Tuhimuna | Cryptography

Kaiako guide

Pūkenga ā-Ipurangi Aotearoa | Cyber Skills Aotearoa

grok academy

Cyber Skills Aotearoa

Tātai Aho Rau CORE EDUCATION

Cyber Skills Aotearoa

A guide to supporting ākonga engagement

Supported by:

ASB aws bnz certnz N4L Te Kāwanatanga o Aotearoa New Zealand Government NCSC

Ngā Ihirangi | Table of Contents

He aha te Grok Academy? What is Grok Academy?
Nau mai, haere mai | Welcome
    Year Levels
    Time
How the Challenge relates to The New Zealand Curriculum
Hōtaka ako | Learning programme
    Learning intentions
    Module outline
        1. Representing Data
        2. Single Key Ciphers
        3. Frequency Analysis
    Challenge introduction for Ākonga — Why do we need to encrypt data?
    Key Vocabulary
        From Digital Technologies:
        From cybersecurity:
        Glossary
Kōwae 1: Te whakaahua raraunga | Representing data
Activity 1.1 - Binary numbers
    Preparation and timing
    Overview
Activity 1.2 - Data representation and encoding
    Preparation and timing
    Overview
    Suggested Implementation
Activity 1.3 - Data in colours
    Preparation and timing
    Suggested implementation
Kōwae 2: Waehere pūtohu | Single key ciphers
Activity 2.1 - The Caesar Cipher
    Preparation and timing
    Overview
Activity 2.2 - Problem decomposition
    Preparation and timing
    Overview
Kōwae 3: Tātaritanga auau | Frequency analysis
Activity 3.1 - Frequency analysis
    Preparation and timing
    Overview
Activity 3.2 - The Vigenère cipher
    Preparation and timing
    Overview
Activity 3.3 - Cryptography in the modern world

He aha te Grok Academy? What is Grok Academy?

Grok Academy provides resources, online courses and competitions, teacher workshops, curriculum guidance and online cyber security advice for all future-focused kaiako.

Our Mission

At Grok Academy, our mission is to educate all learners in transformative computing skills, knowledge and dispositions, empowering them to meet the challenges and seize the opportunities of the future.

To us, computing encompasses basic digital literacy through to advanced computer science and related disciplines, and the application of these skills across all disciplines.

Our Goal

We believe that a solid computer science understanding is vital whether you want to fight climate change, make the next blockbuster movie or unlock the secrets of the universe.

We've taught thousands of ākonga to program in classrooms, lecture halls and online, and are now bringing top-notch STEM education into classrooms and homes around the world.

Partner Acknowledgements

Cyber Skills Aotearoa has been developed by Grok Academy in partnership with Tātai Aho Rau - Core Education, AWS, ASB, BNZ, CERT NZ, The National Cyber Security Centre (NCSC), and Te Kāwanatanga o Aotearoa | the New Zealand Government.

Nau mai, haere mai | Welcome

This guide supports kaiako to create an effective learning programme based on the Cyber Skills Aotearoa Yr 9–13 Cryptography Challenge.

We hope this guide will build your confidence as you support your ākonga to get the most out of the challenge, and that their motivation and engagement grows alongside their understanding of cybersecurity.

If you have any feedback or questions about Cyber Skills Aotearoa, please email us at: help@grokacademy.org

Overview

This Challenge introduces data representation and basic cryptography concepts, and how they relate to securing online communication. It teaches classic cryptographic ciphers like rotation, XOR and mixed-substitution, and explains the techniques used to break these forms of encryption. The challenge also explores how cryptography can be used to hide messages in images and sound.

In this Challenge, students begin with data representation and are taken on a scaffolded journey through different types of ciphers, how they can work for encryption and decryption, and explore algorithmic techniques necessary to design them.

It is important to note that the key objective is to help students understand data representation, different ways to secure data before transmission, and different ways to encrypt and decrypt messages. The Challenge does not assume any prior programming experience.

The three modules of this challenge are:

1. Representing Data
2. Single Key Ciphers
3. Frequency Analysis

The learning materials in each module include notes, guided experimentation, quizzes, unplugged activities and problems to test understanding and skills.

The video resources are designed to teach ākonga about specific encryption concepts. They also give them a glimpse of what working in cyber security is like, and what people working in this field do daily.

The people in the videos are all employees of the organisations they represent and work in a variety of cyber security roles.

Year Levels

This challenge is suitable for students in Years 9–10 as an introduction to data representation and algorithms. For students who are learning Python, the content provides examples of how encryption algorithms can be implemented in a programming language. The content supports learning toward the encryption external assessment topic at Level 2 NCEA.

Programming

Problems do not require programming because they focus instead on cryptographic concepts and algorithms. However, examples of how various concepts could be implemented in the Python programming language are included for ākonga and kaiako who wish to explore this further. This course could be used to complement one of the available Python programming courses within the Grok platform.

