THE DUSTON SCHOOL 4-19

Knowledge Organiser

Computing

Year 7: Code Breaking Unit

Name/Class:

Enquiry Questions

- What is cryptography and how has it been used in previous centuries?
- What is a substitutional cipher?
- In terms of frequency analysis, why will it help us to know the most common letter in the alphabet?

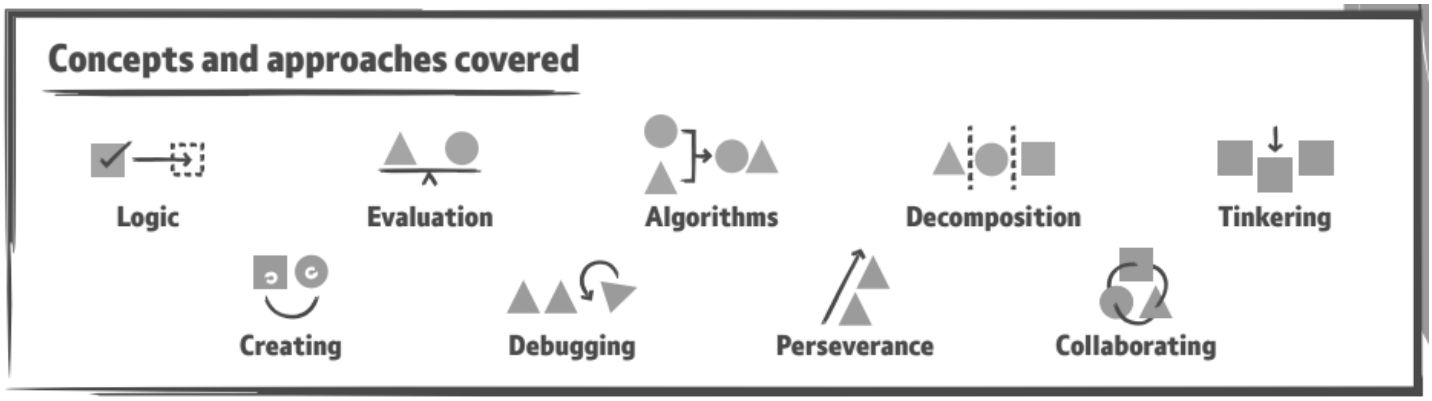
Terminology

Cyber Security The protection of internet-connected systems, including hardware, software and data, from cyberattacks.	**Encryption** The act of protecting data by scrambling it in such a way that only someone with the secret code or key can read it	**Cipher** An algorithm for performing encryption or decryption.
Decryption The act of unscrambling encrypted data, with a secret code or key, so that it can be read.	**Ciphertext** **Ciphertext** is encrypted text transformed from plaintext using an encryption algorithm. **Ciphertext** can't be read until it has been converted into plaintext (decrypted) with a key.	**Decryption Key** **Decryption key** is the code that you need to transform an encrypted message, document, or other data into a form that can be freely read

KNOWLEDGE

Code cracking

This unit introduces pupils to the history of computing and, in particular, how computers were used as code-cracking devices in World War II.



