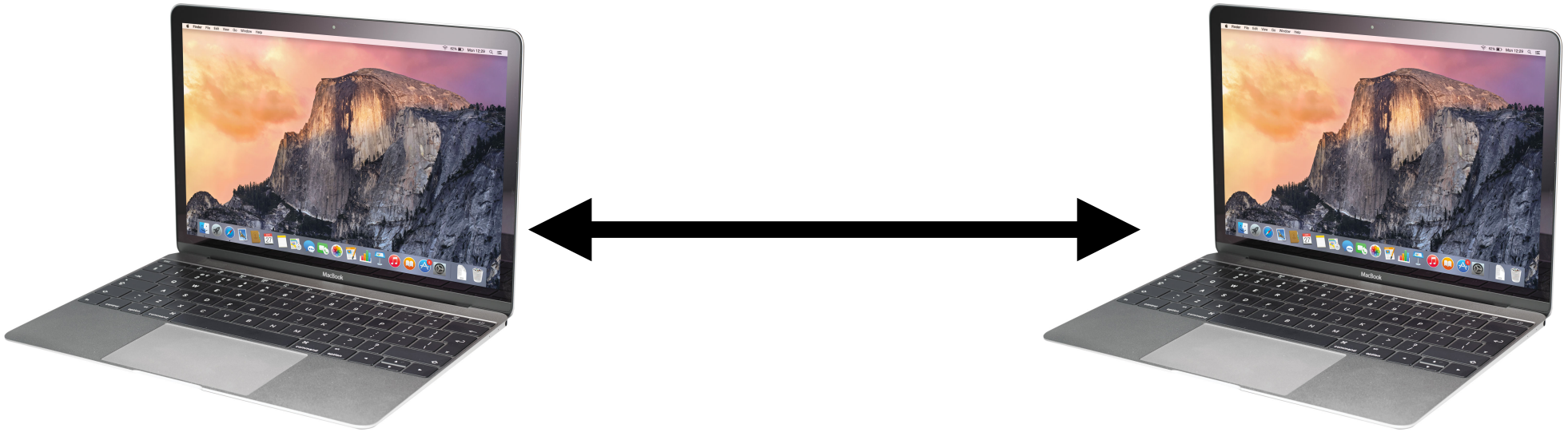

A B C
D E F
G H I


J K L
M N O
P Q R


S
T U
V


W
X Y
Z

Back to the 21st Century



YouTube

NETFLIX


ords

So how do we stop them seeing our passwords?

- This is done using something called **encryption.**

- Encryption takes a word or sentence and jumbles the letters up so that to someone without the knowledge of how to un-jumble it, it looks like gobble-die goop!

West Bromwich Albion

YGUV DTQOYKEJ CNDKQP

We used a Caesar Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25	26

West Bromwich Albion

YGUV DTQOYKEJ CNDKQP

Activity 2 - Cracking the Code(s)

- On the sheet coming round are some pieces of text that have been scrambled using the Caesar Cypher.
- Your job is to work out what these sentences say.
- Once you have found out what the sentences say, you are to answer the question that the sentences ask, writing your answer in the space provided.

You are to work individually to complete this

EXAMPLE

ALEX MW XLI REQI SJ XLI JEQSYW GSQTYXIV WGMIRXMWX ALS LIPTIH XS GVEGO XLI IRMKQE QEGLMRI?

- You are going to be using a website in order to complete this exercise.
- The website is: **tinyurl.com/y8djoyux**

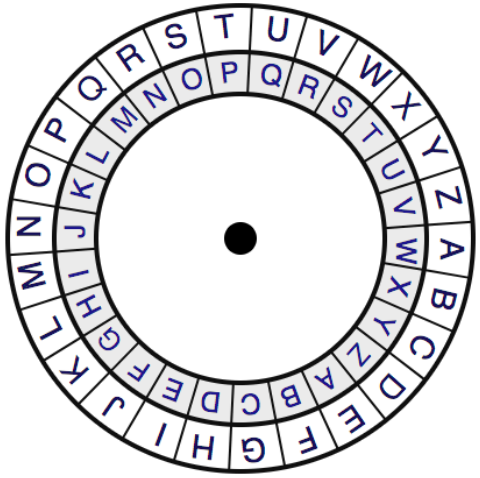
Caesar cipher decryption tool

The following tool allows you to encrypt a text with a simple offset algorithm - also known as **Caesar cipher**. If you are using **13** as the key, the result is similar to an **rot13 encryption**. If you use *"guess"* as the key, the algorithm tries to find the right key and decrypts the string by guessing. I also wrote a small article (with source) on **how to crack caesar-cipher** in an unknown context of an encrypted text.

If you want some in-depth knowledge, I highly recommend to read this **book**.

Alex mw xli reqi sj xli jeqsyw gsqtyxiv wgmirxmwx als liptih xs gvego xli lrmkqe qeglmri?

Use key: 22



Encrypt / Decrypt

Output:

What is the name of the famous computer scientist who helped to crack the Enigma machine?

Extension

- Decode the names of five baby animals by cracking the Caesar Cipher. Shift each letter a constant amount forwards or backwards through the alphabet. For example, you might replace A with C, B with D, C with E and so on. The same code is used for every coded baby animal.

- **WNVDEBGZ**

- **EXOXKXM**

- **DBMMXG**

- **IBZEXM**

- **VABVD**