Time

The Challenge is designed to be completed over 6–8 hours depending on class discussions and the use of additional activities suggested within this guide.

How the Challenge relates to The New Zealand Curriculum

The Challenge has close ties to the Technology learning area. The Technology learning area is about the interrelationship between people, technology, and the environment, and understanding 'intervention by design'.

With its focus on design thinking, technology education supports students to be innovative, reflective and critical in designing new models, products, software, systems and tools to benefit people while taking account of their impact on cultural, ethical, environmental and economic conditions.

> ***The aim is for students to develop broad technological knowledge, practices and dispositions that will equip them to participate in society as informed citizens and provide a platform for technology-related careers***. Technology in the New Zealand Curriculum (2017)

Technology Learning Area

Digital Technologies (NZC)

Computational Thinking for Digital Technologies and Designing and Developing Digital Outcomes focus on developing students' capability to create unique digital outcomes for specific needs and purposes. These two areas also significantly contribute to the knowledge and skills students need as digital citizens and as users of digital technologies across the curriculum. They also provide opportunities to further develop their key competencies:

- Thinking
- Using language, symbols, and texts
- Managing self
- Relating to others
- Participating and contributing

- Computational Thinking for Digital Technologies (CTDT) – ākonga will develop an **understanding of computer science principles that underlie all digital technologies**. They'll learn core programming concepts so that they can become creators of digital technology, not just users.

- Designing and Developing Digital Outcomes (DDDO) – ākonga will develop an understanding that digital applications and systems are **created for humans by humans, with a focus on designing and producing quality, fit-for-purpose, digital outcomes**. They develop their understanding of the technologies people need in order to locate, analyse, evaluate and present digital information efficiently, effectively and ethically.

Nature of Technology (NZC)

There are also many connections to the Nature of Technology strand and the learning outcomes that explore the relationship between humans and technology at each year level.

> The nature of technology strand guides teachers to develop learning activities that support students to question why the world around them is the way it is. They develop perspectives and become aware of the relationship between people as users and designers/creators of technology and how that technology in turn impacts on more people, the environment, and on culture.
>
> They learn to critique the impact of technology on societies and the environment and to explore how developments and outcomes are valued by different peoples in different times. Students have opportunities to increase their understanding of the complex moral and ethical aspects that surround technology and technological developments. They ask big questions such as "if it can be done, should it be done?" Nature of technology | Technology TKI
>
> In Characteristics of Technology (CoT) technology is defined as "purposeful intervention by design", and technological practice as the activity through which technological outcomes are created and have impact in the world. Technological outcomes are designed to enhance the capabilities of people and expand human possibilities. They change the made world in ways that have positive and/or negative impacts on the social and natural world. Characteristics of technology | Technology TKI

This course provides an opportunity for students to explore computer science and programming concepts. The content will provide a broad view of advanced topics and support their development of technological literacy.

The introduction of essential concepts of data representation and algorithms aligns with **CTDT Progress Outcomes 3, 4, and 5**, while more complex concepts such as conventions, encryption, cybersecurity, and data mechanisms align with CTDT Progress Outcomes 7 and 8. In particular, the Cryptography Challenge is related to:

Designing and Developing Digital Technologies Progress Outcome 3 (DDDO PO3)

> In authentic contexts, ākonga follow a defined process to design, develop, store, test and evaluate digital content to address given contexts or issues, taking into account immediate social, ethical and end-user considerations.
>
> Ākonga understand the role of operating systems in **managing digital devices, security,** and application software and are able to apply file management conventions using a range of storage devices. **They understand that with storing data comes responsibility for ensuring security and privacy**.

Computational Thinking for Digital Technologies Progress Outcome 3 (CTDT PO3)

> In authentic contexts and taking account of end-users, ākonga **decompose problems into step-by-step instructions to create algorithms** for computer programs. They use logical thinking to predict the behaviour of the programs, and they understand that there can be more than one algorithm for the same problem. They develop and debug simple programs that use inputs, outputs, sequence and iteration (repeating part of the algorithm with a loop). **They understand that digital devices store data using just two states represented by binary digits (bits).**

Computational Thinking for Digital Technologies Progress Outcome 5 (CTDT PO5)

> In authentic contexts and taking account of end-users, ākonga independently **decompose problems into algorithms**. They use these algorithms to create programs with inputs, outputs, sequence, selection using comparative and logical operators and variables of different data types, and iteration. They determine when to use different types of control structures.
>
> Students document their programs, using an organised approach for testing and debugging. They understand **how computers store more complex types of data using binary digits**, and they develop programs considering human-computer interaction (HCI) heuristics.

