CODING CHALLENGE

In this activity, students will take on the roles of cryptanalysts and will learn about coding and different types of cyphers. Once the students break each code, they will be able to create their own encrypted messages.

Mission brief

You are a **cryptanalyst** at Bletchley Park and it is your first day. You are scheduled to receive training on how to decode secret messages before you are able to help decrypt enemy messages.

1

Types of Messages

A **plaintext** message is the message that can be read normally, without need for any decoding. This definition is a plaintext message, because you can read it without having to change the message in any way!

An **encrypted** message or the cipher text is the message we get after applying a process designed to make the message unreadable (called encryption) to those who don't know what process we have used. It normally looks like a random sequence of letters and numbers, with no way of knowing what the intended message was.

2

You might have heard of decryption before, but what does it mean?

Decryption is the process of undoing encryption. We take cipher text and turn it back into a plaintext message, that can be read normally! A cryptanalyst is someone who attempts to decrypt secret messages that have been encrypted by someone else!

3

Did you know?

Bletchley Park is a mansion located in Buckinghamshire and was the main place during WWII where the British government would decode secret intercepted messages from the enemy! The department based there was called the Government Code & Cypher School, which is now called Government Communications Headquarters (GCHQ), based in Cheltenham. Bletchley Park was a huge employer of women during WWII with over 8,000 women! One of these women, Jane Hughes was based in "Hut 6" of Bletchley Park, which was a decoding room with only women staff. She decoded a message referring to the German battleship Bismarck, which included its current location and destination. This led the Royal Navy to sink the Bismarck on 27th May 1941!

4

ATBASH CIPHER

In this cipher we write the alphabet backwards, and replace A with Z, B with Y, and so on.

Have a go at cracking the message below, and then write a message of your own and see whether a family member or a friend can crack it. Remember you need to tell the recipient that you used this cipher, so that they can work backwards to decrypt your message!

TRY TO DECRYPT THIS MESSAGE:

DVOXLNV GL YOVGXSOVB

DECRYPTED MESSAGE

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

NOW TRY TO ENCRYPT A MESSAGE OF YOUR OWN

_ _

_ _

TIP

Make sure that when you are decrypting a message to use the ciphertext column to find the plaintext letter, and when encrypting a plaintext message, use the plaintext column to find the correct letter to use in your ciphertext.
For example to decrypt the message SR, we look in the cipher text column to find S=H and R=I, and so the message is HI.

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

5 CAESAR CIPHER

This is one of the oldest ciphers around and was used by Julius Caesar himself!

Choose a random letter of the alphabet (except A). This is the start of your new alphabet. If you chose D for example, write D next to A in the box on the left and then continue writing the alphabet downwards from D.

When you decrypt the message you need to know what the start of the alphabet is, so be sure to include this with your message when you write one of your own!

TRY TO DECRYPT THIS MESSAGE (ALPHABET BEGINNING WITH D)

ZSR DW KRPH

DECRYPTED MESSAGE

_ _ _ _ _ _ _   _ _   _ _ _ _ _ _ _ _ _

NOW TRY TO ENCRYPT A MESSAGE OF YOUR OWN (ALPHABET BEGINNING WITH ___)

_ _

_ _

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

6

PLAYFAIR CIPHER

This cipher is different to the ones you did before: it is not a just a case of relabelling the alphabet. Let's go through a worked example!

We start with a square grid and place the alphabet inside. Since the alphabet has one more than 25 letters, we usually just leave the letter j out of the grid. In any message you write use the letter 'i' in place of 'j'. It will be clear to the recipient from the context what the letter should be!

We could use any arrangement of the letters in a square grid, so long as our intended recipient knows which grid we are using!

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

To write your message, break it down into groups of two letters. If you have an odd number of letters, put an extra 'X' on the end of your message. This will be ignored by the recipient when they decode it later!

Let's try to encrypt the message ABORT MISSION to send to a fellow spy.

Our message is now AB OR TM IS SI ON.

If letters are in the same row, like AB, we write each letter as the one shifted to the right, so AB becomes BC. (Note: If we had DE, it would wrap around and become EA).

When the letters are in the same column, we replace each letter with the letter directly below. (For example, MR becomes RW).

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

Now if we want to encrypt any pair of letters that aren't in the same row or column, we form a box with the pair of letters being the corners. For example, if we want to encrypt OR, we form the box on the right, and replace the letters with the furthest away letter in the same row of the box. For example, O becomes M and R becomes T.

We have encrypted OR as MT. Now do this for every pair of letters and we get the encrypted message

BC MT RO HT TH OP

Try to encode HELLO, and the encrypted message you should get is

Plaintext: HE LL OX
Cipher: KC MM NY.

To decode a message, we do the reverse: if letters are in the same row we move to the letter immediately to the left, and if the letters are in the same column, we move to the letter immediately above. For letters that aren't in the same row or column, we still form a box and take the furthest away letter in the same row of the box.

Let's decode the message IK SI BU CZ.

1. I,K are in the same row, so we move one letter back for each of the letters, becoming HI.
2. S,I form a box whose corners are H,I,S,T. We choose the two corners that are n
ot S,I to get HT.
3. Form a box with corners B, U. Opposite to B is E and opposite to U is R. BU becomes ER.
4. Form a box with corners C,Z. Opposite to C is E and opposite Z is X. CZ becomes EX.

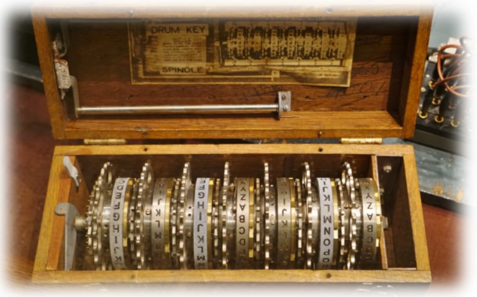
We have decoded the message HI TH ER EX. This says HI THERE, since the X was just in place to make the number of letters in the message an even number.

Interesting Fact:

Alan Turing was a brilliant mathematician. Born in London in 1912. In 1939, Turing took up a full-time role at Bletchley Park.

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.

When he cracked the Enigma code, experts estimate that Alan Turing shortened the war by at least two years. This also meant that cracking the code saved something like 14 million lives.



Source: https://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code (Accessed 20th April 2020)
Source: https://www.factinate.com/things/23-enigmatic-facts-secret-codes-ciphers/ (Accessed 20th April 2020)

TRY TO DECRYPT THIS MESSAGE USING THE GRID OPPOSITE

DN MH QB UQ QF YO PO TX PT SU QB HO HO HK XH PN LM DU CZ

__ __ __ __ __ __ __ __ __ ____ __ __ __
__ __ __ __ __ __

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

NOW TRY TO COME UP WITH A SECRET MESSAGE FOR YOUR FRIENDS OR FAMILY USING THE PLAYFAIR CIPHER! (TIP: Remember when your recipient is deciphering the message, if the letters are in the same row or column, you will need to work backwards.)