PRIMARY + STEM

Teaching Resource

ACTIVITY:

Secret codes and ciphers

ACTIVITY OVERVIEW

People have had the need to send data securely for many years. Whether it's friends passing notes in class, or the location of enemy soldiers in a battle, we want our information kept private. Today, we have encryption, passwords, and security settings on our computers to help us send important information safely. All these modern data security methods began with simple codes and ciphers.

Students will enjoy encrypting and decrypting secret messages in this activity. If you have further time available and interested students, you can easily extend this activity to include other methods of sending information, such as Morse code, semaphore or binary. Cipher keys can be directly linked to maths curriculum, by focusing on relevant operations, such as addition, subtraction, multiplication or division. Use this activity within any learning area by making the secret messages specific to your situation, (e.g. introduce spelling words, key science terms, healthy foods, characters from a class novel, or places in your local area).

SYNOPSIS

People have had the need to send data securely for many years. Whether it's friends passing notes in class, or the location of enemy soldiers in a battle, we want our information kept private. Today, we have encryption, passwords, and security settings on our computers to help us send important information safely. All these modern data security methods began with simple codes and ciphers.

Students will enjoy encrypting and decrypting secret messages in this activity. If you have further time available and interested students, you can easily extend this activity to include other methods of sending information, such as Morse code, semaphore or binary.

Cipher keys can be directly linked to maths curriculum, by focusing on relevant operations, such as addition, subtraction, multiplication or division. Use this activity within any learning area by making the secret messages specific to your situation, (e.g. introduce spelling words, key science terms, healthy foods, characters from a class novel, or places in your local area).

Foundation – Year 2

- Recognise and explore patterns in data and represent data as pictures, symbols and diagrams (VCDTDI014)
- Explore how people safely use common information systems to meet information, communication and recreation needs (VCDTCD018)

Year 3 – 4

- Recognise different types of data and explore how the same data can be represented in different ways (VCDTDI020)

Year 5 - 6

- Examine how whole numbers are used as the basis for representing all types of data in digital systems (VCDTDI027)

ACTIVITY, MATERIALS AND INSTRUCTIONS

Activity - Cipher wheel

Make a cipher wheel to share secret messages in your own classroom. Students begin with a simple shift cipher, with further cryptography challenges added for different year levels.

Materials for a class of 30 students

- Cipher wheel worksheet x 30 (may be printed on thicker card)
- Split pins x 30
- Pencils
- Paper
- Scissors

Instructions

1. Cut out cipher wheel parts from the worksheet.
2. Choose either numbers or letters to be the inner wheel. We suggest using numbers first with younger students, as this is easier to understand for beginners.
3. Poke the split pin through the centre dots on both wheels and secure at back.

Beginner level

Use the inner number wheel. Turn the wheel so that the inner number 'one' lines up with the outer letter 'a'.

To send a message saying 'dog', look for the letters on the outside wheel, then write down the corresponding letters on the inner wheel. The outer wheel is for the original message, the inner wheel is for the encrypted message.

	d	o	g
dog is encrypted to	4	15	7

	c	a	t
cat is encrypted to	3	1	20

Teacher to write a few secret words on the board, for students to decrypt. For example:

1 16 16 12 5 = apple

2 1 14 1 14 1 = banana

3 8 5 5 19 5 = cheese

Then, students to write a secret message to give to a partner.

Note – it may be helpful to print out some grid paper for students to work on (or use the grid maths exercise books). For example:

- http://www.4mation.co.uk/resources/free/graph2cm.pdf
- https://www.subjectcoach.com/blog/wp-content/uploads/2017/06/printable-graph-paper-1cm-sq-a4.jpg

Younger children may need assistance with secret words, consider putting suggested words up on the whiteboard for them to copy. Note - think about where the children are sitting in the classroom during this activity (it's hard to write a secret message to the person sitting next to you!).

Mid-level

Use the inner alphabet wheel. Turn the wheel so that the inner letter ‘c’ lines up with the outer letter ‘a’. If I want to send a message saying ‘dog,’ I look for the letters on the outside wheel, then write down the corresponding letters on the inner wheel.

dog is encrypted to	f	q	g
cat is encrypted to	e	c	v

Remember that the outside wheel is your original message. The inside wheel is the encrypted message.

