

Knowledge Organiser

Computing

Year 8 Term 3:
Encryption & Code Breaking Unit



Name:

Class:

Teacher:

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

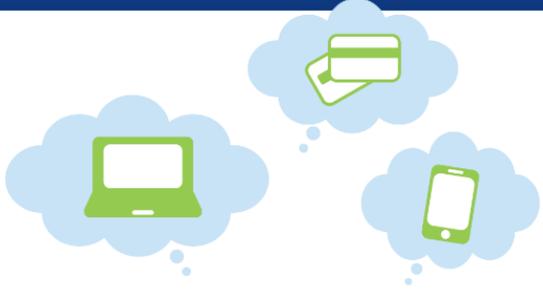
<p><u>Cyber Security</u></p> <p>The protection of internet-connected systems, including hardware, software and data, from cyberattacks.</p>	<p><u>Encryption</u></p> <p>The act of protecting data by scrambling it in such a way that only someone with the secret code or key can read it</p>	<p><u>Cipher</u></p> <p>An algorithm for performing encryption or decryption.</p>
<p><u>Decryption</u></p> <p>The act of un-scrambling encrypted data, with a secret code or key, so that it can be read.</p>	<p><u>Ciphertext</u></p> <p>Ciphertext is the result of the encryption process. The encrypted plaintext appears as apparently random strings of characters, rendering them useless.</p>	<p><u>Decryption Key</u></p> <p>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</p>
<p>Plaintext</p> <p>Plaintext is an un-encrypted, readable, plain message that anyone can read.</p>	<p>Symmetric algorithm</p> <p>A Symmetric algorithm Uses the same key for both encryption and decryption. Both parties must agree on the algorithm key before commencing communication.</p>	<p>Asymmetric algorithm</p> <p>This uses two different keys: a public key and a private key. This enables secure encryption while communicating without previously establishing a mutual algorithm.</p>

KNOWLEDGE

Encryption: Why it matters?



Data breaches exposed at least 423 million identities in 2015 — increasing by more than 20 percent in just a single year.

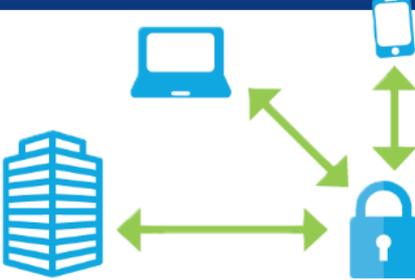


Many Britons worry about hacking — of their credit card information, phones and computers — more than any other crime. And for good reason: nearly half of British adults have been hacked.

ENCRYPTION IS A PART of almost every service or device we use to live our lives online. Every day, often without us even being aware of it, encryption keeps our personal data private and secure. Encryption is a vault that secures our personal information that is held by businesses and government agencies. It is a lock that prevents identity thieves from stealing our information when we log on to our bank accounts. It is an extra layer of security to safeguard our critical infrastructures. And it is a secure envelope that keeps hackers from reading our personal communications. Encryption is all of these things and more:



Use of encryption continues to rise, with more than one third of businesses in one recent survey reporting that their organization uses encryption extensively.



Use of encryption is steadily shifting to a strategic activity, with organizations moving to an enterprise-wide encryption strategy.



Government rules — around patient data, financial transactions, and consumer information — frequently require companies to encrypt the data they hold.

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.

Concepts and approaches covered



Logic



Evaluation



Algorithms



Decomposition



Tinkering



Creating



Debugging



Perseverance



Collaborating

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

Historical Figures

Alan Turing

Mathematician, Computer Scientist

An English mathematician, computer scientist, logician, cryptanalyst, philosopher, and theoretical biologist.

Turing studied undergraduate Mathematics at Cambridge University and completed a PhD in Mathematics at Princeton University.



(23 June 1912 - 7 June 1954)

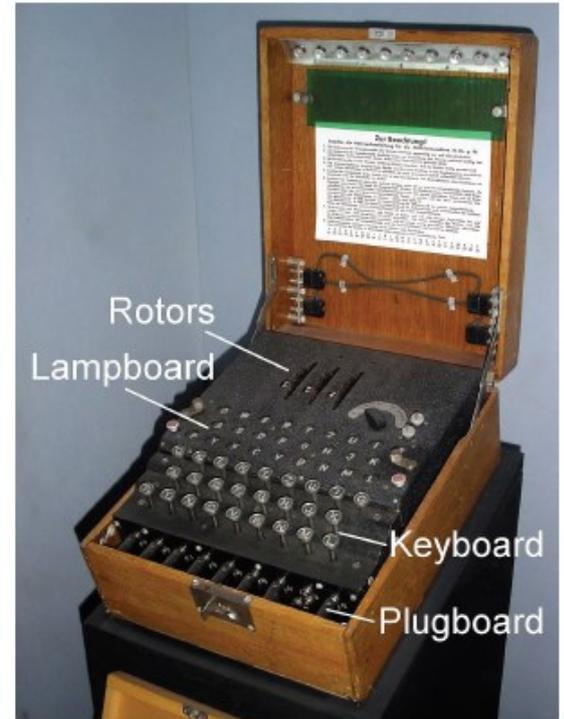
In 1945 he was awarded an OBE as recognition of his wartime work. Alan Turing was a keen long distance runner. He occasionally ran 40 miles from Bletchley to London for meetings.