Computational Thinking for Digital Technologies Progress Outcome 7 (CTDT PO7)

> In authentic contexts and taking account of end-users, ākonga analyse concepts in digital technologies (for example, information systems, **encryption,** computer security, error control, complexity and tractability, autonomous control) by explaining the relevant mechanisms that underpin them, **how they are used in real world applications, and the key problems or issues related to them.**

Content alignment to NCEA

The course content could contribute to students' understanding of the following standards in particular:

1.3 AS92006 Demonstrate understanding of usability in human-computer interfaces.

Students can explore how cryptography and MFA contribute to secure and usable login systems, impacting the user experience.

2.9 AS91898 Demonstrate understanding of a computer science concept.

The course content could particularly contribute to this standard as students develop understanding of the concept of cryptography, how it has been or could be applied, and the relevant mechanisms that shape the concept.

Hōtaka ako | Learning programme

Learning intentions

After completing the Challenge, ākonga will be able to:

- Explain how text and image data are represented in digital systems.
- Recognise that breaking down a problem into smaller steps (decomposing) makes it easier to solve problems.
- Recognise that steps in algorithms need to be accurate and precise.
- Recognise that an encrypted message is only as secure as its key.
- Recognise that an encrypted message is only as secure as its key.
- Appreciate that cyber security is an evolving field, with the quest to create ever more secure methods of data encryption.
- Understand that cryptographic algorithms are applied when data is transferred between devices during the authentication processes in MFA.
- Explore career opportunities available in cyber security and related fields.

Module outline

The Cryptography Challenge consists of three modules:

1. Representing Data

   This module introduces the concept of data representation, and that all data is stored as numbers. Ākonga explore a range of functions (ord(), chr(), input()) in order to be able to represent and process characters and numbers. The module also demonstrates how messages can be hidden within image files (using steganography) and sound files (using spectrograms).

2. Single Key Ciphers

   This module introduces ākonga to cryptographic keys: specifically rotation ciphers. The module goes through the process of encryption and decryption and the underpinning algorithms. It addresses the ease with which these ciphers can be cracked using a brute force algorithm.

3. Frequency Analysis

   This module introduces ākonga to a mixed alphabet substitution cipher as a technique that can't be broken with the previously written brute force algorithm. The technique of frequency analysis using most frequent words and letters is explored as a means to decrypt messages without a key. Ākonga explore the Vigenère cipher as an example of a more complex (poly-alphabetic) substitution cipher. The XOR method of encryption is introduced, where two bits of data are compared to each other and they learn to encrypt and decrypt using XOR. Lastly, ākonga look at applications of cryptography in today's world.

Types of component:

 Discussion

 Worksheet

 Computer-based Activity

 Group Activity

 Unplugged Activity

 Video

 Read

 Animation

 Reflection

 Game

 App

Challenge introduction for Ākonga — Why do we need to encrypt data?

People have been hiding messages for many centuries. Given so much of our lives are online, there is an increasing need to improve how systems secure our data for both storage and transmission.

One of the principles of modern organisational cyber security is to build multiple layers of defence, so that even if one layer is breached, there are subsequent layers of protection that safeguard the data. These layers of defence not only include system security (such as strong passwords and 2FA), but also physical security (controlling access to buildings, physical computing resources etc).

One such layer of system security is the encryption method (or algorithm) used on the data itself, and the security of the key (or code) used to encrypt it.

The process of translating raw data (or plaintext) into a secret code is called *encryption*. The process of translating encrypted data back into its original text is called *decryption*.

Hackers use patterns in data to force their way into systems or find loopholes in the many layers of protection. Analysing the patterns of data to find the key (thus breaking the cipher) is a commonly used method of hacking. As more complex keys are used, manually breaking ciphers can be both problematic and time-consuming. The skill of programming allows us to automate the process of applying different, prospective keys to an encrypted message. The same skills can also help us decrypt a long message with a known key.

Programming a computer means giving it instructions - a sequence of steps - to follow in a way that it “understands”. Although ākonga do not learn programming directly in this course, they do explore problem decomposition and write algorithms for organising step-by-step instructions for someone else to follow in order to solve a problem of encrypting and decrypting data.

The ciphers we explore in this Challenge are introductory, but these same principles are used in the cyber security industry and by hackers.

Key Vocabulary

From Digital Technologies:

Algorithm: A set of rules or step-by-step instructions to solve a problem or achieve an objective. A recipe is an example of an algorithm because it sets out what you need and the steps you follow to combine everything to create a dish.

Decomposition: breaking down a problem into smaller parts which can then be dealt with individually. This allows very complicated problems to be solved by first solving their individual parts separately and then working out how those individual solutions can be used together.

Binary: In computing, a means of representing all data using just two values. Often through the process of converting a numeric value into its binary equivalent using only 0s and 1s.

From cybersecurity:

Encoding: The process of converting data into a format required for processing with a computer. Decoding is the reverse - converting that data back into a human-readable form.

Steganography: A technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection. The Challenge uses the example of hiding secret data inside an image.

