Codebreaking, Ciphers and Cryptography

The allies won WWII in 1945 not simply with the bravery of the soldiers on the front line physically fighting the enemy but also with the help of intelligence personnel using their brains here in the UK to decode and intercept crucial information such as battle plans so that we could stay one step ahead of the German forces. This involved spies and double agents (collecting intelligence), mathematicians and computer scientists (creating machines to crack the codes) and linguists (translating between German and English). In the tasks below we will introduce you to a few different types of basic ciphers and you can see if you've got what it would take to help the war effort.

Task 1 – Symbol Substitution Cipher

Each symbol in the ciphertext relates to one letter in the plaintext. The words are all related to WWIIs war effort.

Cipher text	✌	🖐	👆	👎	☞	☞	☝	👆	✋	☺	😐	☹	💣	☠	🚩	🏴	✈	☀	💧	❄	✝	✝	☦	✠	✡	☾
Plain text	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

1. _ _ _ _ _ _ _ _ _ _   _ _ _ _

2. _ _ _ _ _ _ _ _ _ _ _ _ _

3. _ _ _ _   _ _ _ _ _ _ _

4. _ _ _ _ _ _   _ _ _ _ _ _ _ _

5. _ - _ _ _ _

6. _ _ _ _ _

Optional Extra Research Task

Find out more about either:
Bletchley Park and what they did in WWII (especially D-Day) OR some other types of ciphers.

Task 2 – Pigpen Cipher

Each symbol in the ciphertext relates to the location of one letter in the key.
Here you will decode a joke. The first word has been done for you.

Cipher Key:

A	B	C		J•	• K •	L•
D	E	F		M•	• N •	O•
G	H	I		P•	• Q •	R•

H O W
_ _ _   _ _ _   _ _ _ _   _ _ _ _ _
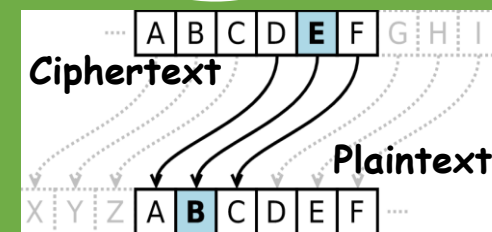
_ _ _ _ _ ?   _ _   _ _ _ _ _ _ _   _ _ _   _ !
?

Task 3 – Caeser Cipher

A Caesar cipher replaces each plaintext letter with a different one a fixed number of places up/down the alphabet. The cipher here uses a left shift of three, so that each occurrence of E in the plaintext becomes B in the ciphertext. Here you will decode another joke. The second word has been done for you.

Zkdw's d pdwkv whdfkhu's idyrxulwh irrg? Wdnhdzdb.

_ _ _ _ ' _   a   _ _ _ _ _   _ _ _ _ _ _ _ ' _ _ _ _ _ _ _ _   _ _ _ _ ?   _ _ _ _ _ _ _ _ .

Ciphertext | **Plaintext**

Extension Tasks – Choose one of the following:

1. Write coded messages for your friends and family to decode. Maybe your name, your hobbies, or a secret message!

2. Try to decode the following joke: **OLMQ NHN QLX YXWU CMP QU QLX XHDLQ? BHAX ZXVQ!**

It is coded with a substitution cipher, where any letter can go to any other letter e.g. A→c, B→p, C→m D→a etc. The following website is a handy tool to help you decode it https://www.cryptoclub.org/#vAllTools. Hints: guess a few common short words (like the, on, etc) or look at the most commonly used letters (google Frequency Analysis for more info!)