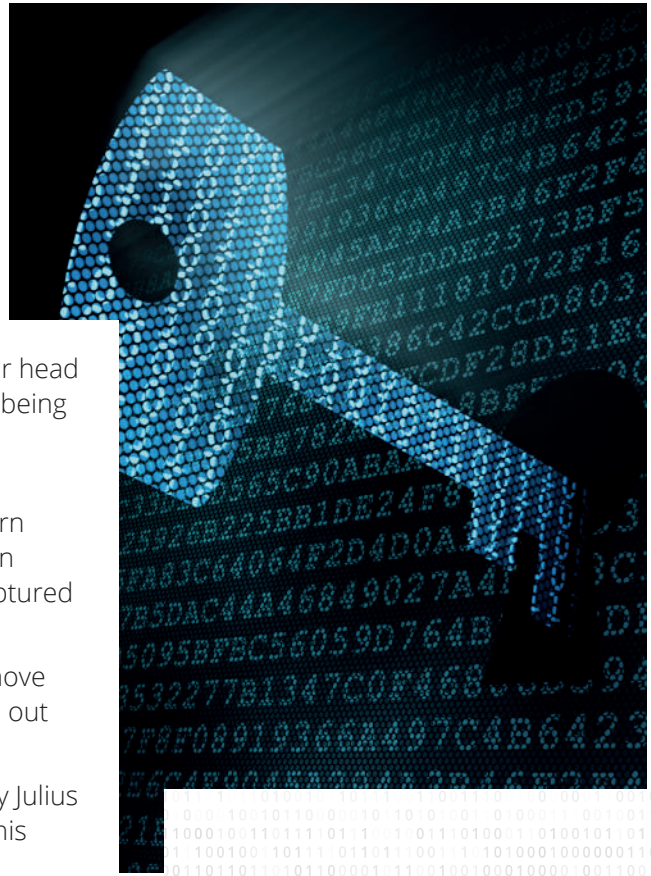
Pearson **Year 7 Term 6** Codes and Encryption

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.

Answers:

1. Encryption means turning words or data into code.
2. Monarch means king or queen.
3. So that the information stays private.
4. UV light is ultra violet light.
5. No! The length of time needed to wait for the hair to grow would make it a very poor method of encryption for an urgent message.
6. Alphabet.
7. I LOVE BREAKING CODES
8. Message.
9. Message.
10. Not really—they're very easy to break!

k = CRYPTO|CRYPTO|CRYPTO

m = HAVEANICEDAYTODAY

c = KSUUUCLUDTUNWGCQS

Video link: **Codes and encryption**

Year 8 Term 6 Codes and Encryption

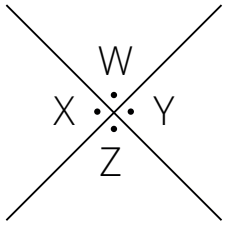
Mary, Queen of Scots and Queen Elizabeth

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.

A	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	Q	R



Answers:

1. Encryption means turning words or data into code.
2. Mary was under house arrest because Elizabeth was worried that she would have too much influence over the Catholic population.
3. The five highest frency letters in the English language are e, t, a, o, I—in that order.
4. Message.
5. Message.
6. The first few letters are;

   A B C D E F

   
7. Because the grid lines look like pig pen fences that farmers use.
8. Name.
9. X MARKS THE SPOT
10. Messages.

Video link: **Mary Queen of Scots**

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.

Answers:

1. He was born in London in 1912, 110 years ago.
2. He was 27.
3. Armed forces means the forces that bear arms, ie the military; the Army, the Navy and the Royal Air Force.
4. Because they are coordinating a military attack.
5. The Enigma code.
6. He was forty.
7. He was prosecuted for homosexual acts.
8. A post-humous pardon means that he was pardoned after his death. Homosexuality was decriminalised in 1967.
9. High frequency words are words that are used a lot.
10. The top five are the, said, in, he and I.

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.

Answers:

1. 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47, 53, 59, 61, 67, 71.
2. No, 531 = 3 x 59
3. Try to memorise the prime numbers below 30.
4. Product.
5. Product.
6. Product—it probably took a little while? This is why encryption using prime numbers is secure—its hard to crack the code!
7. Because otherwise people could access your money and steal from you!
8. Debit cards pay using money from your bank account, and credit cards pay with borrows money that you then need to pay back.
9. Inform the bank asap so that they can block the card, ie prevent it from being used.
10. Phisihing is when people ask questions like 'what was the first road you lived on?', or 'what was the name of your first pet?' Sometimes these questions are asked by people who are trying to break into your bank accounts.

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

@JennyHillParker