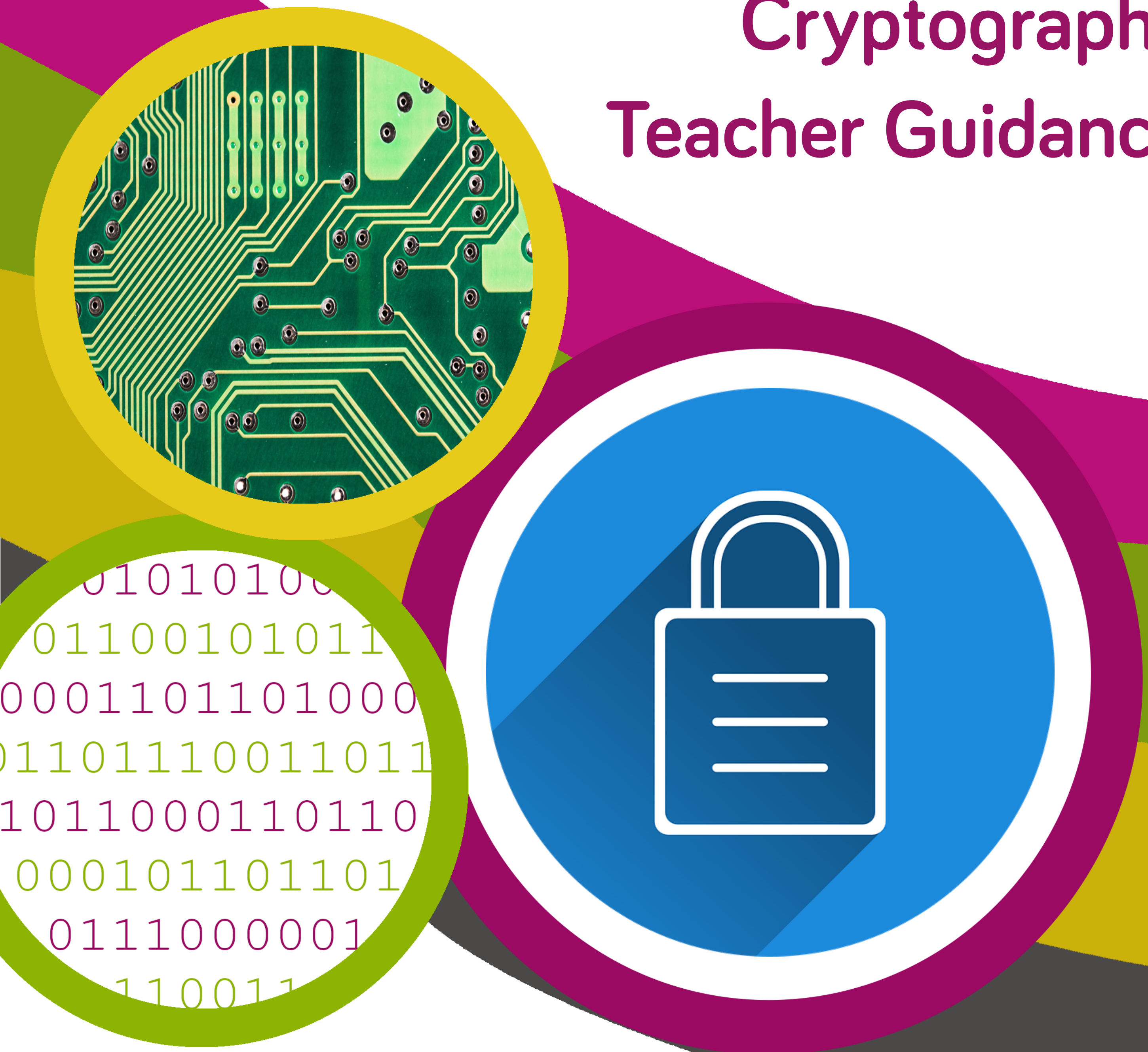
technocamps

Cryptography Teacher Guidance



UNDEB EWROPEAIDD
EUROPEAN UNION

Llywodraeth Cymru
Welsh Government

Cronfa Gymdeithasol Ewrop
European Social Fund

Prifysgol Abertawe
Swansea University

Cardiff University
Prifysgol Caerdydd

Prifysgol Bangor University

Cardiff Metropolitan University
Prifysgol Metropolitan Caerdydd

i.t.wales

Prifysgol Aberystwyth University

Prifysgol Glyndŵr Wrecsam | Wrexham Glyndŵr University

University of South Wales
Prifysgol De Cymru

Curriculum Links

Links to Science and Technology AoLE

Computation:

(PS4) I can explain the techniques used to store and transfer data and understand their vulnerabilities.
(PS3) I can explain the importance of securing the technology I use and protecting the integrity of my data.

Being Curious:

(PS4) I can describe the impacts of science and technology, past and present, on society.
(PS3) I can evaluate my methods to suggest improvements.

Links to Other AoLEs

Humanities:

(PS3) I have an understanding of how factors in the past and present have shaped my communities.

The Four Purposes and Cross-Curricular Skills

This resource provides opportunities for **Critical Thinking and Problem Solving** throughout. When evaluating each encoding and encryption method, the learners will recognise potential issues with the security of the methods and be able to suggest ways of improving upon them.

Some of the aspects of the **Data and Computational Thinking** strand of the **DCF** is covered in the resource with learners needing to follow decryption instructions in order to receive the plaintext messages. Any mistakes they make during the decryption process will allow them the opportunity to correct the mistakes they have made.

Why Is Learning This Important?

This resource allows the learners to explore the history of cryptography and learn the basic ways that information has been communicated secretly for millenia. The developments of different encoding and encryption techniques is explored and learners can apply the techniques to gain access to information hidden in code. Cryptography plays a pivotal role in protecting people online, whether it be protecting their authentication details for a website, or keeping their personal messages to friends and family private. This resource serves as an introduction to the world of cybersecurity and the importance of keeping safe online.

Suggested Approaches Key