Cryptography: A way of protecting information and communications by applying an algorithm and secret code (or key) such that only those for whom the data is intended (and who have the key) can read or process it.

XOR: A logical operation performed on two bits of data that outputs False (or 0) if they are the same and True (or 1) if they are different.

Multi-factor authentication (MFA): is an authentication method that requires the user to provide two or more verification factors to gain access to an account.

Glossary

Please click here for a glossary of Grok technical words translated into te reo Māori.

Kōwae 1: Te whakaahua raraunga | Representing data

Activity 1.1 - Binary numbers

Preparation and timing

This activity can be completed at any time, no prior knowledge is needed except some numeracy and counting skills.

Overview

- What are binary numbers?
- How do they work?
- What is the relationship between binary numbers and the number 97 used to represent ‘a’?

 Unplugged Activity 1

This unplugged activity can be completed as individuals or in groups. It enables students to see the relationship between decimal and binary numbers.

Codes for letters using binary representation - CS Unplugged

Extension activity:

- What is the maximum integer value that can be represented in 3 bits? 4 bits? 7 bits? 8 bits?
- What is the significance of the 255 (as in the max value of a channel in an image), in terms of its relationship to the number of bits?

 Unplugged Activity 2

Computational thinking for digital technologies: NZ Curriculum

Coded messages

 Unplugged Activity 3

Students represent their date of birth as binary numbers. This requires them to understand how to convert between decimal and binary numbers.

Extension activity:

- Students explore the rule / pattern / algorithm to convert a decimal number into a binary number. To test their understanding, they can convert a larger number (such as their student number or the population of their school or town) into a binary number.

 Game

The following game is designed to test if students can convert between decimal and binary. It allows for differentiation in the classroom, and is suitable for older students who may already be familiar with binary numbers.

Binary Game v2 - App Lab - Code.org

Activity 1.2 - Data representation and encoding

Preparation and timing

No prior knowledge is required for this activity.

It can be done at the beginning of a lesson or the unit. This activity would be best delivered as an introduction to Module 1 - Representing Data.

Overview

- What is data encoding?
- What is the difference between data and information?
- Why do computers use numbers to represent data?

Suggested Implementation

Encoding and decoding are important concepts to understand, both in digital technologies and cryptography. They allow characters, images and sound to be represented as numbers, which is the format needed by computers for processing. Without a common method of encoding, computers would not be able to communicate with each other.

Video

Representing numbers and text digitally

Watch this video, What is ASCII? | YouTube, published by Bitmerge: What is ASCII?

The video demonstrates the concept of characters represented by numbers and introduces the terms ASCII and Unicode. ASCII as a subset of Unicode, the relationship between uppercase and lowercase letters, and the need for a common data encoding system are also discussed.

Discussion

What might be the consequences if we didn't have a common method of encoding?

Everything we type, listen to and watch on computers is ultimately represented as numbers. Other computing devices (such as gaming consoles) work on exactly the same principle. The controls on joysticks etc. also represent data as numbers.

Discussion

What do you think might happen if every computer had its own way of encoding? Say my computer thought "A" was 97, but another computer manufacturer decided that "A" was represented by 200. Or my game controller sent an "accelerate" command as a 300, and another game controller's 300 was the equivalent of a stop. What could be the impacts or consequences of these inconsistencies?

Answers to the above might include:

- Computers may not be able to understand each other.
- We could not play multiplayer games.
- If I send a message to someone whose phone is from a different company, the message could look different to what I wanted to send.
- People could not do online shopping, or banking or other examples of online and digital interactions.

Discussion

What are some other conventions we use around the world to communicate?

Throughout the 'Conventions' section in Module 1, the following discussion question can be posed.

The slide gives the example of stop signs around the world to show how conventions determine how we communicate and understand each other. What might be some other examples of conventions used in communication?

Answers to the above might include verbal or non-verbal signs:

- A wave with the hand to signal a greeting (hello/goodbye)
- Facial expressions

Reflection

Group Activity

We use conventions all the time, and computers need encoding conventions to ensure data can be interpreted in a consistent manner.

Students might share examples of situations where conventions haven't been understood, for example:

- If they went to a country where they were unfamiliar with the language.
- If someone spoke to them in a language they didn't understand.
- If a sign/symbol was unfamiliar or ambiguous.
- If a text message came through with upside down question marks or some other indication that some of the message was lost.

Data encoding is a fundamental concept in cryptography. By understanding *how* data is represented, we can begin to imagine how we might be able to *manipulate* this encoding! This can be the teaser for the next lesson/activity.

Unplugged Activity

Group Activity

Designing, developing and implementing a sign-language convention.

Note: The Module 1 slide Teacher's notes for "The need for conventions" explicitly asks students to perform this task and provides a choice of two contexts: a deep sea diver or astronaut.

