Sending secret messages with cryptography

An activity by the Australian Computing Academy

Activity overview

What's it all about?

The activity uses "ciphers" to encode and decode "secret" messages.

By following a simple sequence of steps (an *algorithm*) students can encode and decode different texts.

It allows students to explore concepts of collecting, managing and analysing data, investigating and defining problems and collaboration. It can also be used as a platform for discussing the role of cryptography and information communication technologies in the community.

It is accessible to students of all ages, and ties in nicely with the Digital Technologies subject in the Australian Curriculum.

Resources needed

Preparing for the activity

The activity doesn't require computers - almost everything you needed is included in this presentation and linked resources.

Students will need copies of the necessary worksheets, and you can guide them through the activity using the slides in the relevant section of this presentation.

In addition you will need:

- Scissors
- Butterfly pins

Extension activities and alternative suggestions are included at the end of this presentation.

Introducing the topic

What do the kids need to know before they start?

Before we begin the activity we'll explain to the students what cryptography is and why it is relevant historically and presently.

Then we'll go through some examples of decoding and encoding messages. It might be preferable to do the decoding activity before moving on to encoding.

Sending/Receiving secret messages with cryptography

What is cryptography?

Cryptography is derived from the Greek words *kryptos* which means “hidden” or “secret” and *graph* meaning “writing”. So cryptography is all about hiding messages in an effort to create secure communication.

Cryptography is about creating protocols and algorithms for encoding and decoding messages so that third parties cannot read your communications. But it is also about analysing and deciphering the protocols that generate the encrypted messages.

How is cryptography used?

Cryptography is the reason modern computers exist! The Colossus series of computers (https://en.wikipedia.org/wiki/Colossus_computer) were used by the British during WWII to break German secret messages.

In contemporary times a common example of encryption can be seen in web browsers (https://en.wikipedia.org/wiki/Transport_Layer_Security). When a page has a lock in the address bar this means it is sent over the internet in an encrypted form. So no one, except the website you are using, can see the information being transmitted, like your password or bank details.

Unlike historical examples, today we don't see encrypted messages very often. A computer does the hard work of encoding or decoding the information for us.

What is an algorithm?

An *algorithm* is a sequence of steps for solving a problem or completing a task.

In the case of cryptography, the steps of an algorithm will help us transform a *plain text* message into an *encoded message* and vice versa.

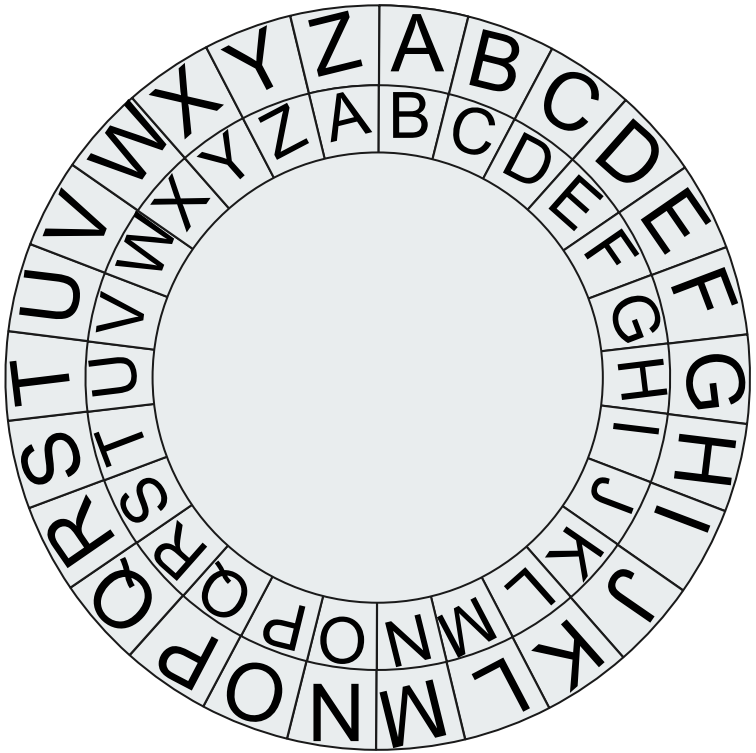
This activity also uses a particular algorithm to help us analyse encoded messages in order to decode them.

