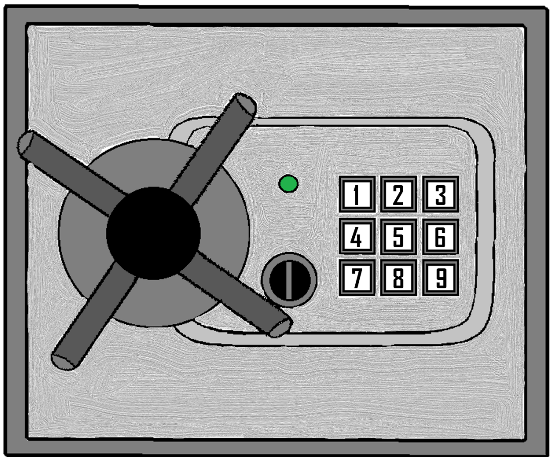
Cryptography Lesson Plan

2nd Class Maths

Kerry Brooks and Eoin Delaney



Abstract

We hope to introduce cryptography through the lens of simple arithmetic and patterns. Students will gain an insight into the historic background of cryptography and its application in the Roman Empire and during the American Civil War. Students will decrypt messages using the Caesar Cipher and the Pigpen Cipher. They will also design their own secret messages. Scratch will be incorporated into this lesson where the students will use interactive Caesar wheels and partake in several problem solving role play activities. We have designed a *classified* cryptography workbook where students can test their understanding of code-breaking and design their own codes. Students should appreciate that computers can be used to generate and break codes. We have also designed some interactive games on Scratch where students can practice cracking codes.

1 Learning Outcomes

According to the Curriculum documents (NCCA, 1999), students should be able to;

- Count the number of objects in a set
- Develop an understanding of addition by combining or partitioning sets
- Recognise patterns and predict subsequent numbers
- Sort and classify objects by two and three criteria
- Solve one-step and two-step problems involving addition and subtraction
- Construct number sentences and number stories; solve problems involving addition within 99

2 Learning Intentions

Upon successful completion of this lesson, students will be able to...

- Explain the meaning of the terms cryptography and cipher
- Recall some basic facts about the historic background of different ciphers
- Recognise the alphabet as a set and identify that there are twenty-six elements in this set
- Assign numbers to different letters in the alphabet
- Apply the arithmetic techniques of addition and subtraction to shift the letters of the alphabet
- Interpret geometric patterns
- Break simple codes using a Caesar Wheel
- Encrypt and decrypt messages using the Pigpen Cipher
- Design simple codes and communicate messages with classmates

3 Lesson Rationale

3.1 Prior Knowledge

For many children this will be the first link between code-breaking and mathematics. Students have previously covered the basic properties of arithmetic such as the associative, commutative and distributive properties of addition. Students should also be comfortable with ordering numbers and recording place values. Students should also recognise that a number frame or blank box can be used to show the presence of an unknown number. Children should enjoy the espionage theme that permeates this lesson.

3.2 Resources Required

- Cryptography Workbook (See our attached workbook!)
- Caesar Wheel (Available to print out)
- Colouring Pencils
- Scratch

3.3 Common Student Misconceptions

- Students may encounter difficulty in decoding messages using the Caesar wheel. We expect that some students may mix up the application of the inner and outer wheel when decrypting messages.
- The concept of a key and shift may be confusing for some students. It is useful to use simple shifts (1-3) to build up confidence in using the Caesar wheel.
- Some students may not realise that the shift can change for different messages. They may believe the shift is always k = 2 for the Caesar Cipher if this is an example that we are providing them with.

3.4 How will learning be assessed?

- Teacher Questioning
- Checking if students can break simple codes
- Listening to student conversations
- Scratch Games

4 Lesson Flow

Timing	***Learning Activity***	***Notes for Teacher & Scripted Questions***
10 mins	Introduction to Cryptography What is a cipher? Who uses codes and how are they broken? Historic background	Link to spies "Has anyone ever heard of a code" "How do spies communicate? Link to mathematics - Alan Turning Link to arithmetic & patterns
20 mins	The Caesar Cipher The concept of a shift and a key Scratch interactive wheel Workbook Examples Design your own secret code	Several demonstrations using wheel Emphasize what each wheel is used for "What happens if I use a shift of 26?" Consider student misconceptions
15 mins	Pigpen Cipher introduction Geometrical Code Class Exercises Scratch Games Mini Reflection	Problem based learning "What is a pattern?" "Can somebody remind me what geometry is?" Code locations; GRAFTON STREET Check work List three new things that you learned today

5 Cryptography

5.1 What is Cryptography?

Cryptography is the art of solving and writing of codes. The word cryptography comes from the greek words *kryptós* which means “hidden secret”. In ancient times cryptography was used to send secret messages between people. The purpose was to prevent outsiders who obtained the message from understanding the contained information. The messages would often be sent between army generals, diplomats and even spies. In order to reveal the secret, one would need a *key* to decode the message. In WWII the Germans used a device known as an enigma machine to encrypt and decrypt secret messages. The Allies employed thousands of mathematicians to try and break this code. It was the work of the great Bletchley Park scientists, most notably, Alan Turning who developed a computer to break the code. Modern computers can now easily break codes that were previously thought impenetrable. It is the arduous work of cryptographers that ensures our personal information is somewhat safe when we surf the web, make payments and call our friends! We will commence our lesson by looking at one of the oldest and simplest ciphers, the Caesar cipher.