In this suggested approach we use the following colours to differentiate the types of activities:

- **Yellow - Explain.** Teachers should explain the slide/example to the class.
- **Green - Discuss.** Teachers should start an open discussion with the class to get them to feedback some answers/ideas.
- **Purple - Activity.** Learners are expected to complete an activity whether it be in their workbooks or on the computer, followed by a discussion of their solutions.
- **Green - Introduction/Conclusion.** The introduction/conclusion is also colour coded green. Teachers should hand out materials in the introduction and conclude the session and collect materials at the end.

Introduction

Begin with introductions, and a brief explanation of the Technocamps programme, before handing out any necessary resources for the activities.

Activity: Spider Diagram

Learners to fill in the spider diagram with examples of when they think they need to send and receive secure messages.

Explain: Steganography

Steganography is the practice of concealing messages or information within other non-secret text or data.

Steganography comes from the greek steganos meaning concealed and graphein meaning writing.

Steganography is used in digital watermarking and sometimes used to send hidden messages.

Example include:

- Watermarking
- Invisible ink
- Bacon Ciphers
- Micro-dots

Activity: Define Steganography

Learners to fill out workbook sections on:

- What is steganography?
- What does steganography mean?
- When is steganography used?

Histiaeus's Servant

Explain: Histiaeus's Servant

Histiaeus sent a message to his vassal by shaving the head of his most trusted servant, then tattooed the message on the back of the servant's head. After the servant's hair had grown back, Histiaeus sent the servant off to the vassal. When the servant arrived, he shaved his head to reveal the hidden message.

This is a form of steganography. If the servant was searched, no message would be found unless they shaved his head.

Activity: Histiaeus's Servant

Learners to draw out a story board of the servant example in their workbooks.

Discuss: Problems with the System

Discuss with the class what problems there are in our servant example:

- How long does it take to send a message?

We have to shave the head, tattoo the head and then wait a long time for the hair to grow back. So sending an urgent message quickly is not possible.

