Unit 5.2: We are cryptographers

5 Key words to remember

Cipher – an algorithm (set of agreed rules) for turning a message into code or used for cracking the code.

Cryptography – the writing or solving of hidden messages.

Encode – to change a message into an agreed code. (**Decode** turns the message back into understandable text.)

Encrypt – to convert a readable message into a form which cannot be read by those who do not know the key or cipher system. (**Decrypt** converts the encrypted message back to readable text.)

Transmission – a communication of a message over a long distance.

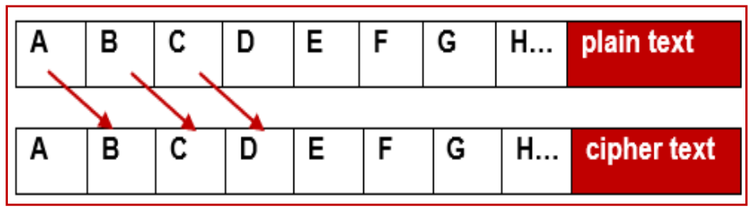
Key takeaways

- ‘Crypt’ means hidden or secret. **Cryptography** is the study of the hidden or secret **transmission** (sending) of messages and of how such messages can be created and worked out.
- Semaphore messaging uses brightly coloured flags held in different positions as a visual signal system to spell out messages. They are not widely used today but were commonplace at sea in the 19th century.
- Morse code is a method of communication which uses dots or dashes, made up of sound or light pulses, to **encode** messages. Morse code is named after Samuel Morse (1791–1872).
- Caesar **cipher** is where each letter of the alphabet is substituted by another letter being shifted (moved) a certain number of positions along the alphabet.
- Looking at how often certain letters occur (letter frequency) in **encrypted** messages can sometimes provide useful clues for **decoding**.
- Computers use **encryption** to make sure that communications between devices are secure. Look out for a padlock icon and HTTPS at the start of website addresses. (This stands for Hypertext Transfer Protocol Secure.)
- Learning about **cryptography** can help us to create strong passwords. For example, random words and nonsense phrases which include numbers, symbols, upper- and lower-case letters would be hard for others (and computers) to guess!

Knowledge check – Caesar Cipher

Caesar **cipher** is a substitution **cipher** named after the Roman Julian Caesar. He used it to send secret messages to his generals in the field. If one of his messages got intercepted, his opponent could not read it.

Caesar shifted (moved) each letter of his message a certain number of letters down the alphabet to produce what could be called the ciphertext. For example, with a shift of 1, A would be replaced by B, B would become C, and so on.

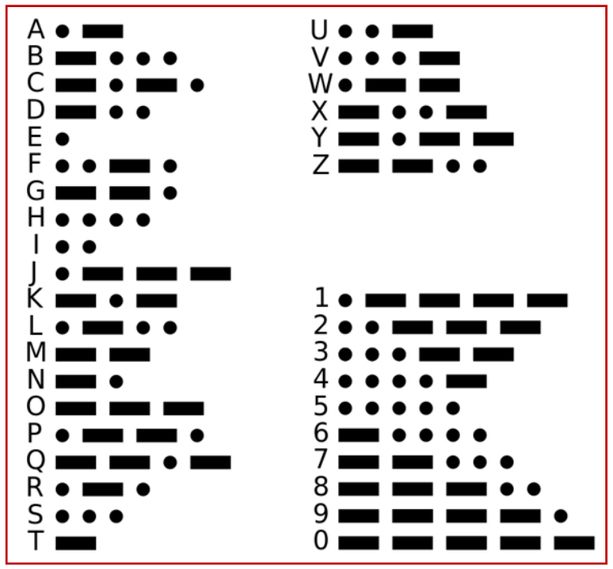


Test yourself: Try writing your name using this cipher.

Knowledge check – Morse code

Look at the Morse code for letters and number below.

Test yourself: Which letters have the shortest code? Why do you think this is?



People – The Enigma Code Crackers

During the Second World War, the Enigma machine was used for the **encryption** of German secret messages. The machine looked a bit like a typewriter keyboard and for each letter that was tapped in, another letter would come out so messages would be received in code.

Building on the work of Polish mathematicians, Alan Turing (1912–1954) and his team at Bletchley Park designed a code cracking machine known as the Bombe. They used the Bombe to decipher German military secret codes. Experts believe that breaking the Enigma code may have shortened the war by up to two years!