What is a Caesar Cipher?

A Caeser Cipher, also known as a rotation cipher, is a method of encoding text by replacing a letter with a letter that is a certain number of places away in the alphabet.

For example we can replace **A** with **B** which means we replace **B** with **C** and so on and so forth. There are 26 different ways to rotate the alphabet. The letter that lines up with **A** is known as the *key*.

A cipher wheel (shown to the right) is an easy way to keep track of these translations. A print out for making a cipher wheel is provided with the course materials.



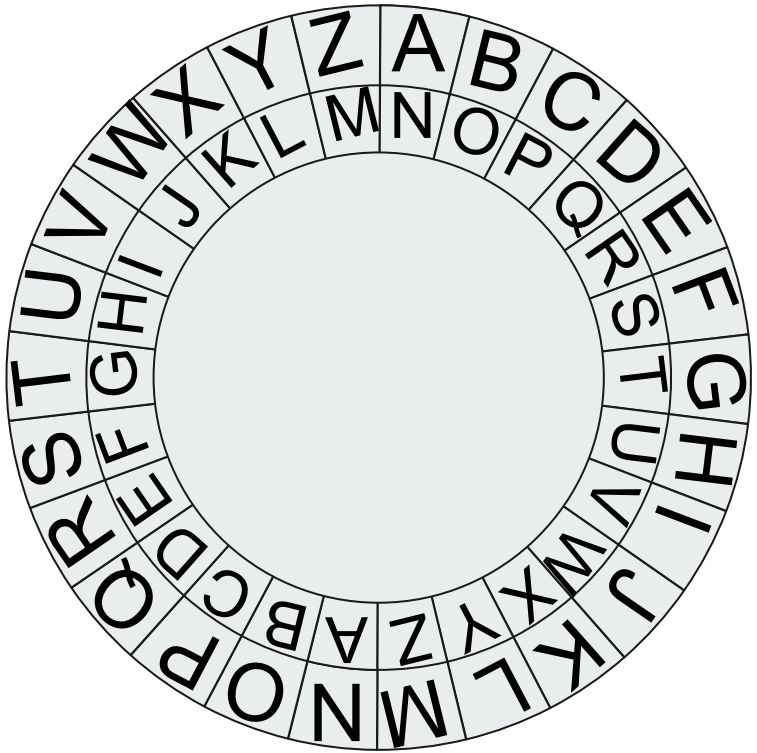
Example: Decoding a Caesar Cipher

Take the following message: **FUU VG VF N FRPERG**

If we know that the key for this cipher is **N** then we can rotate the cipher wheel so that the letter **A** lines up with the letter **N**.

The first letter is **F**, which corresponds with **S** on the wheel, the second is **U** which corresponds to **H**.

And so on for each letter of the encoded message we can discover the decoded message: **SHH IT IS A SECRET**