- Can the same system and servant be used multiple times?

The system could be used multiple times, but tattoos don't exactly come off, so a different servant may be needed each time.

- Are we allowed to have servants and tattoo them?

No, we don't have servants any more and people are unlikely to consent to us tattooing general messages on their heads.

Explain: Sir Francis Bacon

Sir Francis Bacon was born in 1561 and died in 1626. He served as legal advisor to Queen Elizabeth. When King James I succeeded Queen Elizabeth, Francis Bacon's standing grew very quickly. He was knighted, then made a Baron, and finally was given the title Viscount St. Alban.

Francis Bacon has been called the father of empiricism, that scientific knowledge should be based only on inductive reasoning and observations. Prior to this, people were following the Aristotleian method: If sufficiently intelligent men discussed a topic long enough, they would discover the truth.

As a result Francis Bacon is often credited as the father of the scientific method.

Importantly for us, he came up with a steganographic method of hiding messages through the use of different fonts.

Explain: The Bacon Cipher

The Bacon cipher is a method of hiding a message inside another message by changing the font.

The first step is to write out our hidden message. We then choose two different font types such as bold and italic or comic sans and Edwardian script.

Then we write out a boring message which needs to have at least 5 times as many letters in it as our hidden message.
One of our fonts will be A, one will be B. We change the font of our boring message from A to B for each corresponding letter in our hidden message.

Now run through the example in the slides step by step so the learners fully understand how the encoding process works.

a: AAAAA	h: AABBB	o: ABBBA	v: BABAB
b: AAAAB	i: ABAAA	p: ABBBB	w: BABBA
c: AAABA	j: ABAAB	q: BAAAA	x: BABBB
d: AAABB	k: ABABA	r: BAAAB	y: BBAAA
e: AABAA	l: ABABB	s: BAABA	z: BBAAB
f: AABAB	m: ABBAA	t: BAABB	
g: AABBA	n: ABBAB	u: BABAA	

Activity: Bacon Cipher Practice

Learners to attempt to decrypt the messages provided on the slides and in their workbooks.

Solutions:

ChoCOLAtE CaKEs ArE TaSTY WE ALSo lOVE pIE
ABBAA AABAA BAABA BAABA AAAAA AABBA AABAA
M E S S A G E

THe grAsS IS GREenEr WHERe yOu WAteR
AABBB ABAAA AAABB ABAAA ABBAB AABBA
H I D I N G

ChEeSEY cHIps YUM
ABABA AABAA BBAAA
K E Y

tHe qUICk brOWn FOX juMpS oVER tHE lAZy Dog aNd SO Did I. iT IS vERY fun
BABBA AABBB AABAA ABBAB ABAAA BAABA ABABB BABAA ABBAB AAABA AABBB
W H E N I S L U N N C H

Discuss: Problems with the Bacon Cipher

Discuss with the class what problems there are in the Bacon cipher:

- How obvious is it that there is something hidden in the message?

It is really obvious that some message is hidden in the text because different fonts aren't very subtle. The closer the choice of two fonts are to each other, the less obvious it is there is a hidden message but this will add to the difficultly of both encoding and decoding the message.

- How hard would this be to do by hand

This method was developed in the 1600's so most if not all messages would have been written by hand. Creating two different fonts and interchanging between them whilst writing by hand is quite difficult especially when characters need to be consistent.

Extension Activity: Make Your Own Invisible Ink

Learners to mix one part baking soda with one part water.
Using an ear bud, write a message on a separate piece of paper.
Wait for the invisible ink to dry.
Paint lightly over the "plain" paper with dark fruit juice.
The hidden message should be revealed.
Learners should then write down the steps for making the ink in their workbooks.
Ask if the learners have an idea why this happens:
Acid + Alkali reaction causing a colour change on the paper.

Discuss: Recap

Recap the steganographic techniques the learners have used, how they work and some of the problems associated with them.

Activity: What Is Cryptography?

Learners to write down what they think cryptography is in their workbooks.