Students are asked to make a simple sign language convention in groups of 2-4:

1. Create up to 10 hand gestures.
2. Map each hand gesture to a word or phrase. Remember, you all have to agree!
3. Have a conversation using your hand gestures. No talking allowed!
4. Discuss and refine your sign language convention.

Ask students questions to guide them:

- What is the purpose of the language?
- Who is the audience?
- How do you ensure instructions are consistent and understood by all?

Activity 1.3 - Data in colours

Preparation and timing

No prior knowledge is required for this activity.

This activity would be best delivered prior to, or in conjunction with the 'Hiding messages in images' section in Module 1.

Overview

- How do computers store colour data?

Suggested implementation

Modern computing devices represent millions of colours, and a common way to represent colours is using RGB channels. Each channel has a value ranging from 0 to 255, and combined with the values from the other channels to result in a display colour.

Although there are other forms of encoding colour data (such as CMYK), this Challenge primarily looks at RGB channels.

The following links can be used to show students how the values in each of the 3 channels can be set, and when combined form a display colour.

- RGB Colour mixer - CS Field Guide

Suggested activity:

- How can shades of grey be made with RGB?
- Develop a colour palette of 4/6 colours for a social media header / blog / instagram page. Students are to create a table with the colours in one column, and the corresponding RGB values in another column.
- What might be some general observations about channel values and the colour displayed?
    - Answers might include:
        - The higher the number, the lighter the colour displayed in the channel.
        - The lower the number, the darker the colour displayed in the channel.
        - When the values for r, b, g are equal, the result is a neutral colour.

You may also visualise the computer's representation of images using Pixel Viewer - Computer Science Field Guide

Computer-based Activity

Students may be interested in further exploring the idea of separating and combining colour channels. This can be achieved using photo editing software such as CorelDraw, Photoshop, or the PineTools website: RGB channels online

Students may open/upload an image of their choice (suitable images can be found on Pixabay).

To split the image into separate channels on the free PineTools website, upload the image and check/uncheck the colour channels and select 'Decompose'.

How to split the image into separate channels in Photoshop.

How to split the image into separate channels in CorelDraw.

Discussion

How many colours can be represented in total if each colour has a range from 0 to 255?

This discussion is designed to get students thinking about the range of values available, and the combinations of the 3 channels.

Students may initially have difficulty with the concept, so a suggested scaffold would be to get them to imagine they had 2 channels, each with only 3 possible values (instead of 255). The following table provides a way to imagine this hypothetical scenario:

CHANNEL 1	CHANNEL 2
A1	B1
A2	B2
A3	B3

Working this out to find all the possibilities gives us the following values:

A1 B1	A1 B2	A1 B3
A2 B1	A2 B2	A2 B3
A3 B1	A3 B2	A3 B3

As the total number of possibilities is 9, it can be deduced that:
*total colours = number of colours in channel 1 * number of colours in channel 2*

Expanding this rule to 3 channels with 256 colours each (0-255 gives us 256 colours) results in:
Total colours = 256 * 256 * 256
= 16777216 (ie over 16 million colours!)

Reflection

RGB encoding allows us to use numbers to represent colours. This also allows us to communicate colour values easily to each other.

Students might share examples of situations where colour values need to be communicated, for example:

- Between a UX designer and a programmer.
- Between a client who wants a certain colour and the web developer / graphic designer.
- Between teams to ensure consistency in the work produced.

More resources to explore colours and their digital representation:

Computational thinking for digital technologies: NZ Curriculum

- Exemplar 14: 24-bit colour calculations

Computer-based Activity

Representing sound digitally.

Audacity is an easy-to-use, multi-track audio editor and recorder. Allow students to explore the program. The software can be freely downloaded: https://www.audacityteam.org/download/.
If you would like to extend this topic https://www.sciencebuddies.org/blog/sound-science-lessons provides STEM lessons focused around understanding how sound works.

Computer-based Activity (Extension)

For more information and activities on data representation (suitable for high school students) see the following online resource from the Computer Science Education Resource Group at the University of Canterbury:

Data Representation - Computer Science Field Guide

Kōwae 2: Ngā waehere pūtohu kī takitahi | Single key ciphers

Activity 2.1 - The Caesar Cipher

Preparation and timing

It is assumed that students have completed Module 1 (Data Representation).

This activity would be best delivered prior to, or in conjunction with Module 2 (Single Key Ciphers).

Overview

- How does the Caesar Cipher work?

Unplugged Activity

This resource was developed by the Grok Academy and explores the ideas in the Caesar Cipher using a series of unplugged activities.

https://groklearning.com/a/resources/cryptography-cipher-wheels/

Computer-based Activity

The interactive resource within the Challenge can be used by students to see how the Caesar Cipher works with different shift values:

https://groklearning.com/learn/cyber-nz-eng-crypto/crypto/4/

Some possible messages that students can try to encrypt with different shift values:

- their names
- their favourite food
- a sentence from their favourite book/movie.