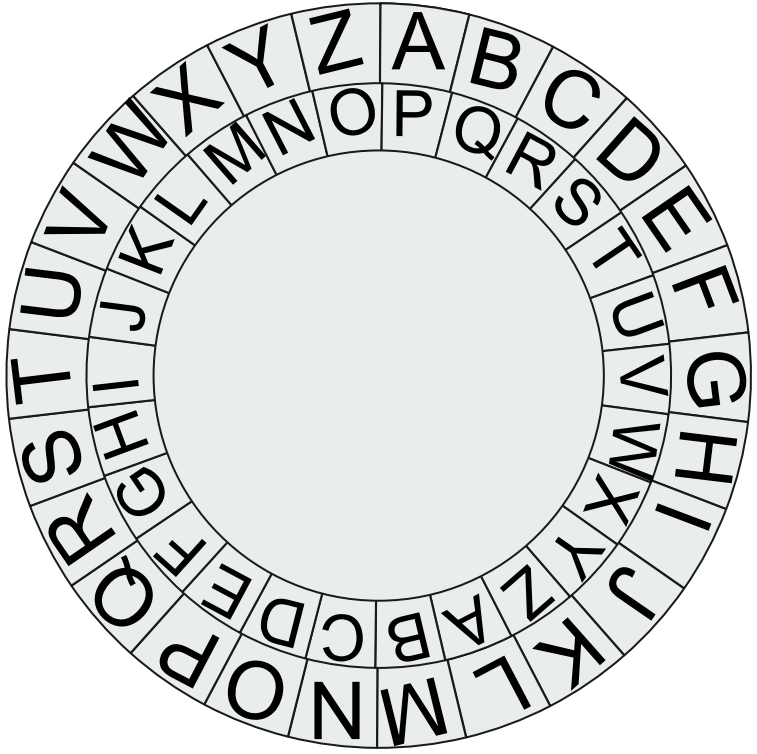
Example: Encoding a Caesar Cipher

The process encoding a message using a Caeser cipher is just the reverse of decoding Caeser cipher. Pick a key, for example **P**, and rotate the cipher wheel so the **A** lines up with the **P**

Now take a message like: **I BET YOU CAN'T SOLVE THIS**

For each letter look at the cipher wheel to see which letter it gets encoded into. You should end up with **X QTI NDJ RPC'I HDAKT IWXH**

To check that your encoding was correct, just use the decoding process on your encoded message. You should end up with the message that you started with!



Exploring things further

Doing the activity

Now the students have been shown an example of decoding/encoding a message they should be given the opportunity to decode and encode some messages themselves.

The first set of slides outline the challenge of decoding messages and provide some already encoded messages for the students to decode.

The next set of slides describes an activity for students pairing with each other to encode messages, swap the messages and then decode them.