Explain: Cryptography

Cryptography is the practice and study of techniques that are used for secure communication.

Cryptography comes from the greek kryptos meaning secret and graphein meaning writing.

Cryptographic techniques are used all the time in day to day life without you even noticing. Examples include:

- Bank account payments
- Web browsing
- Messaging apps including Snapchat and WhatsApp
- Online stores and user account verification

Cryptography is different from steganography. We don't hide the fact that a message has been sent. Instead our security comes from the difficulty in decrypting the message without a specific key that has been used in encryption.

Activity: Define Cryptography

Learners should fill out their workbook:

- What is cryptography?
- What does cryptography mean?
- When is cryptography used?
- How are cryptography and steganography different?

Explain: Code Books

One cryptographic method that is commonly used is based on code books. We write an entire dictionary type book that changes the meaning of words or phrases.

We have a copy and the receiver has a copy.
We write out our message and encrypt each word of phrase in the message according to our code book.

Our receiver decrypts the message using an identical copy of the code book.

Activity: Make Your Own Code Book

Learners should complete the activity in their workbooks on creating their own code books.

Get some learners to share their messages, especially those who have attempted the extension.

Discuss: Code Talkers

Changing individual words and phrases during encryption is kind of like translating to another language that we hope an eavesdropper doesn't speak. The code book kind of works like a phrase book or dictionary for a second language

We need to make sure the language we choose to encrypt to isn't widely spoken. Can we think of any obscure languages?

Welsh is a fairly obscure language and has actually been used during some wars as an encryption technique. This is because not many people outside of Wales speak welsh.

Explain: Navajo Code Talkers

During the second world war, the Americans used native American Navajo people as code talkers. The Navajo language was spoken by very few people outside of the Navajo reservations.

So by translating the military messages into Navajo before sending them over radio was a great encryption system. Each platoon would have a Navajo person whose job it was to encrypt and decrypt messages.

This was most commonly used in the battles around the South Pacific. If people in America outside the Navajo reservations didn't speak Navajo then it was very unlikely that the Japanese could understand it.

However, there were some interesting problems with using Navajo. Modern military terms in English didn't have an equivalent in Navajo, so boats were named after sea creatures, whereas planes and helicopters were named after birds.

Explain: Pig Pen Cipher

The Pig Pen cipher has been used throughout history as an encryption technique by a secret group called the Freemasons.

The Freemasons are a fraternal organisation that are kind of like a secret club. They have special handshakes, codes and rituals that they aren't supposed to share with the outside world.

They also aren't allowed to write any of their lengthy initiation rituals down in plain English. So many new members use ciphers like the pig pen cipher to record the rules to make it easier for them to learn.

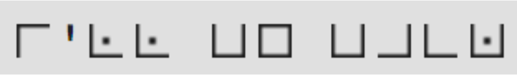
To use the pig pen cipher, each letter in your plaintext message is encrypted using the grid seen in the learners' workbooks.

The weird symbols are then sent as the message and the receiver, decrypts them.

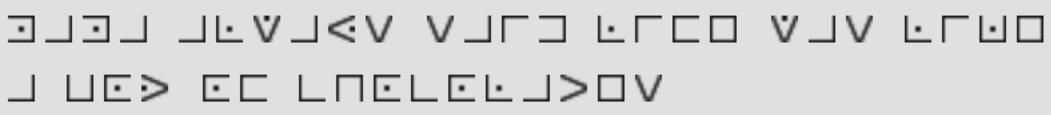
Activity: Pig Pen Practice

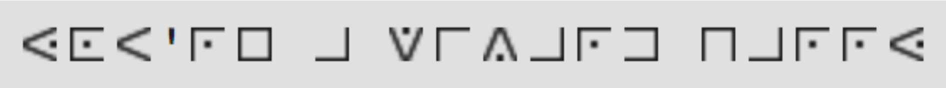
Learners should attempt to encrypt and decrypt the messages provided in their workbooks.
Solutions:

I'll be back.