Discussion

How might some of the programming concepts that we learnt in Module 1 be useful to create a Caesar Cipher in code?

Answers to the above might include:

- We can use input() to get the value we want to shift by (the key), and the message we want to encrypt.
- ord() and chr() can be used to get the underlying number representation for each letter in the original message.
- Print() can be used to display the encrypted message after it has been shifted.

Discussion

Why is using programming and the ord() and chr() functions not so straightforward using the te reo Māori alphabet?

You may like to discuss the following points:

Using the English alphabet, a program can use the logic that if we add the value of the key to the ASCII value of each letter we can work out the new letter. This works because in English each letter in the alphabet is numerically one number bigger than the one before on the ASCII table. Look at the table below.

a	b	c	d	e	f	g	h	i	j	k	l	m
97	98	99	100	101	102	103	104	105	106	107	108	109

n	o	p	q	r	s	t	u	v	w	x	y	z
110	111	112	113	114	115	116	117	118	119	120	121	122

The English alphabet and ASCII

When it comes to the **te reo Māori alphabet** things are a little bit different. Let's look at the pattern of letters and ASCII values in the te reo Māori alphabet.

a	ā	e	ē	h	i	ī	k	m	n
97	257	101	275	104	105	299	107	109	110

o	ō	p	r	t	u	ū	w	ng	wh
111	333	112	114	116	117	363	119		

The te reo Māori alphabet and ASCII

As you can see the numbers are not consecutive and therefore the logic of adding the value of the key to the ASCII value of the letter to obtain the new letter does not work. If the students are familiar with arrays or lists, you can discuss how a rotation cipher can work by shifting the letters using an index value.

Discussion

What are the benefits of creating a Caesar Cipher through code?

Answers to the above might include:

- Creating a cipher through code means that the shift can be applied to very long messages much faster than it can be done manually.
- Using a paper cipher wheel may not result in accurate encryption, as the inner/outer wheel may move slightly or may not be perfectly aligned. This might mean that the shift is not *consistently* applied throughout the message, making it harder/impossible to decrypt.

Activity 2.2 - Problem decomposition

Preparation and timing

It is assumed that students have completed Module 1 (Data Representation). This activity would be best delivered prior to, or in conjunction with Module 2 (Single Key Ciphers).

Overview

- How do we decompose a problem and write algorithms to solve it?

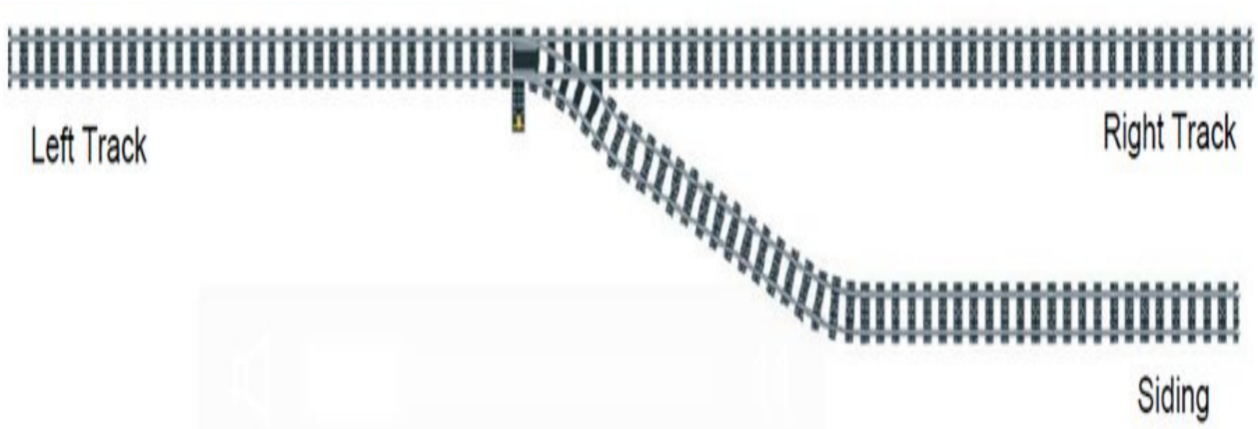
Unplugged Activity

This resource is designed to teach students how to solve problems computationally. The following resource was adapted from Richard Cox's 2015 seminar on how to introduce students to algorithms. There is a big developmental jump between intuitively solving a problem and prescribing the rules and steps that allow any person or machine to follow a set of instructions to replicate the process.

The more complex the problem, the harder this process becomes, so start with simple tasks. Small group work is an effective approach as it forces students to explain their reasoning.

Train Shuffle Task

Track needs to be enlarged to A3, or alternatively, students can draw the track on butcher's paper.



Carriages

Cut out the carriages and place them on the track.