Activity: Decoding secret messages

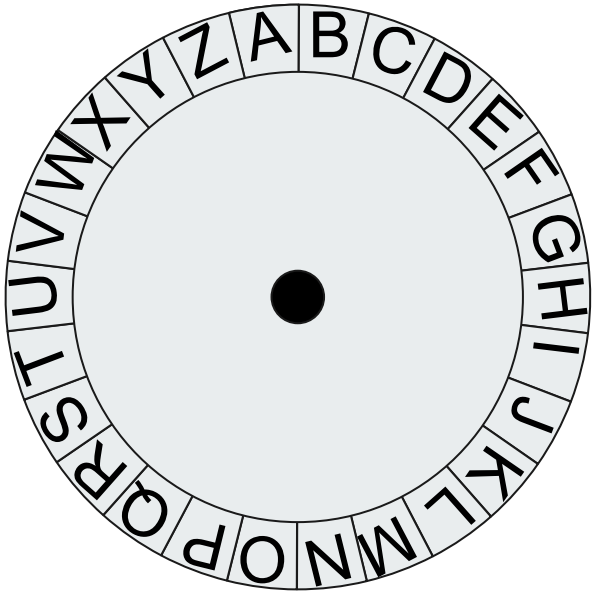
Decode the secret messages

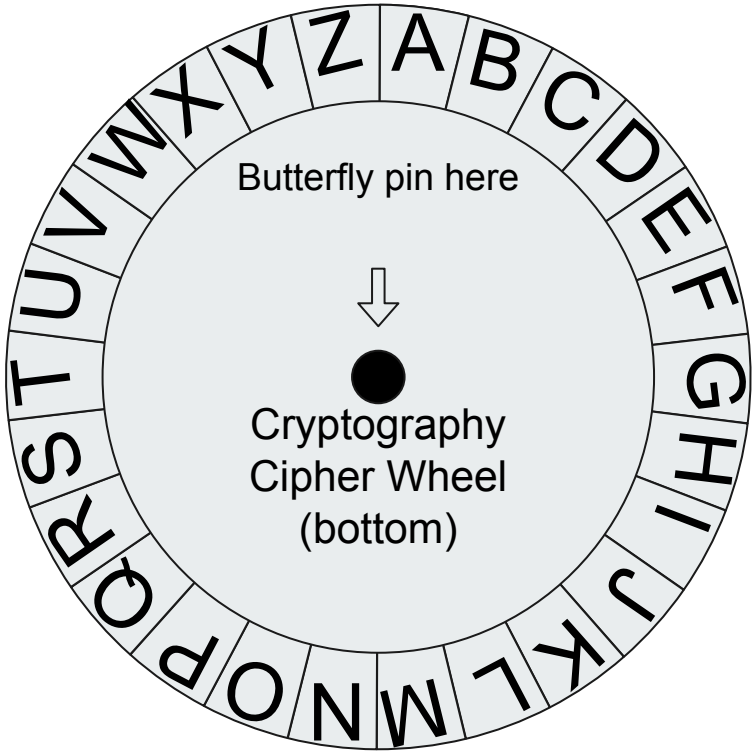
The following messages have been intercepted but they look like nonsense! We know that there are code names of secret agents hidden in them. Help us decode these messages and figure out those code names!

First you'll need to construct your cipher wheel before you can start cracking the codes.

Then for each encoded message use the *key* and your cipher wheel to decode the secret messages.

Once you've uncovered all the secret identities you'll be able to use them to find the mastermind behind it all!


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


Butterfly pin here
Cryptography
Cipher Wheel
(bottom)
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

Key: C											
encoded	M	K	O		R	Q	U	U	K	D	N	G
decoded						3						

Key: X														
encoded	P	E	B	O	I	L	Z	H		E	L	I	J	B	P
decoded														7	

Key: J															
encoded	Q	J	A	A	R	N	C		V		F	N	U	B	L	Q
decoded			2													

Key: H										
encoded	Q	H	T	L	Z		I	V	U	K
decoded							8			

Key: M															
encoded	W	M	F	Z	U	E	E		Q	H	Q	D	P	Q	Q	Z
decoded			4										1			

Key: S																	
encoded	H	W	J	J	Q		L	Z	W		H	D	S	L	Q	H	M	K
decoded					5												6	

Key:		Who is the master mind?							
encoded	1	2	3		4	5	6	7	8
decoded									

Sending secret messages

Your mission now is to send and receive secret messages.

Pair up with another secret agent and encode a secret message for them to read. Make sure you write down the key you used so your partner can decode your message!

Swap your message with your partner. Once you have their encoded message start decoding the message and see what they have to tell you.

Key:																
encoded																
decoded																
encoded																
decoded																
encoded																
decoded																
encoded																
decoded																
encoded																
decoded																

Activity Answers

Answers: Secret messages

1. Kim Possible
2. Sherlock Holmes
3. Harriet M. Welsch (AKA Harriet the Spy)
4. James Bond
5. Katniss Everdeen
6. Perry the Platypus
7. The Joker

You can use this website http://rumkin.com/tools/cipher/vigenere.php to check the messages the students create.
Use the key letter as the passphrase. And make sure you choose ‘encrypt’ (encode) or ‘decrypt’ (decode) depending on which is appropriate.

Reflection and evaluation

What have we learned?

It is important that students get a chance to reflect on their learning, and to evaluate how cryptography plays a role in their lives.

You can begin by having students think about how computers can use similar techniques for encoding messages.

Applications of cryptography like website and computer logins are also good areas to discuss and give students an idea of how cryptography is relevant to their digital lives.

This is also an opportunity to discuss issues of privacy and ethical and social implications in regards to private communication.