Who was Alan Turing

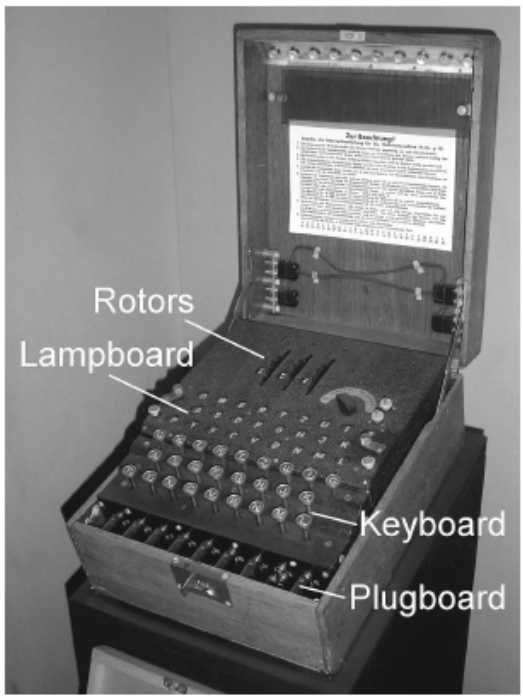
- Alan Turing was a brilliant mathematician who was born in London in 1912 and studied at both Cambridge and Princeton universities.
- He worked part-time for the British Government's Code and Cypher School before the Second World War broke out.
- In 1939 he took up a full-time role at Bletchley Park in Buckinghamshire.
- He died in 1954 and the vital work he carried out did not fully come to light until long after his death.
- His impact on computer science has been widely acknowledged: the annual 'Turing Award' has been the highest accolade in Computer Science since 1966.
- The work of Bletchley Park – and Turing's role there in cracking the Enigma code – was kept secret until the 1970s, and the full story was not known until the 1990s.
- The efforts of Turing and his fellow code-breakers shortened the war by several years. They saved countless lives and helped the Allies win the war.
- In 1945, Turing was awarded an OBE for his wartime work.

Alan Turing statue Manchester

KNOWLEDGE

Enigma and the Bombe

- Turing's main job at Bletchley was in cracking the 'Enigma' code.
- The Enigma was a type of enciphering machine used by the Germans to send secret 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 played a key role in cracking this code, inventing a machine known as the Bombe, along with fellow code-breaker Gordon Welchman. This device helped to reduce the work of the code-breakers. From mid-1940, German Air Force signals were being read at Bletchley and the intelligence gained from them was helping the war effort.



Enigma machine

Bletchley Park

- Turing also worked to decrypt the complex German naval communications that had defeated many others at Hut 8 in Bletchley Park.
- German U-boats were inflicting heavy losses on Allied shipping so it was important that the signals could be deciphered.
- With the help of captured Enigma material, and Turing's work in developing a technique he called 'Banburismus', the naval Enigma messages were able to be read from 1941.

Bletchley Park

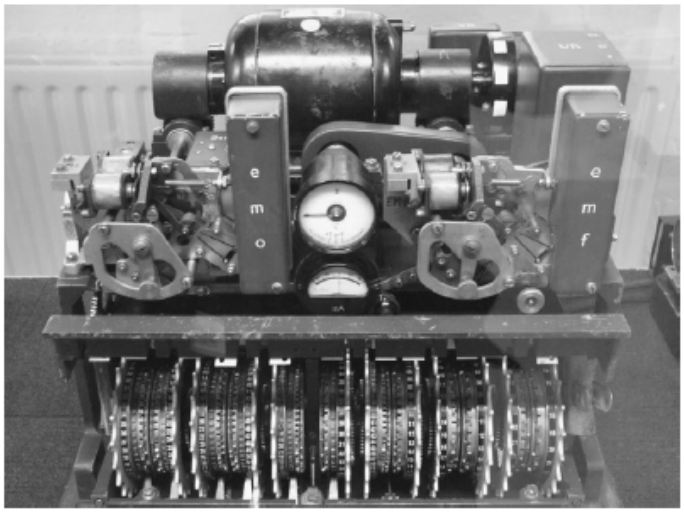
- He headed the 'Hut 8' team at Bletchley, which carried out cryptanalysis of all German naval signals. This meant that, apart from during a period in 1942 when the code became unreadable, Allied convoys could be directed away from the U-boat 'wolf-packs'.
- Turing's role was pivotal in helping the Allies during the Battle of the Atlantic.