This is a shift cipher, sometimes called the Caesar Shift. Julius Caesar, a Roman general who lived over 2000 years ago, used this method to send his secret messages.

The key to decrypting these messages is knowing how many letters we have shifted the alphabet wheel. In our example here, we have shifted the wheel by two letters, to match the outer ‘a’ with the inner ‘c’. So, the key to this cipher is two. The person receiving the message needs to know this key to help them decipher the original message.

Students can rotate the letter wheel and select their own shift key now (e.g. outer wheel ‘a’ lining up with inner wheel ‘m’ is a shift of 12). Caesar liked to use a key of three.

Write a secret message and pass it to a friend. Don’t forget to let them know the key (the shift number) – but don’t write it on the secret message, you will have to whisper it to them when you pass the message.

Expert level

Use the inner alphabet wheel. Turn the inner wheel to any position of your choosing.

Write a secret message sentence that tells someone about your favourite food.

Note – this time we will not let the receiver know the key for the secret message. How can we decrypt this message? We will need to look for clues in the writing.

Did the writer use their own name? Check for the right number of letters, or maybe an apostrophe.

Did the writer use the word ‘food’? Check for a four-letter word with a double letter in the middle. Did the writer use the word ‘my’? Look for two-letter words.

This might take a few attempts to get right.

For example, I have a message from Doris that says:

rd kfatzwnyj ktti nx hmthtqfyj hfpj

I am pretty sure that Doris will have used the word ‘food’ in her sentence. This must be the third word there, ktti, with the double letter in the middle.

So, I turn my cipher wheel so that the inner letter ‘k’ matches up with the outer letter ‘f’.

Remember that the inside wheel is the secret message, and the outside is the original message.

Then, I can see that those four letters do spell the word 'food'. I can decipher the secret message now, by reading the letters from the inside wheel and writing down the matching outside letters of the original message. Doris has used a shift key of five to write her message.

r	d		k	f	a	t	z	w	n	y	j		k	t	t	i	
m	y		f	a	v	o	u	r	i	t	e		f	o	o	d	

n	x		h	m	t	h	t	q	f	y	j		h	f	p	j	
i	s		c	h	o	c	o	l	a	t	e		c	a	k	e	

HOW TO USE THIS ACTIVITY WITH YOUR STUDENTS

Foundation - Year 2

When we use secret messages, we are representing data in a different way. In this cipher, we replace letters of the alphabet with numbers, to hide our message. Note - this activity relies on students being familiar with all letters of the alphabet and numbers 1 to 26. Therefore, this may not be suitable for all children in Foundation to Year two.

Extend this activity by making your own alphabet to symbol cipher and spell out some more secret messages to your friends. This activity can be conducted as a class, in small groups or individually. Give each letter of the alphabet its own symbol. Use the 2cm grid paper (see link above) to set out work clearly. Students begin by writing their names in the new code. Other options for secret messages include writing your spelling words, favourite food, a message to a family member. Remember that whoever the message is for will need to know the key to deciphering it to be able to read it.

Years 3/4

When we use secret messages, we are representing data in a different way. In this cipher, we replace letters of the alphabet with different letters, to hide our message. By providing the key to decipher the message to only the intended recipient of the message, we keep our message secret from everyone else. Sending messages using codes and ciphers is a simpler version of how computers keep our messages private when we send them over the internet.

Morse code

Morse code is another fun way to represent data (and is actually a cipher, not a code). Originally, morse code was used by tapping out long and short sounds on the telegraph (this was how we communicated over long distances, before telephones and computers).

Each letter of the alphabet has its own combination of short dots or long dashes that represent it in Morse code. Students will need a morse code chart to be able to communicate using this cipher. There are many worksheets and Morse code games available online, but here are two hands-on options you might like to use with Morse in your classroom.

Students use Morse code to send a friend their shopping list (or maybe it will be your Christmas wish list!).

Option 1 – Recorder Morse code

All students need a copy of the Morse code chart. The sending student blows long and short notes on the recorder to represent different letters of the alphabet. Perhaps the music teacher has taught the children about ta-ah and ti-ti notes.

The Morse dots can be a short ti (eighth) notes, while the dashes can be a longer ta-ah (half) notes. The receiving student/s needs a pencil and paper to record each letter.