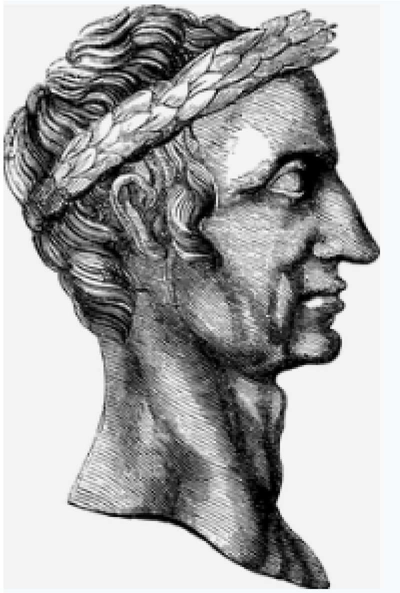


Figure 1: Julius Caesar

5.2 The Caesar Cipher

The Caesar Cipher was named after the roman emperor Julius Caesar. He is believed to have used this cipher to send secret messages across the Roman Empire. The cipher itself is a simple substitution cipher where each letter in the alphabet is replaced by a different letter that is a fixed number of positions down the alphabet. This cipher can be demonstrated by considering a simple example.

In order to encrypt the following message; *SECRET SPY* we can use a k = 2 shift. This means that each letter in the code will be shifted two letters along the alphabet, so the letter A becomes C and the letter B becomes D as shown in the Caesar wheel below.

The encrypted message becomes; *UGETGV URA*

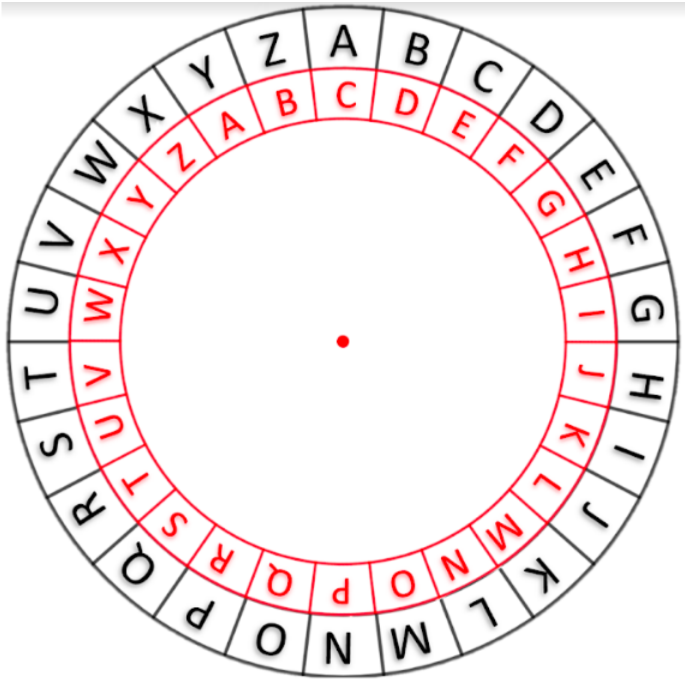


Figure 2: Caesar Wheel

We can also reverse this process and decode a secret message. If I receive the code; *CVVCEM CV FCYP*, I can use the wheel to decode the cipher to reveal the secret message *ATTACK AT DAWN*

The previous example used the key k = 2, meaning each letter was shifted two spaces down the alphabet. We can choose k to be any number between 1 and 25 to get a unique Caesar shift. If we use k = 26 the wheel does a full revolution and there is no difference between the encrypted message and the actual message.

5.3 The Pigpen Cipher

The Pigpen Cipher is a geometric cipher that assigns a unique shape to each letter in the alphabet. A secret message is then encrypted using these shapes. Only someone who knows what each shape means can decrypt the message. Variations of this code were used by the Freemasons and in the American Civil War.

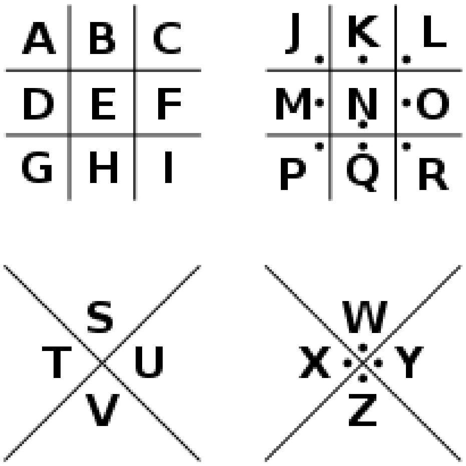
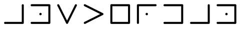
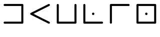


Figure 3: Graphical Symbols of the Pigpen Cipher

Using these symbols it is possible to encode secret messages. For example if I wanted to encrypt the location; *AMSTERDAM*

My code using the pigpen cipher would become; 

Similarly if I received the code  I could use my geometric key to reveal the message *DUBLIN*

5.4