Pearson **Year 7 Term 6** Codes and Encryption

Where it all started

Since the start of civilisation people have wanted to communicate with each other in privacy. Maybe the monarch or head of state of one country wanted to give a personal message to the king or queen of another without the messenger being able to see it. Encryption is when a message is written in code.

There are two different aspects of message hiding. The first is stenography (from Greek Steganos – covered – and graphein – to write). This is where people hide the actual message itself. For example, disappearing ink. Even modern spies have used their own urine when they run out of invisible ink! This is because urine looks clear, but can be seen under UV light. The ancient Greeks would tattoo messages on the scalps of couriers. When those couriers were captured and their heads shaved, the messages would be revealed.

Writing in code dates all the way back to Julius Caesar. His cipher was pretty easy to break, though. All he did was move the entire alphabet over four letters, so that A became D, and B became E, and so on. Once you were able to figure out one word using the cipher (something easy and often repeated, like “the”) everything became clear.

The “Caesar Box,” or “Caesar Cipher,” is one of the earliest known ciphers. Developed around 100 BC, it was used by Julius Caesar to send secret messages to his generals in the field. In the event that one of his messages got intercepted, his opponent could not read them. This obviously gave him a great strategic advantage.

k = CRYPTO CRYPTO CRYPTO

m = HAVEANICEDAYTODAY

c = KSUUUCLUDTUNWGCQS

Questions:

1. What does encryption mean?
2. What does monarch mean?
3. Why might someone want to send a message that is encrypted?
4. What does ‘UV light’ mean?
5. The ancient Greeks wrote messages on the scalps of couriers. Would this be a good method of encryption for an urgent message? Why?
6. Write out the alphabet, and then repeat it underneath with a Cae-sar shift of three.
7. Use it to decode L ORYH EUHDNLQJ FRGHV
8. Write a short message to your partner (at least six words).
9. Decode your partner’s code.
10. Is the Caesar Cipher a good way to write messages in code? Why?

@JennyHillParker

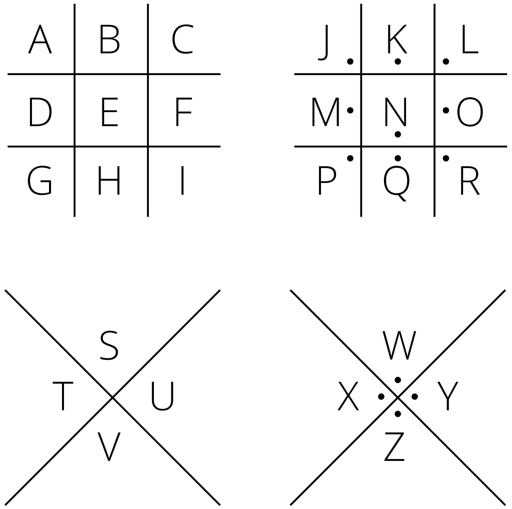
Video link: **Codes and encryption**

Year 8 Term 6 Codes and Encryption

Mary, Queen of Scots and Queen Elizabeth

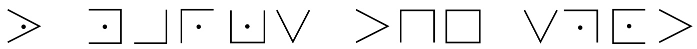
Mary Queen of Scots produced a code of her own whilst being held under house arrest in England. She was deemed to be a large threat by Queen Elizabeth, who feared Mary's influence over the Catholic population. In order to enable herself to communicate outside of her house arrest, Mary developed a relatively complicated code. Her code begun with a standard coded alphabet; however, it also featured many interesting aspects. Mary's code was particularly sophisticated, using over 100 different ciphers in order to prevent the code from being cracked. She also includes many symbols with no assigned meaning in order to throw off anybody attempting to decipher the code.

Despite the fact that countless hours of hard work went in to producing intricate codes such as the one developed by Mary queen of Scots, they can also be deciphered. In fact, it was through deciphering Mary's code that she was incriminated, and this ultimately led to her execution. Due to the clear importance of the exchanges of coded letters, Elizabeth sent a team of coding experts to try and crack this secret code. One of the leading cryptologists of the time, Thomas Phelippes, was tasked with the job of cracking Mary's code and was eventually able to. He did this by examining the symbols that she repeated frequently. Therefore, whilst the intention of codes may be to further the political and social lives of people within difficult situations, it is clear that the risks are also incredibly high.