This activity would be best conducted outdoors, as it will be noisy. Or, it could be conducted in the classroom, with students taking turns to play their recorder Morse notes, and the whole class compiling a list.

Option 2 – Torchlight Morse code

All students need a copy of the Morse code chart. This is a silent version of the above activity, with students using long and short flashes of light to represent the dots and dashes of the code.

Use light Morse in small groups, or take it in turns at the front of the classroom, as with the above activity. This version of Morse is still sometimes used by the Navy, between ships, or in emergencies.

Years 5/6

Here, we are using an example of one of the earliest secret codes that people used.

It was important for people thousands of years ago to send information securely, without everyone being able to see it.

Students can have fun playing around with the cipher wheels and changing the key to unlock the secret message.

Then use this activity to introduce the topic of binary code, the way that all our digital information is stored, sent and received.

Binary code

Binary code is the language of our digital worlds. It is the language that computers use to represent information.

Every piece of information on our digital devices is changed into the numbers zero and one. Every picture on the screen, every letter that we read, every word that we hear over an online chat - these have all been converted into zeros and ones, transferred to the place they are needed, and then converted back from the zeros and ones into the image/word/sound in front of us.

Just like we replaced the letters of the alphabet with numbers and other letters, in binary code, we can represent letters and numbers using only zeros and ones. Representing numbers in binary is a good introduction to this topic, as students will enjoy cracking the code by using simple addition.

There are some good introductory videos on binary code here, given by other primary school children:

- https://fuse.education.vic.gov.au/Resource/LandingPage?ObjectId=9c2e465d-3fe0-4311-9dd8-ba5508dad536&SearchScope=Teacher
- https://fuse.education.vic.gov.au/Resource/LandingPage?ObjectId=11bfd54b-eabf-44d5-9cdb-bc80c8610318&SearchScope=Teacher

This is a fun binary code game, teaching kids to convert numbers into, and from, binary:

- https://games.penjee.com/binary-numbers-game/

DISCUSSION SECTION AND KEY THEMES

KEY THEMES

Encryption

Encryption is the process where information is changed from the original data into a form that cannot be read by everyone. When data is encrypted, it is scrambled up into a form that can only be deciphered by its intended recipient.

Decryption is the process where you convert this scrambled secret code back into its original form.

Cryptography

Cryptography can be defined as simply as writing or solving codes but is most commonly used to refer to the practise and study of secure communication methods that are used to ensure that only intended recipients can view the information.

People who study cryptography are called cryptographers. In the past, cryptographers may have worked with pencils and papers, trying to crack codes. Now, cryptographers play a big role in building all the digital systems that we use. Cybersecurity makes up an important part of university Computer Science courses.

Codes vs. ciphers

Many people use the words code and cipher interchangeably, but they do not have the same meaning.

Codes replace a word or phrase with another word or symbol. Codes need a code book (like a dictionary) that the message recipient uses to translate the code back into the original message.

Common codes that students may be familiar with include:

- postcodes (e.g. 3149 is Mount Waverley, 3152 is Wantirna South)
- ISBN codes on books (every book has one of these codes)
- barcodes found on items for sale
- number plates on vehicles
- catalogue numbers (e.g. in book club catalogues distributed at schools)

Ciphers replace every letter of the alphabet, numbers and symbols with another letter, number, or symbol. To decipher, you need to know the rule used to create the secret message. Ciphers have become more and more complicated over time, as people have tried harder to keep information secret. Most of the time, when people talk about codes and ciphers, they are usually referring to ciphers, where each letter is replaced.

Common ciphers that students may have heard of include:

Morse code, braille, pigpen code, Caesar cipher

Algorithms

An algorithm is a set of instructions for completing a task (e.g turning room lights on or off at a certain time of the day). In the case of encryption, the algorithm is the step (or steps) that are needed to encrypt your information, and then to decrypt it. Algorithms can be simple, like shifting the letters of the alphabet on a certain number of places, or complex, like the scrambling of digital information using multiple mathematical calculations found in security software.

QUESTIONS AND ANSWERS

Does anyone still use Morse code?

Morse code was originally developed to be used with the telegraph (the tapping wire code that we used before telephones were invented to transmit voices), but these days Morse code is mostly used by radio operators. Sometimes 'light Morse' is used by the Navy to blink Morse code from ships using lights.

