Key Turn

|  |  |
| --- | --- |
| Number of Pupils: | 4 + |
| Age Range: | 13-15 |
| Duration: | 50 minutes |
| Type of Activity: | Worksheet |
| Workshop Creator: | Ally Weir - [ally.pcgf+keyturn@gmail.com](mailto:ally.pcgf+keyturn@gmail.com) |

# Introduction:

This workshop aims to make students more aware of how their personal data is shared across the internet and let them experience some of the approaches that companies and governments handle their personal information.

By exploring simple, manual encryption methods, this workshop explores how algorithms are constructed to obscure the content of a message. These are then taken and students are given the opportunity to problem solve the decryption of the simple cypher presented. Through contemporary examples that the age group can relate to, these simple examples give a deeper understanding of encryption's importance online in protecting them and their identities.

For classes that grasp the topic quickly or are at a higher level, this learning can be expanded to interactively demonstrate the difference between public/private key encryption and symmetric key encryption.

# Intended Learning Outcomes:

After completing the “Key Turn” Workshop, pupils should be able to …

* Explain what it means to encrypt a message
* Explain what it means to decrypt a message
* Give examples of where encryption is used
* Give reasons why encryption is important in business and personally
* Explain what a brute force attack is

# Curriculum Links:

* Ties into the learning outcome in National 4/5 curriculum of encryption within the Security section of the course.
* This workshop is best taught alongside other Internet related content as it can be contextualised in this setting.
* Also a topic of general interest, showing students how important encryption is to them personally and society as a whole.

# Setup:

*Materials provided with the Workshop –*

* + - Powerpoint presentation
    - Summary sheet
    - Caesar Wheel template PDF

*Photocopy Instructions:*

* Enough Caesar wheels need to be printed for either one each or one per pair.

*Equipment Required:*

* Scissors to cut the wheel template out
* Scrap paper for the participants to use
* Split pins to attach the inner and outer wheels together
* A lockbox with two padlocks (preferably the locks are different colours)

*Optional:*

* Having the Caesar wheels pre-printed and made will give more time for material. This is recommended to give lots of time for discussion of the topic.
* Could lay the Caesar wheel parts together rather than attaching together if you can’t get split pins. Less fun!

*Room Layout*

* The participants work together in pairs in the last exercise.

# Background Information

Encryption is the process of encoding messages or information in such a way that only authorised parties can read it. This is essential in situations such as online banking, e-commerce or any business that handles and stores sensitive personal information.

Encryption has a long history. From Roman leaders sharing hidden messages to its ubiquity online to protect banking, e-commerce, social networks and any other personal, sensitive data. This history is rich with exciting stories worth discovering as background information and using to enthuse students. An example is Alan Turing’s work during WWII at Bletchley Park.

The workshop explores the following two types of encryption generally without requiring a huge amount of in-detail knowledge.

Symmetrical Key Encryption is when both the encryption and decryption keys are the same. Both parties must have the same code before they can secretly communicate.

Public Key Encryption is when the encryption key is published for anyone to use and encrypt their message. The receiving party then has a secret decryption key they use to read any message sent. This is used to avoid the issue of getting a symmetrical key to the other person.

**This video explains these two concepts clearly and is definitely worth watching!** (6 mins): https://www.youtube.com/watch?v=GSIDS\_lvRv4

A **Caesar Wheel** has two sets of the alphabet, one within the other. You can turn the inner alphabet wheel a set number of *shifts* to make a Caesar cipher. The *plaintext* alphabet matches a *ciphertext* alphabet which can be used in place of sending a plaintext message, encrypting a message to be sent. If the receiving party knows the number of times to shift the inner wheel from its rest position (*ciphertext* **a** matching *plaintext* ***A***), they can then decrypt the message.

# Overview of Activity

* **Introduction – the Grab** **–** Discussion of online accounts (5-10 Minutes)
  + Pose the question “How many online accounts do you have online?”
    - Ask what kind of accounts they have. Banking, gaming, social, app store, e-commerce…
    - How many accounts do most people have?
    - How many times are they logging into accounts everyday?
    - How do companies protect (or at least try to) personal information?
    - Does anyone know of times companies have been hacked and information stolen?
* **Crossover** **–** A Brief History of Encryption (5 Minutes)
  + Ancient Romans hiding messages to make sure they got to the recipient safely
  + WW2 work at Bletchley Park essential to winning the war
  + Snowden getting messages to Journalists (**in slides as prompts**)
  + Spies & espionage in the 21st century, but they don’t need to meet up in a park
  + **Tell the pupils we are going to try encrypting our own secret messages to share amongst ourselves**
* **Activity 1** **–** Caesar Ciphers (20 Minutes)
  + **Use the basic cipher to decrypt the first message together as a class**
  + **Hand out the Caesar wheels**
  + **Encrypt a word and decrypt a word together as a class using the wheels.**
* **Activity 2 -** Caesar Ciphers cont. (10 Minutes)
  + **Get everyone in each pair to write a 3 word phrase encrypted with a Caesar Cipher Key of their choice**
  + **Swap with another pair but don’t give them the key. Let them try to decrypt the message.**
    - Ask how they tried to break the code
      * Brute Force
      * Letter/Word Frequency
      * Trying to get the other person to tell them the key
      * Other ways possible such as social engineering/theft.
    - Discuss how in a Caesar Cipher, you can easily brute force the answer.
      * Any encryption system is eventually breakable
* **Activity 3-** Public Key Lockbox Demonstration (5 Minutes)
* **(See this video for demo:** [**https://www.youtube.com/watch?v=jJrICB\_HvuI**](https://www.youtube.com/watch?v=jJrICB_HvuI)
  + **Get 5 participants to stand at the front of the room**
    - The participants at either end are sender/receiver
    - 3 in the middle are the Internet
    - Participant A want the lockbox (with chocolate inside) to get to Participant E without the Internet in the middle getting whats inside.
  + **Send the box with A’s padlock to E through B,C,D.**
    - It gets there but they can’t open it
  + **E puts their padlock on the box**
  + **E sends the box back to A**
  + **A removes their padlock**
  + **A sends box to E**
    - At this point only E’s padlock should be on the lockbox
  + **E unlocks their padlock and gets to the chocolate**
    - This is an example of public key encryption
* **Conclusion / discussion / next steps / sustain** **–** Encryption is essential (5 Minutes)
  + Highlight that there are many types of encryption. They become harder to break more every year.
    - But nothing is 100% secure
  + Highlight its importance in many different areas and essential for businesses
  + “Next time you are online or using an app, think about what information is getting transmitted about them, who it is going to, how it gets there and how is it kept secure.”