He is known for the Turing test, Turing Machine and the crucial role he played as a code breaker at Bletchley park during the second world war.

In particular he helped improve the bombe method, an electro-chemical machine that worked to break the German Enigma code, in the second world war.

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

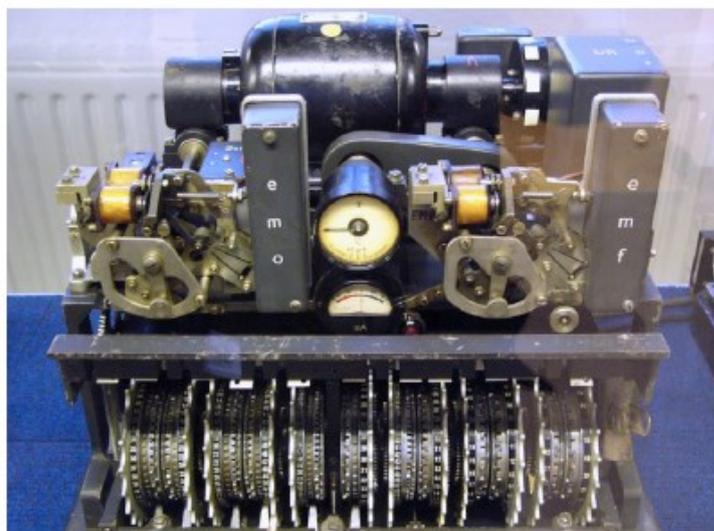
- Turing also worked to decrypt the complex German naval communications that had defeated many others at Hut 8 in Bletchley Park.
- German U-boats were inflicting heavy losses on Allied shipping so it was important that the signals could be deciphered.
- With the help of captured Enigma material, and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



Bletchley Park

Turingery and Delilah

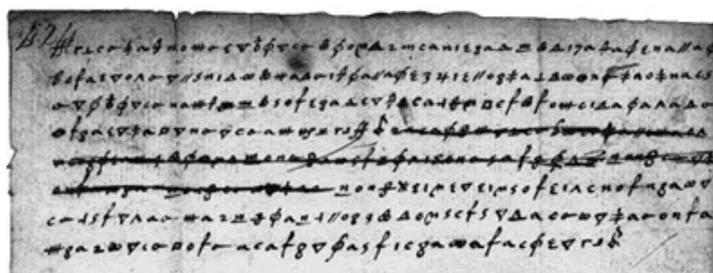
- In July 1942, Turing developed a complex code-breaking technique he named 'Turingery'. This method fed into work by others at Bletchley in understanding the 'Lorenz' cipher machine.
- Lorenz enciphered German strategic messages of high importance: the ability of Bletchley to read these contributed 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.



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.

Engage Task

Lesson 1

Big Question: What is cryptography and how has it been used in previous centuries?

Complete the word search below.

E	D	C	J	T	G	E	S	P	M	L	L	J	A
C	G	E	K	T	K	U	N	Y	P	Z	V	D	X
O	R	C	C	M	U	J	R	T	N	H	C	Y	J
D	Z	I	Y	R	Z	R	Z	H	K	A	A	U	Q
E	Q	P	U	O	Y	P	I	O	M	N	E	F	E
B	C	H	P	Y	X	P	L	N	R	K	S	B	N
R	R	E	N	C	H	O	T	N	G	E	E	M	C
E	I	R	A	C	J	K	K	I	E	B	R	E	R
A	G	T	X	B	R	E	Z	A	O	D	C	S	Y
K	E	E	T	U	X	Y	K	W	N	N	I	S	P
I	Z	X	X	A	D	U	Z	X	J	X	P	A	T
N	H	T	K	Z	O	O	I	F	T	S	H	G	I
G	V	U	R	L	F	T	T	T	P	T	E	E	O
G	C	O	D	I	N	G	P	K	A	G	R	Q	N

ENCRYPTION
 KEY
 CODING
 DECRYPTION
 PYTHON
 CIPHERTEXT
 TURING
 MESSAGE
 CODEBREAKING
 CAESERCIPHER

Engage Task

Lesson 2

Big Question: What is the purpose of encryption?

Work out the hidden code using the key below.