Place carriages on the **Left Track** in “Start” position
TASK 1 - Start: A B, C
TASK 2 - Start: A, B, C, D, E, F

Move carriages to the **Right Track** in “Finish” position using only the allowable moves
TASK 1 - Finish: C, B, A
TASK 2 - Finish: Reverse order.

Only three moves are allowed.

One or more carriages can be moved from:

- left track to right track
- left track to siding
- siding to left track.

STEPS

1. Ask students to solve the train task problem.
2. Ask students to write down step-by-step instructions so that someone else (or a computer) can solve the problem.
3. Students give their instructions to another group and ask them to follow them **exactly.**
4. Reflection: Were your instructions clear, precise, correct?
5. Make changes to your instructions if needed (repeat steps 3-4 until correct).

Note: You can create many variations of this activity by changing the start and finish carriage configurations.

The steps could be used to teach computational thinking and algorithm creation using a range of problems. However, it is advisable to start with small problems and slowly build up the complexity.

Kōwae 3: Tātaritanga auau | Frequency analysis

Activity 3.1 - Frequency analysis

Preparation and timing

It is assumed that students have completed Module 1 (Data Representation) and Module 2 (Rotation Ciphers). The following unplugged activities have been designed to allow for differentiation in the classroom.

This concept is explored as the basis for Module 3 - Frequency Analysis.

Overview

- How does frequency analysis work?
- How can we use this technique to decrypt text encrypted with a mixed substitution cipher?

Unplugged Activity 1

The following website contains the top baby names (in English and te reo Māori)

Top Baby Names in New Zealand

Using the following table (either manually or using word processing / spreadsheet software), students are to keep a tally of the number of times a letter appears in the top baby names for a given year.

Letter	*Tally (how many times it is in names on the list)*

They can compare various years to see if the frequency is similar.

The number of times a certain letter appears on the list is the *frequency*. A similar technique is used in letter frequency analysis, by analysing very large volumes of texts and keeping a tally, and converting this into a percentage for each letter. This is an important technique for breaking cryptographic ciphers.

Unplugged Activity 2

The tables provided in Module 3 show the most commonly used letters in the English and te reo Māori languages.

The frequency of letters in any language is utterly dependent on the syntax and grammatical structure of that language.

Students who learn another language or speak a language other than English or te reo Māori can explore what the letter frequencies are in their chosen language, and compare the vowels/consonant frequencies in other languages.

https://en.wikipedia.org/wiki/Letter_frequency#Relative_frequencies_of_letters_in_other_languages

Discussion

The greater the volume of text to decrypt, the more useful letter frequency analysis is. True or False?

The most frequent letters in English (ETAOINSHRD) and te reo Māori (AITKUHREON) have been detected by analysing thousands of pieces of published texts.

If a smaller piece of text is analysed against frequency analysis e.g. the single word 'hello', the letter frequencies in this word will not correspond to the most frequent letters ETAOIN. Therefore, 'hello' encrypted using mixed alphabet substitution that gives us 'pzbbi' cannot be easily decrypted using most frequent letters.

In the discussion, students may attempt to articulate the relationship between the volume of encrypted text and the usefulness of frequency analysis. An interesting way to explore this further is to use the Frequency Analysis Tool used in Module 3, to type/paste in increasingly larger volumes of text (say from a textbook or novel), and observe that the larger the amount of text, the closer the letter frequencies resemble ETAOINSHRD/AITKUHREON.

Wordle and its derivatives are popular online games. How do people use letter frequency to help them play these games?

Activity 3.2 - The Vigenère cipher

The Vigenère cipher is an example of a polyalphabetic substitution, but instead of a simple substitution or shift, it uses a word as a key.

Preparation and timing

It is assumed that students have completed Module 1 (Data Representation), Module 2 (Rotation Ciphers) and have understood frequency analysis and polyalphabetic substitution in Module 3 (Frequency Analysis). This cipher is explored in the Challenge section Frequency analysis can also be beaten.

Overview

- How does the Vigenere cipher work?

Use the worksheet on the next two pages to demonstrate the Vigenère cipher in action. Students have been given an example and can use this method to encrypt the remaining letters of the plaintext with the key. They should come up with the following solution.
ENGLISH

Plaintext	C	I	P	H	E	R
Key	T	U	R	I	N	G
Result	*V*	*C*	*G*	*P*	*R*	*X*

Students can try encrypting a few other pieces of plaintext with a key (either set by the teacher or of the student's choosing). It is important to emphasise that the word length of the plaintext and the key should be the same.

Discussion

What might be some techniques that could be helpful to break the Vigenère cipher?