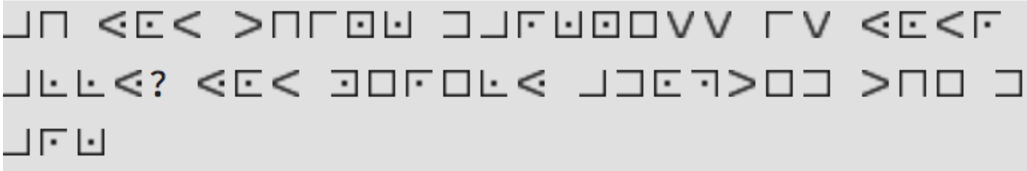


Mama always said life was like a box of chocolates.





You're a wizard Harry.



Ah you think darkness is your ally? You merely adopted the dark.

Discuss: Codes vs. Ciphers

Discuss with the class the differences between codes and ciphers:

- How is the pig pen cipher different from a code book?
- What does a code book encrypt?
- What does the pig pen cipher encrypt?

So what is the difference between a code and a cipher?

A pig pen cipher encrypts individual letters whereas a code book encrypts entire words or phrases i.e. codes encrypt words or phrases, ciphers encrypt individual letters.

Explain: Julius Caesar

Gaius Julius Caesar was born in 100 BC and died in 44 BC. He was assassinated in the senate by republican senators. He was a roman politician, dictator, military general and historian. He led 2 expeditions to Britain in 55 BC and 54 BC. He was elected to Consul, the highest rank in the roman army when he was 40 years old.

In his 20's he was captured by pirates. He was so charismatic that, whilst being ransomed, he joined in with the pirates during their games and exercises as if he was part of the crew. He even told them to ransom him for more money as they didn't appreciate his worth. He often joked with them that when he was free he would have them all hanged.

When the ransom was paid and he was set free, he raised a fleet of ships and set sail to capture them. After the pirates were imprisoned, Julius Caesar removed them all from prison and crucified them as he had often told them he would.

As a military general he devised an encryption method called the Caesar cipher. It is a form of shift cipher. Each letter in the plaintext is shifted forward by three. During decryption each letter is shifted backward by three.

Activity: Julius Caesar Fact Profile

Learners should fill out the Julius Caesar fact profile in their workbooks.

Explain: The Caesar Cipher

The Caesar cipher is a shift cipher with key = 3.

This means even letter in the plaintext message will be shifted forward 3 letters in the alphabet during encryption. So the letter "A" is encrypted as the letter "D".

To decrypt a Caesar cipher the receiver shifts each letter in the cipher text backward 3 letters in the alphabet. The letter "E" is decrypted to mean the letter "B".

Example:

Plaintext message: Hello world

Ciphertext: Khorr zruog

Activity: Cipher Wheel Cut Out

Learners should cut out the two wheels from their workbooks and pin them together with paper fasteners. By rotating the wheels, learners can see the different alphabets for the different shift keys.

Activity: Shift Cipher Practice

Learners should attempt to decrypt the messages provided on the slides and in their workbooks.
Solutions:
Key = 3

Whfkqrfdpsv lv ehwwhu wkdq vfkrro zrun
Technocamps is better than school work

Brx'uh jrqqd qhhg d eljjhu erdw
You're gonna need a bigger boat

Key = 9

Cxcx r'en j onnurwp fn'an wxc rw tjwbjb jwhvxan
Toto I've a feeling we're not in Kansas anymore

Key = 21

Yj jm yj ijo. Oczmz dn ij omt
Do or do not. There is no try

Extension: Key = 17

Z druv r gifdzjv di wifuf. R gifdzjv. "Ufe'k pfl cvrmv yzd jrdnzjv xrdxvv" reu z ufe'k dvre kf
I made a promise mr Frodo. A promise. "Don't you leave him Samwise Gamgee" and I don't mean to

Discuss: Breaking a Shift Cipher

Discuss with the class how hard it is to break a shift cipher:
How hard do we think it is to break a shift cipher?
How many keys are there to check?
How quickly can you check each key?
How quickly could a computer check each key?
How could we make it more difficult?