A	B	C	J	K	L
D	E	F	M	N	O
G	H	I	P	Q	R
S			W		
T		U	X	Y	
	V			Z	

7 0 0 > J 7 0 0

7 J V V V 7 0 0 > 0 0 > 0 0 7 V

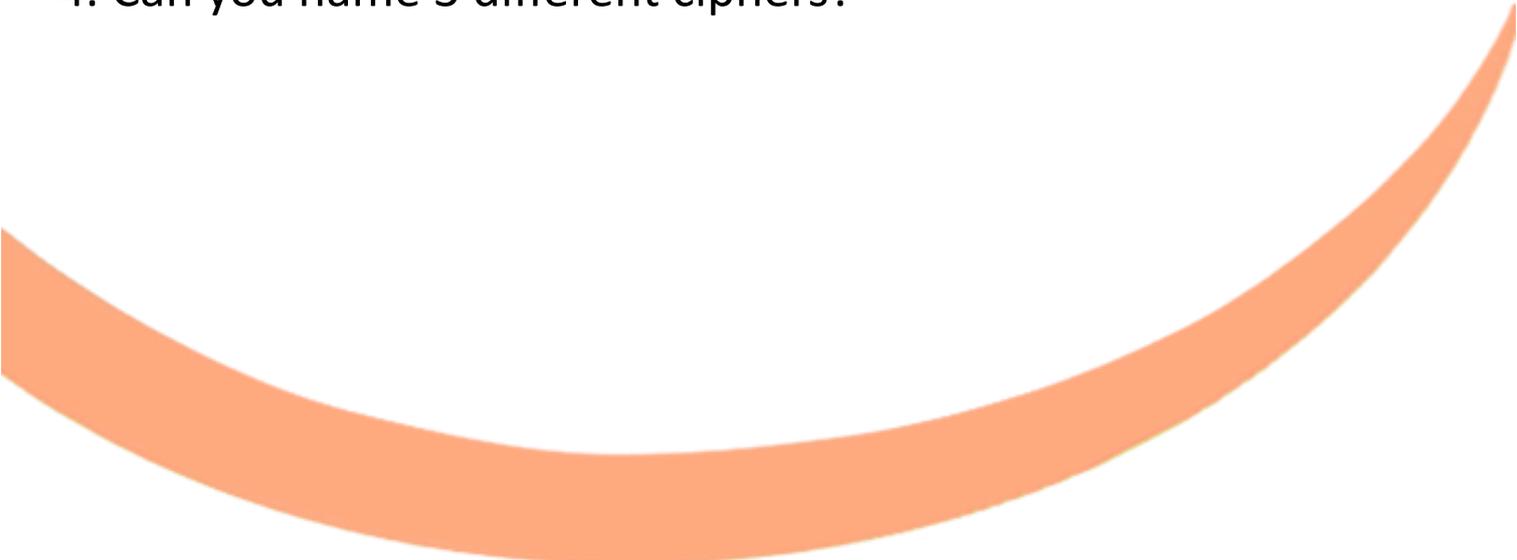
7 0 0 > J 7 0 0

Engage Task

Lesson 3

Big Question: Can numbers and images be used in cryptography?

Answer the questions below:

1. What does the word substitution cipher mean?
 2. Who was Morse Code named after?
 3. Who is Alan Turing?
 4. Can you name 3 different ciphers?
- 

Engage Task

Lesson 4

Big Question: Can you name 3 historical figures in cryptography?

Can You work out the message using the code?

								
B	N	E	K	T	U	C	S	G
								
P	L	V	I	H	A	C	D	

 |    |      |     |   |

     |  |         |   |

  |   |     |

Spelling

Lesson 4 - Keywords

Spelling keywords is important. Working on your feedback we will now work on spelling some key words from this unit.

You will write the keywords as they are announced then you will mark them at the end with your green pen.

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

How many did you get?

/ 9

Engage Task

Lesson 5

Big Question: What is a substitutional cipher?

Answer the questions below:

1. Who was the Caesar Cipher named after?
 2. When does the Caesar Cipher date back to?
 3. Which country used the Caesar cipher in 1915?
 4. When was the morse code used?
- 

Homework Tasks

Homework 1

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

Homework Tasks

Homework 2

Homework 2

Due date: _____

Work out the pigpen cipher messages using the key below. Then answer the encrypted question.

1. J VOLFO > LJOF < JFO
 F WOFV FV FFFFOO
 LFFFOF.

2. JOO > FFOO E > FOF
 LFFFOFV < E < WOFV?

Message:

Cipher Key

A	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	Q	R

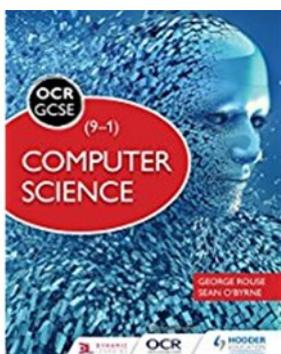
	S	
T		U
	V	

	W	
X		Y
	Z	

Wider Reading List

Wider Reading

- OCR Computer Science for GCSE Student Book
- Explorer Academy: Code Breaking Activity Adventure?



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>

<https://schoolcodebreaking.com/>