Some answers might include:

- Looking for patterns again: if the plaintext and the key are the same length, we can look for similar looking letter patterns in the encrypted text that can help us discover most common words
- If the keyword contains 3 letters, then every plaintext letter can be encrypted in 3 different ways
- Repetitions in the ciphertext can be identified, which could identify repetitions in the plaintext

Unplugged Activity

The following table shows each of the 26 letters of the alphabet progressively shifted by 1. This is commonly known as the Vigenère tableau or table, and can be used to help understand the Vigenère cipher to encrypt the plaintext “CIPHER” with the key “TURING”.

Look at the first letter of the plaintext (C) in the horizontal column and the key (T) in the vertical column. The columns intersect at ‘V’ which is the result of the encryption.

Use this method to encrypt the remaining letters of the plaintext with the key.

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

Plaintext	C	I	P	H	E	R
Key	T	U	R	I	N	G
Result	*V*					

Unplugged Activity

Kei te tūtohi o raro ngā pū 20 o te arapū i nekehia ki te 1. E mōhiotia whānuitia ana tenei ko te tūtohi Vigenère, ka whakamahia tēnei kia mārama ai ki te tuhioro Vigenère hei whakamuna i te kuputuhi tōkau “TUHIORO” ki te kī “MARUTAU”.

Tirohia te pū tuatahi o te kuputuhi tōkau (T) i te tīwae huapae me te kī (M) i te tīwae poutū. Ka whakawhitia ngā tīwae e rua ki te pū 'Ē', arā ko te hua o te whakamuna. Whakamahia tēnei tikanga hei wetemuna i ngā pū o te kuputuhi tōkau e toe ana ki te kī.

	A	Ā	E	Ē	H	I	Ī	K	M	N	NG	O	Ō	P	R	T	U	Ū	W	WH
A	A	Ā	E	Ē	H	I	Ī	K	M	N	NG	O	Ō	P	R	T	U	Ū	W	WH
Ā	Ā	E	Ē	H	I	Ī	K	M	N	NG	O	Ō	P	R	T	U	Ū	W	WH	A
E	E	Ē	H	I	Ī	K	M	N	NG	O	Ō	P	R	T	U	Ū	W	WH	A	Ā
Ē	Ē	H	I	Ī	K	M	N	NG	O	Ō	P	R	T	U	Ū	W	WH	A	Ā	E
H	H	I	Ī	K	M	N	NG	O	Ō	P	R	T	U	Ū	W	WH	A	Ā	E	Ē
I	I	Ī	K	M	N	NG	O	Ō	P	R	T	U	Ū	W	WH	A	Ā	E	Ē	H
Ī	Ī	K	M	N	NG	O	Ō	P	R	T	U	Ū	W	WH	A	Ā	E	Ē	H	I
K	K	M	N	NG	O	Ō	P	R	T	U	Ū	W	WH	A	Ā	E	Ē	H	I	Ī
M	M	N	NG	O	Ō	P	R	T	U	Ū	W	WH	A	Ā	E	Ē	H	I	Ī	K
N	N	NG	O	Ō	P	R	T	U	Ū	W	WH	A	Ā	E	Ē	H	I	Ī	K	M
NG	NG	O	Ō	P	R	T	U	Ū	W	WH	A	Ā	E	Ē	H	I	Ī	K	M	N
O	O	Ō	P	R	T	U	Ū	W	WH	A	Ā	E	Ē	H	I	Ī	K	M	N	NG
Ō	Ō	P	R	T	U	Ū	W	WH	A	Ā	E	Ē	H	I	Ī	K	M	N	NG	O
P	P	R	T	U	Ū	W	WH	A	Ā	E	Ē	H	I	Ī	K	M	N	NG	O	Ō
R	R	T	U	Ū	W	WH	A	Ā	E	Ē	H	I	Ī	K	M	N	NG	O	Ō	P
T	T	U	Ū	W	WH	A	Ā	E	Ē	H	I	Ī	K	M	N	NG	O	Ō	P	R
U	U	Ū	W	WH	A	Ā	E	Ē	H	I	Ī	K	M	N	NG	O	Ō	P	R	T
Ū	Ū	W	WH	A	Ā	E	Ē	H	I	Ī	K	M	N	NG	O	Ō	P	R	T	U
W	W	WH	A	Ā	E	Ē	H	I	Ī	K	M	N	NG	O	Ō	P	R	T	U	Ū
WH	WH	A	Ā	E	Ē	H	I	Ī	K	M	N	NG	O	Ō	P	R	T	U	Ū	W

Kuputuhi tōkau	T	U	H	I	O	R	O
Kī	M	A	R	U	T	A	U
Kuputuhi waehere pūtohu	*Ē*						

Activity 3.3 - Cryptography in the modern world

What are some techniques used to hide our data from unwanted eyes? The following activities explore some of the techniques used to transmit information securely.

Unplugged Activity

https://classic.csunplugged.org/activities/information-hiding/

Many of the slides and problems include “Teacher Notes” that verified teachers can access. These provide additional information, suggestions and activities for teaching each concept and exploring ideas further with students in class.