KNOWLEDGE

THE DUSTON SCHOOL

Turingery and Delilah

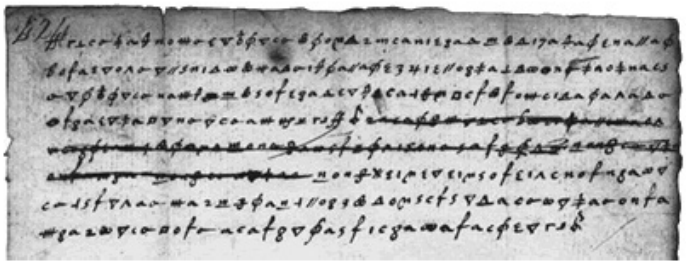
- In July 1942, Turing developed a complex code-breaking technique he named 'Turingery'. This method fed into work by others at Bletchley in understanding the 'Lorenz' cipher machine.
- Lorenz enciphered German strategic messages of high importance: the ability of Bletchley to read these contributed greatly to the Allied war effort.
- Turing travelled to the United States in December 1942 to advise US military intelligence in the use of Bombe machines and to share his knowledge of Enigma.
- Whilst there, he also saw the latest American progress on a top secret speech enciphering system. Turing returned to Bletchley in March 1943, where he continued his work in cryptanalysis.
- Later in the war, he developed a speech scrambling device which he named 'Delilah'. Delilah was a small, compact device for working out the settings on the "Turingey" or "Turingismus".



Lorenz cipher machine

More Code Cracking History

- Code and cipher-breaking has been around for centuries
- Cryptanalysis – the art of deciphering encoded messages – became vital during WW2 as British boffins strived to decode encrypted German military messages.
- Nearly 2000 years ago, Julius Caesar (a Roman Emperor), invaded many countries to increase the size of the Roman Empire. He needed a way of communicating his battle plans and tactics to his army without the enemy finding out. So Caesar would write messages to his generals in code. Instead of writing the letter 'A', he would write the letter that comes three places further on in the alphabet, the letter 'D'.
- Mary Queen of Scots, when she was plotting against Elizabeth the First, devised a code replacing letters with symbols. Mary wanted to kill Elizabeth so that she could become Queen of England so sent coded messages to her co-conspirator Anthony Babington.
  Unfortunately for Mary, her code was easy to decode using Mathematics!
  Above is part of a letter sent by Mary Queen of Scots to Anthony Babington.



A coded message sent by Mary Queen of Scots.

Online Dangers

Homework

Homework 1 **Due date:**

- There are 6 lines of code!
- How will we crack it in time to save the invasion?
- The Allies are relying on us to crack this!

Code Cracking Activity Strips

12 15 3 1 20 5 4	12 15 1 4	19 16 5 5 4	4 5 16 20 8	1 20
21 2 15 1 20	10 21 14 15	15 18 4 5 18 19	3 8 1 18 7 5 19	
20 5 14	2 5 1 3 8	20 23 5 12 22 5	18 5 1 4 25	
13 9 12 5 19	11 5 5 16	11 14 15 20 19	1 23 1 9 20	
14 15 18 20 8	15 6	6 21 18 20 8 5 18	15 21 20	
25 15 21 18	3 15 13 13 1 14 4	8 9 7 8	7 5 18 13 1 14	

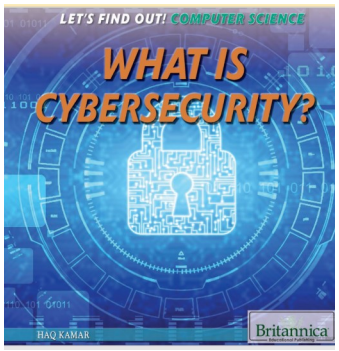
Cipher (Key)

A = 1	G= 7
T = 20	E = 5

Wider Reading List

Wider Reading

- OCR Computer Science for GCSE Student Book
- What is cyber security?



Useful websites for further research:

BBC information about the Bletchley Park Colossus Computer: http://news.bbc.co.uk/1/hi/technology/8492762.stm

The Enigma Machine: http://www.bbc.co.uk/history/topics/enigma

How Alan Turing cracked the Enigma Code: http://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

Imperial War Museum: http://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

BBC History:http://www.bbc.co.uk/history/code_breaking/

NRich Maths - The Secret World of Code Cracking: https://nrich.maths.org/2197

https://www.bbc.com/bitesize/guides/zs87sbk/revision/1

https://www.futurelearn.com