Explain: Transposition Ciphers

All of the cryptographic techniques we have looked at so far have involved replacing words or letters with other words or letters or symbols. These are referred to as substitution methods.

A second type of method is known as transposition method. Instead of substituting the letter or words, we jumble them up. This creates a very hard anagram that would need to be broken, unless you knew how we had rearranged the letters.

Explain: Scytale

Back in ancient Sparta transposition ciphers were used to send messages, using a usually wooden cylinder called a scytale.

Two cylinders with identical circumference were created, one kept by the messenger and one kept by the recipient.

A long and narrow piece of material, normally leather, was wrapped around the scytale and the message was written across it.

The material is then unwrapped and sent as one long list of letters. The recipient wraps the material around their identical scytale and can read the message.

Extension Activity: Scytale

Learners should cut out long strips of paper. The paper is then wrapped around one of the provided scytales to encrypt a message.
This can be done a couple of times at the front of the class as an example or in pairs/threes with one learner acting as an eavesdropper.

It should be clear how difficult it is to unscramble even short phrases, let alone entire messages.

Explain: Rail Fence Cipher

The rail fence cipher is another transposition cipher. This time instead of relying on specific circumference cylinders, we rely on a shared key.
We will write our message in a zig zag pattern along a certain number of rails. We then read out the message along the rails and send it to our recipient.

To decrypt the message, the recipient writes out a zig zag pattern of boxes according to the number of rails and then writes the message out across these, starting from the top rail and working down. Write the message back out across the same number of rails.

The number of rails acts as the key in this system.

For example:
Key = 4

Plaintext:	this is a secret message
Ciphertext:	tatghssemaeiieresscs

Activity: Rail Fence Cipher Practice

Learners should attempt to encrypt and decrypt the messages provided on the slides and in their workbooks. Solutions:
Key = 4

Tytiwghmsecanlanraseratiayaytcpms
Thats my secret captain, I'm always angry

Tnddoiinbniftaeonyy
To infinity and beyond

Key = 2

Loamiteatinwoktemhcpano
Look at me I am the captain now

Myhodeebiyufvuatedsvrenoraor
May the odds ever be in your favour

Key = 3

Wittuvaoeeldnwntsriewntlyloaoviti
Well I don't want to survive, I want to live

Jksmutepwmigsein
Just keep swimming

Extension: Key = 5
Mdsriolosknegtrteodafo
Mr Stark, I don't feel so good

Discuss: Recap

Recap with the learners both the cryptographic and steganographic techniques they have learnt today:
What is the difference between steganography and cryptography?
What is a Bacon cipher?
How do we reveal invisible ink?
What is the difference between a code and a cipher?
What is a pig pen cipher and how does it work?
What is a shift cipher, how do we encrypt and decrypt one?
What is a scytale?
What is a rail fence cipher, how do we encrypt and decrypt one?