Occasionally we hear about Morse code being used in emergency situations involving members of the military (e.g. hostage situations, signalling for help with a broken leg on a beach).

Morse code is useful because it uses simple equipment and it doesn't transmit with an accent, like voices, so it's harder to identify the operator.

What is a 'hacker'?

The word 'hacker' is usually used to describe someone who breaks into a computer system in order to commit a crime. Hacking may involve altering software, causing damage to data or stealing secret information.

Originally the word hacker was used to describe someone highly skilled who could solve computer problems and the word 'cracker' was used for the criminals.

Sometimes the word hacker is used to describe a person who can simply change or program something. For example, kids may talk about Minecraft hacks or hacking in a game. This doesn't mean that they are committing crimes, it's just the way that they describe doing something outside the standard game programming.

Australia's most famous hacker is Julian Assange, currently imprisoned in London, and known for releasing classified military information from the USA.

What's the most commonly used password (in English)?

In Australia and the world, the most commonly used password in 2021 was '123456'.

If this is your password and you are reading this, you definitely need to change this password! Other commonly used passwords are 'password', 'password1', '123456789' and '12345'.

A security software company, Nordpass, analyses password information using a huge database of information over many countries.

Their advice for a good password is to make is complex, never reuse it and update it regularly.

If Mum's phone has a 4-digit code to unlock, how many possible combinations are there?

There are 10,000 possible 4-digit combinations using the numbers on a phone keypad (0 to 9).

We calculate this by multiplying the possible options for each of the four numbers...

10 x 10 x 10 x 10 = 10,0000

But, here are a few hints (from a 2012 study of 3.4 million 4-digit codes):

- more than 10% of 4-digit codes are '1234'
- about 20% of 4-digit codes are '1234', '0000' and '1111'
- birthday years are popular 4-digit codes
- try '2580', as it includes the numbers straight down the middle of a phone keypad

Do all codes use letters and numbers?

No, there are well-known codes that do not use letters and numbers. These include:

- Morse code (transmitted by sound – dots and dashes, short and long beeps, or by short and long blinks of a light)
- Semaphore is a code that uses flags. It was used by sailors sending messages between ships
- Pigpen cipher uses symbols which are parts of a known grid, using lines and dots

Do only spies use secret codes?

No, lots of workplaces have secret codes that only they know and use.

For example, hospitals have different coloured codes to use over their public announcement system, so that people don't get too worried but staff know what is happening.

If you hear 'code red' there's a fire, 'code blue' is a medical emergency, and 'code orange' is an evacuation.

A surf lifesaver has a particular hand signal to use when a shark has been spotted and swimmers need to be evacuated from the water. Teachers sometimes instruct students to complete a certain activity (e.g. move to the next classroom) by using a code word. Does your class have any code words?

What is end-to-end encryption?

You might have seen or used online services that tell you they are using end-to-end encryption, so that only you and the person you send the message to can read it. This means that your message is scrambled up, transmitted in this encrypted form, and only the intended recipient can unscramble it.

Messages and files are encrypted before they leave one device and are only decrypted when they reach the recipient. For example, my sister's friends and family's phones all know the special key needed to encrypt messages to my sister's phone. But only her phone has the private key needed to decrypt messages sent to her.

Can people listen to my phone calls or read my emails?

Yes, someone could be listening to your phone calls. How? A spy app could be installed on your phone, allowing someone access to your phone calls, text messages and emails. A hacker could also get access to your information through a security weakness in an existing app or software on your device. However, most types of phone hacking are not to actually listen to what you are saying, rather they are to get information on your location, or account and password details.

Are there people whose job it is to break codes and ciphers so they can read secret messages?

Yes, there are cryptographers whose job it is to break ciphers. Here we are thinking about people who are not hackers, and who are not breaking the law.

Sometimes these people, called cryptanalysts, decrypt data by breaking down ciphers and algorithms.

Usually they will be employed by the company that wants to keep the information secure, to make sure that no one from outside will be able to get access to their private information.

Governments are another big employer of cryptanalysts. Here they are working to protect national security (keeping one country's information private from others), particularly in relation to military data.

Areas that cryptanalysts are constantly testing include medical and banking records.

To become a cryptanalyst you will need to develop skills including:

- Knowledge of computer systems
- Understanding of complex mathematical theories and algorithms
- Use of multiple programming languages
- Experience with different operating systems
- Experience with security software

What machines were used for encryption before we had computers?