Extension activities

What else can we do with this idea?

If you would like to use or extend this activity for more advanced students the following slides provide some examples and materials for doing so.

An indicative year level based on the standards expressed generally in the Australian Curriculum has been provided as a guide, but this isn't a hard and fast rule.

Analysing and decoding secret messages with cryptography

Example: Analysing an encoded message

In the previous examples the person decoding the message knew the “key” to decoding the message. But what if we don’t know the key? Well we have to analyse the message to find it.

The most basic method of analysing a message is to look at uncommon occurrences like double letters, two letter words, one letter words, contractions or repeating words.

Once we’ve identified an usual feature of the message we can rotate our cipher wheel to match a letter with a possible replacement and try decoding the message. If the message makes sense then we’ve found the key! If not we’ll have to try again.

Example: Analysing an encoded message

OLSW, P'T ZABJR HUK JHU'A NLA VBA! P OHCL ILLU AYHWWLK PU H TLZZHNL HUK LUJVKLK!

With the above message we might notice several features worth looking at: there are some one letter words, a two letter word with an apostrophe a four letter word with an apostrophe and some words with double letters.

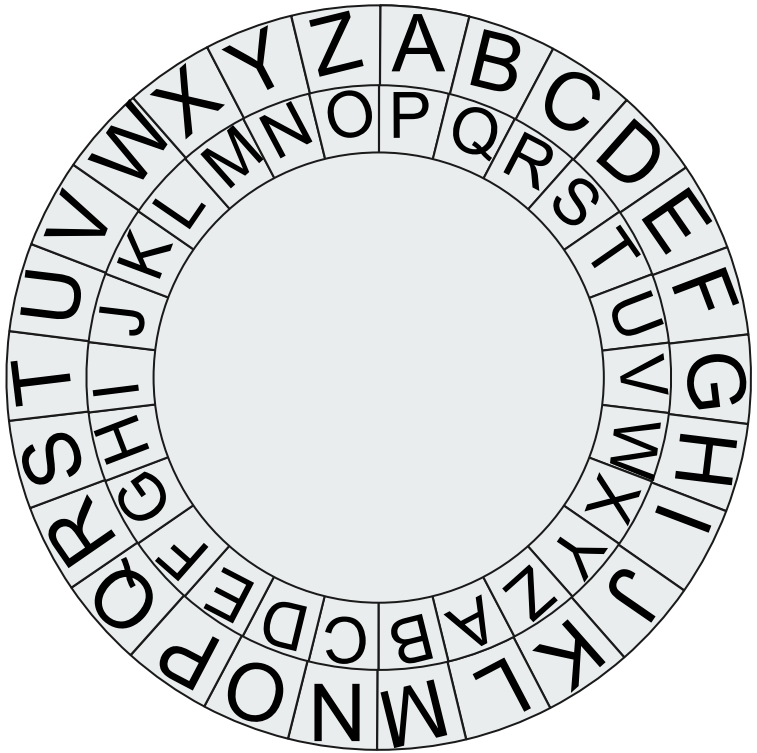
Since there are only two common one letter words in English (I and A) let’s start with those first.

Example: Analysing an encoded message

OLSW, P'T ZABJR HUK JHU'A NLA VBA! P OHCL ILLU AYHWWLK PU H TLZZHNL HUK LUJVKLK!

The one letter words in the encoded text are **P** and **H**. Let's start by trying **P** as **A**. Align the cipher wheel so that **P** i s matched with **A**. Since **A** is translated into **P** that means **P** is the *key*.

Immediately you should notice that **H** translates to **S** which means that the rest of the letters are also probably gibberish, but let's test it out on the first word anyway.
When translating with **P** as the key we get **ZWDH** as the first word, which is gibberish as expected.