Questions:

1. What is encryption?
2. Why was Mary under house arrest?
3. Thomas Phelippes cracked the code by looking at what symbols Mary repeated most. What letters in the alphabet are used the most in English? Try to list the top five.
4. Write a message to your partner using Mary's code (top left).—at least six words.
5. Decode your partner's message.
6. Look at the pigpen code to the right; use it to write the alphabet.
7. Why do you think it is called the 'pigpen' code?
8. Write your full name in pigpen code.
9. Decode this;



10. Write a short message to your partner, and decode theirs.

Pearson

Year 9 Term 6 Codes and Encryption

WWII - Alan Turing and the Enigma

Alan Turing was a brilliant mathematician. Born in London in 1912, he studied at both Cambridge and Princeton universities. He was already working part-time for the British before the Second World War broke out. In 1939, Turing took up a full-time role at Bletchley Park in Buckinghamshire – where top secret work was carried out to decipher the military codes used by Germany and its allies. The main focus of Turing's work at Bletchley was in cracking the 'Enigma' code. The Enigma was a type of enciphering machine used by the German armed forces to send messages securely. Although Polish mathematicians had worked out how to read Enigma messages and had shared this information with the British, the Germans increased its security at the outbreak of war by changing the cipher system daily. This made the task of understanding the code even more difficult.

Turing was prosecuted in 1952 for homosexual acts. He accepted hormone treatment with DES, a procedure commonly referred to as chemical castration, as an alternative to prison. Turing died on 7 June 1954, 16 days before his 42nd birthday, from cyanide poisoning. An inquest determined his death as a suicide, but it has been noted that the known evidence is also consistent with accidental poisoning.

Following a public campaign in 2009, the British Prime Minister Gordon Brown made an official public apology on behalf of the British government for "the appalling way [Turing] was treated". Queen Elizabeth II granted a posthumous pardon in 2013. The term "Alan Turing law" is now used informally to refer to a 2017 law in the United Kingdom that retroactively pardoned men cautioned or convicted under historical legislation that outlawed homosexual acts.

Questions:

1. When and where was Alan Turing born? How long ago was this?
2. How old was he when the Second World War broke out?
3. What does the term 'armed forces' mean?
4. Why would members of the armed forces want to send messages that couldn't be read by others?
5. What was the name of the famous code that was broken by Alan Turing?
6. How old was Turing when he was prosecuted?
7. What was he prosecuted for?
8. Queen Elizabeth issued a post-humous pardon; what does this mean?
9. The Enigma code was cracked by looking for high frequency words. What does this mean?
10. List five high frequency words in English.

@JennyHillParker

Video link: **Alan Turing**

Year 10 Term 6 Codes and Encryption

Prime numbers and credit cards

Each time you make a purchase online, your credit card number is kept safe using the power of prime numbers. Cryptography is the study of coding and sending secret messages. The idea is to construct a system where one person can safely send sensitive information to another person. This means that if some nefarious third party got a hold of that message, they couldn't figure out what it meant. Only the intended third party would know how to crack the code.

The RSA cryptographic system is one of the first and most widely used cryptographic systems. It relies on a basic fact about whole numbers: if you take a big enough odd number, it's hard to figure out whether it can be divided evenly by any smaller whole numbers.

Some numbers are prime, like 5 and 173. This means they can only be divided by 1 and themselves. Most numbers are not prime, like 6, which can be divided by 2 and 3. When you type out your credit card numbers and hit enter, that information is immediately encrypted or turned into a code before it's sent over the Internet. In the RSA cryptosystem, your credit card number is encoded into a huge prime number — say, a 600 digit long prime number — and then multiplied by another huge prime number — say, a 550 digit long prime number — the result is a mind-bogglingly huge number that can only be divided by those two primes and nothing else. To crack the code, someone would have to figure out which primes divided that number. And that's a near-impossible task, even for a computer.

Questions:

1. What are the first twenty prime numbers?
2. Is 531 a prime number? How can work this out?
3. To do prime factor decomposition, we need to know the smaller prime numbers. What is the biggest prime number that you know?
4. Choose two prime numbers under 20 and find the product. Tell you partner and ask them to work out the two primes.
5. Repeat with two primes that are between thirty and fifty.
6. Repeat with two prime numbers between fifty and one hundred. How long does this take?
7. Why is it important that credit card details are kept secure?
8. What steps should you take if you believe that someone has details of your bank card?
9. What is the difference between credit cards and debit cards?
10. There are people who post 'phishing' questions on social media. What does this mean, and what information are they trying to get?

Video link: **Prime factors and credit cards**

@JennyHillParker