Encryption began with simple ciphers, like the ones we have tried out in this activity. Messages were written in coded form (ciphertext), sent out, then decrypted by someone who was given the key. Just like we had written out codes here using pencils and paper, early encryptors would have done the same, whether they were using Caesar cipher, Scytale, or any other written code.

With the invention of electricity, people were able to make more complex cipher machines, with wiring and moving rotating discs, making more complicated secret messages to protect sensitive information, particularly for military use.

The Enigma machine, invented by a German engineer, is probably the most famous cipher machine of the 20th Century.

The Enigma machine was crucial for Nazi Germany during World War 2, and once this code was able to be cracked, contributed to their defeat. Many British mathematicians worked hard during the war to decipher messages. The Enigma machine looks like a funny typewriter. Each key has scrambled wiring leading to 3 rotating discs, numbered 1 to 26.

A key press results in an electrical signal travelling down a wire, then through a particular path through metal pins connected between the rotors, leading to another wire, and then lighting up a coded letter. Each time a key is pressed the rotors move and the code shifts slightly.

The person sending the message writes down the encrypted message, then can send this over the radio without worrying about people understanding the message. Information was shared with intended recipients detailing the exact way to set up the Enigma machine to send and receive messages, as to decrypt these messages you had to have your own Enigma machine.

OUTSIDE OR SUPPLEMENTARY READING

Crypto Corner (maths website)

- https://crypto.interactive-maths.com/

Crypto Corner downloadable resources

https://crypto.interactive-maths.com/downloadable-resources.html

-

Binary code

- https://thekidshouldseethis.com/post/how-exactly-does-binary-code-work

Binary code - transmitting image activity

- https://onlypassionatecuriosity.com/binary-code-for-kids/#:~:text=At%20its%20most%20basic%2C%20binary,to%20send%20and%20receive%20information.

Another binary game

- https://games.penjee.com/binary-bonanza/

The Enigma machine explained (World Science Festival)