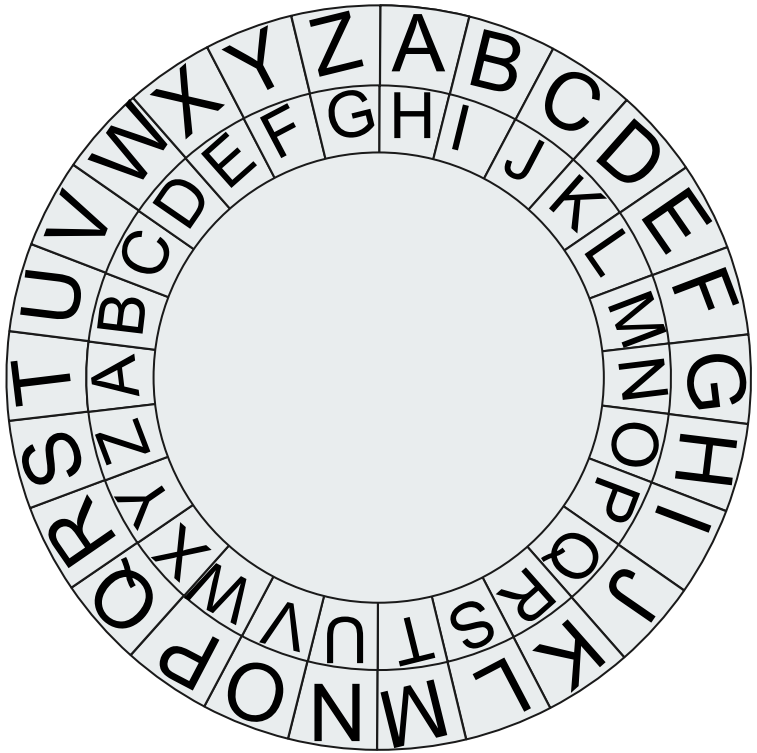
Example: Analysing an encoded message

OLSW, P'T ZABJR HUK JHU'A NLA VBA! P OHCL ILLU AYHWWLK PU H TLZZHNL HUK LUJVKLK!

Let's try **P** translates to **I** next. Rotating the cipher wheel gives **H** transforms to **I** which is very promising!

Decoding the first word gives us **HELP**, which is a real word! The next word is an **I** then an apostrophe, which is another good sign.

If we decode every single letter in the message we get the following message: **HELP, I'M STUCK AND CAN'T GET OUT! I HAVE BEEN TRAPPED IN A MESSAGE AND ENCODED!**



Even more secret messages with Vigenere ciphers (years 7+)

What is a Vigenere Cipher?

A Vigenere Cipher is very similar to a Caesar Cipher, except the letter we use as the key changes for every letter in the message. So now the key is a series of letters instead of just a single letter for the entire message.

The advantage of a Vigenere Cipher over a Caesar Cipher is that it is harder for someone who doesn't have the secret key to decode. Instead of an attacker only having to try **26** different keys to check there are $\mathbf{26}^{\text{(number of letters in the key)}}$ different combinations anyone without the key would have to try.

Example: Encoding a Vigenere Cipher

A Vigenere Cipher is very similar to a Caesar Cipher, except the letter we use as the key changes for every letter in the message. So now the key is a series of letters.

For example if we use the key **CAT** on the message **A BIG SECRET**

key	C		A	T	C		A	T	C	A	T	C
message	A		B	I	G		S	E	C	R	E	T
encoded	C		B	B	I		S	X	E	R	X	V

Example: Decoding a Vigenere Cipher

Much like with encoding, decoding a Vigenere Cipher is the same as decoding a Caesar Cipher. Except with several letters for the key.

For example if we are given the key **WIN** for the encoded message **RQTAVRNM VO KBKT**

key	W	I	N	W	I	N	W	I		N	W		I	N	W	I
encoded	R	Q	T	A	V	R	N	M		V	O		K	B	K	T
decoded	V	I	G	E	N	E	R	E		I	S		C	O	O	L