Activity: Escape the Box

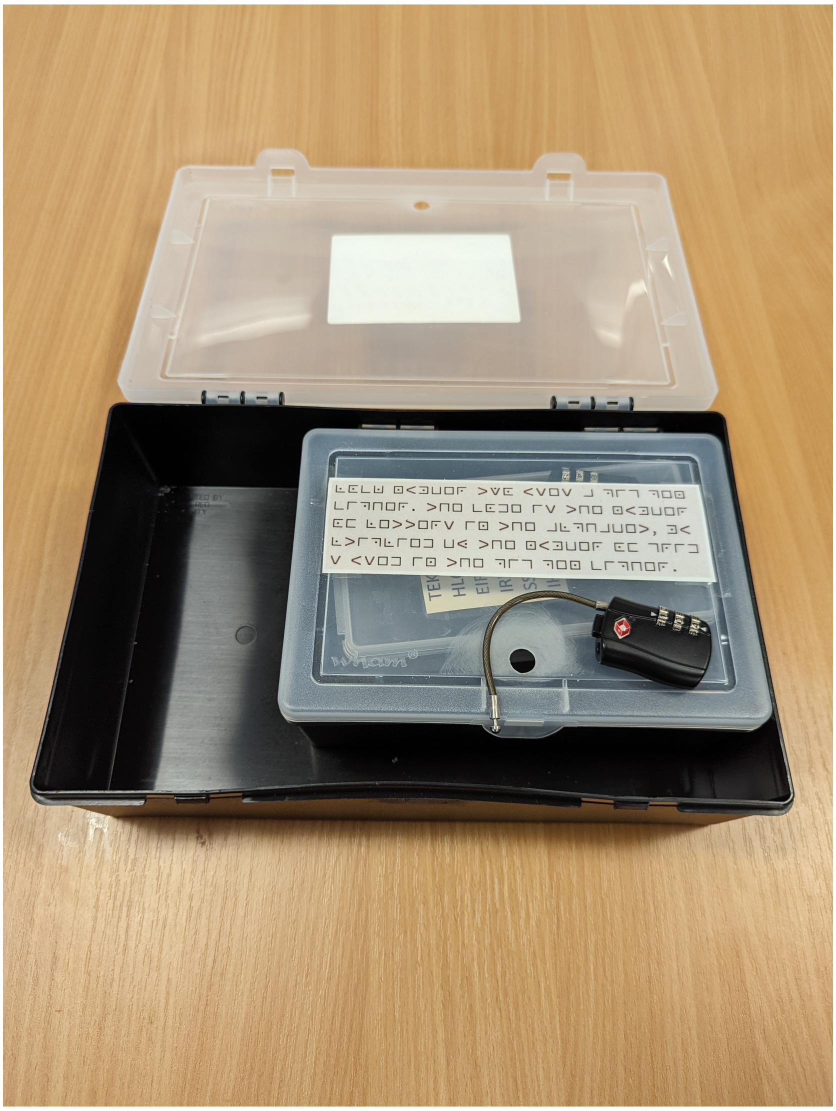
In small groups of 5-6, learners to try and break into the box by solving clues and decrypting ciphers that are based on the techniques they have been taught so far that day.
Set up the task as a race between the teams with the first team to finish getting a prize. It is best to reward all learners but the first place team should get something extra.

Puzzle 1: The code for lock number one is the shift used to decrypt this message multiplied by the age at which Julius Caesar was elected to consul
640
Puzzle 2: Lock number 2 uses a pig pen cipher. The code is the number of letters in the alphabet, multiplied by the number of grids used in the pig pen cipher **104**
Puzzle 3: NINE NINE SEVEN **997**
Puzzle 4: This is the last lock, be careful its tricky the code is nine eight three
But you need to flip the code from the scytale puzzle so answer = 389

Activity: Escape the Box

It is possible to facilitate this activity by purchasing closable containers and locks with flexible loops (as seen in the image below.) The codes can be set on the locks to suit and having smaller containers within larger ones can lead to more interesting puzzles and steps for the learners to complete.

A virtual example of this sort of puzzle can be seen at https://scratch.mit.edu/projects/423550886/



Differentiating for Learners

- For learners working towards different progression steps, the choices of ciphers can be adapted to suit.
- For learners looking to work towards higher progression steps, extensions are provided in the activities which require more problem-solving skills such as not providing the key.
- There is also opportunity to explore other ciphers not provided here such as the columnar transposition cipher, or if there is genuine interest, the Vignere Cipher and Playfair Cipher.

Where To Go Next

- This resource focuses on the historical approaches and applications of cryptographic techniques.
- This serves as an appropriate introduction into how cryptography is used in everyday life now. This would connect well with the topics of online safety and cyber security, as well as a discussion on the ethics surrounding how our personal data is handled.
- The topics of hacking can also be explored, particularly the different reasons that someone may try gaining access to information and the ethical and legal implications surrounding doing so.

technocamps

@Technocamps

Find us on Facebook