- https://www.youtube.com/watch?v=ASfAPOiq_eQ

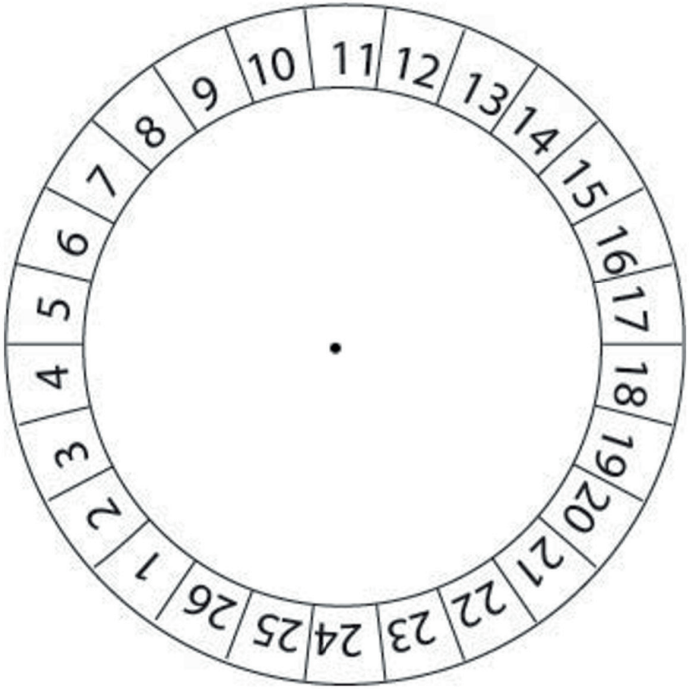
Odd Squad code breaker game

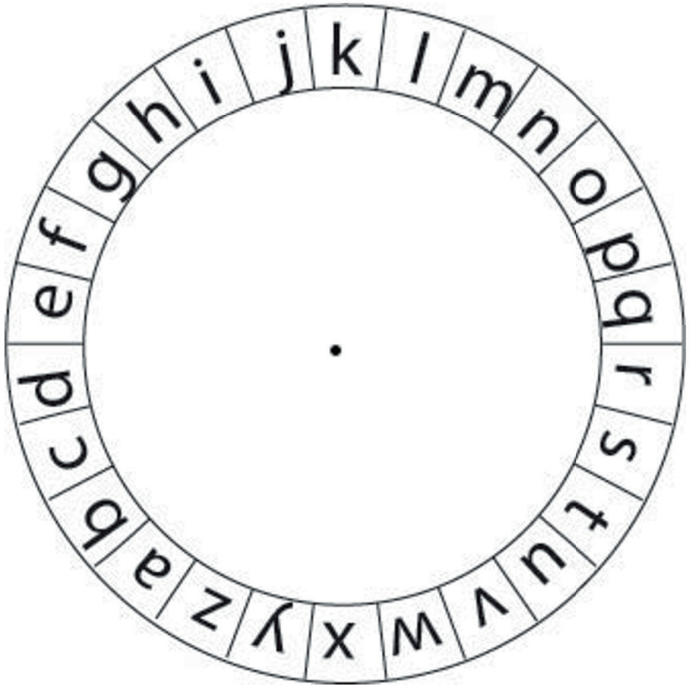
- https://pbskids.org/oddsquad/games/code-breaker

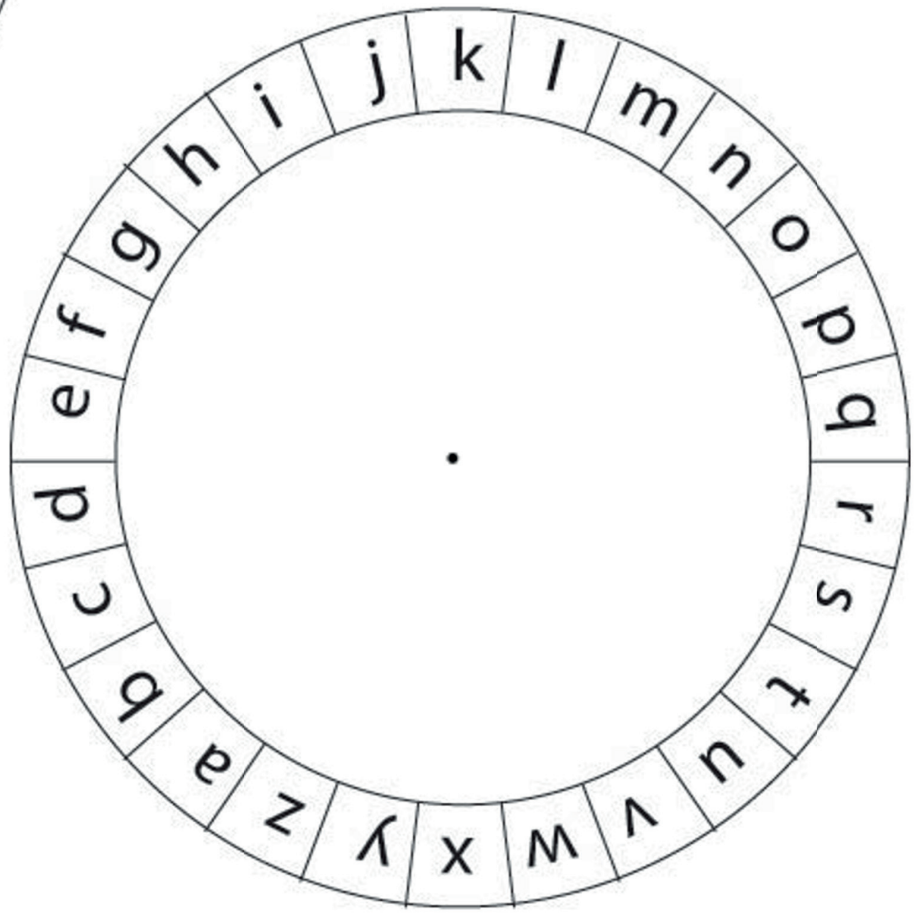
TOPIC WORDS

- code
- cipher
- cryptography
- cryptanalyst
- encrypt
- decrypt
- algorithm
- hacker

CIPHER WHEELS







PRIMARY + STEM

For more teaching resources, visit

WWW.PRIMARYANDSTEM.ONLINE

Supported by

The Invergowrie Foundation

Swinburne University

The INVERGOWRIE Foundation

SWINBURNE UNIVERSITY OF TECHNOLOGY