CRYPTOLOGY- HOW TO BE A SPY



Throughout history, secret codes have been used to pass messages so the enemy would be none the wiser to your intentions on the battlefield. Julius Caesar, a Roman Emperor, used a simple cypher that replaced letters of the alphabet with other letters by shifting the letters to the right by several spaces. Doing this helped him hide his plans from the enemy, which is vital for the element of surprise and gives him a big advantage in winning a war.

In 1854, Charles Wheatstone used a 5x5 grid to encrypt messages, swapping pairs of letters to hide the real message. It was used by his friend, Lord Lyon Playfair, who championed its use in World War I. This code then became known as the Playfair Code.

During the Second World War, the British used a machine called the Typex (also known as TypeX). The Germans used a machine which sent encrypted messages to each other, called the "Enigma" machine, which the Typex was based upon. The code was transmitted by Morse code. Morse code used electronic signals in the form of dots and dashes to spell letters of the alphabet.

Encryption today is more complex and used in most technologies. From logging into your computer to sending text messages on your mobile phone. Even logging into Roblox and Minecraft uses encryption. Encryption plays an important part in keeping your details and messages safe from code breakers.

ROYAL AIR FORCE museum

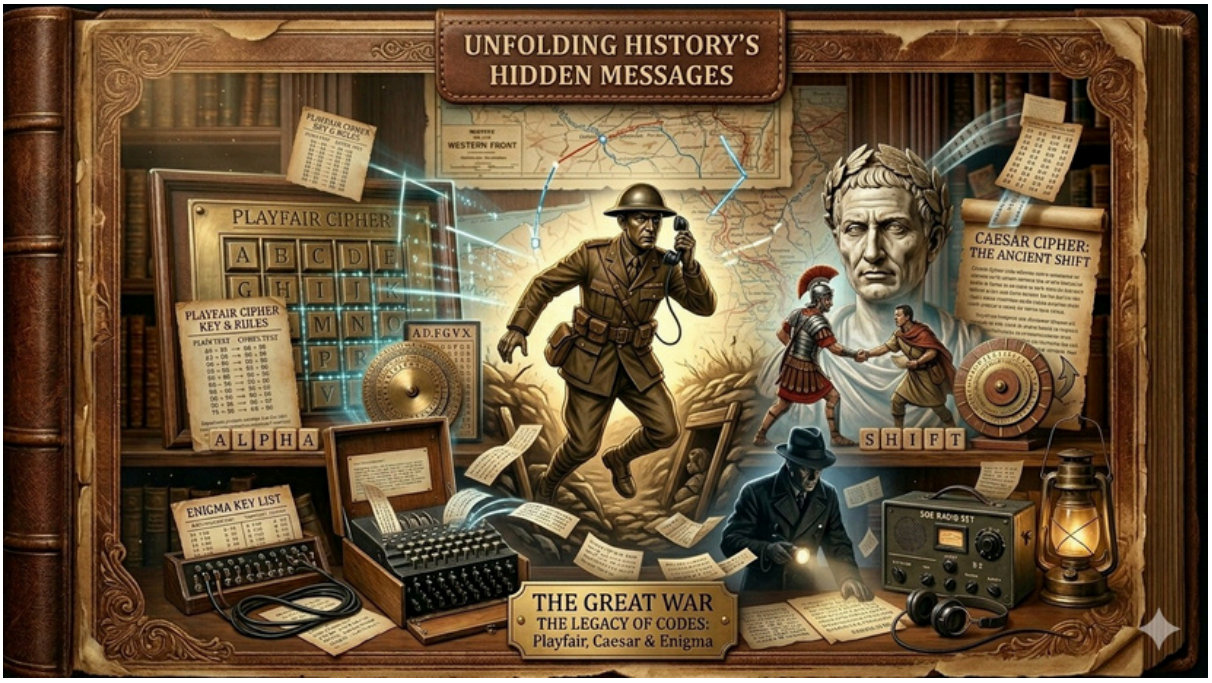
WHAT IS ENCRYPTION?

Encryption is a fancy word that means to jumble up the letters in a message (Encrypted) into a secret code that can only be unjumbled (Deciphered) by someone who knows the code.

Example:

Message: HELLO
Encrypted (Jumbled up): XFMAR
Deciphered (Unjumbled): HELLO

You can use encryption to send messages to your friends without parents and teachers spying on you. Today, we are going to show you how to create your own code using the Caesar, Playfair and Enigma cyphers.



ROYAL AIR FORCE museum



Caesar Cypher

The code works by aligning two alphabets above and below each other; plain text is used for your message, and the cypher text is used to jumble the message (Encryption).
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
Cypher 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

Decide between you and your friend how many spaces you will be moving the cypher text, and keep it secret. Here, I have moved the cypher three spaces to the right. The three spaces are known as the KEY. KEY = 3. Now the cypher alphabet begins with X and ends with W.

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

Let's write a message:

Plain Text: HELLO WORLD
Write down the letter below in the Cypher row. Cypher Text: EBHHL TLOHA

Your friend is given the encrypted message: EBHHL TLOHA

ROYAL AIR FORCE museum

Your friend takes their cypher and does the opposite. Reading the code on the cypher alphabet and reading the plain text alphabet above.

E = H
B = E
H = L
H = L
L = O
T = W
L = O
O = R
H = L
A = D

Deciphered message: HELLO WORLD

If your code is broken, change the key number. Move the cypher line that many spaces to the right and encrypt your new message. Remember to tell your friend the new key number.

ROYAL AIR FORCE museum



Playfair Cypher

The Playfair cypher uses a 5 x 5 grid. Write the alphabet from left to right, moving down a row until the end. Notice a letter is missing. In this case, the letter "J" is missing. This is on purpose. You can leave out any letter you like.

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

ROYAL AIR FORCE museum

Letters are written in pairs. If we have say, G and R, they appear in a column, so we write down the letter next to G in that column. G = M and R = W.

If we have two letters that appear in a row, say, H and K, we write the letters next to them in that row. H = I and K = F

Sometimes letters appear on different rows and columns, like E and T. Now we imagine a square box and where the corners meet opposite to the letters, we will use in our coded message. For example, E = D and T = U.

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

GR	Column	G becomes M	R becomes W
HK	s Rows	H Becomes I	K becomes F
ET	Square	E becomes D	T becomes U

ROYAL AIR FORCE museum

Let's write a message

Message: MEET ME AT NOON

The message is written down in pairs.

For example,

MEET ME AT NOON = ME ET ME AT NO ON

Using the rules and grid above, we now get the encrypted message:

Plain Message: MEETMEATNOON
Encrypted: PBDUPBDQOPPO

But what if we send a single word like "BALLOON"? We can't pair these letters

BA LL OO N

To avoid this, we use a letter that isn't used much. For example, the letter "X". Now we get:

BA LL OO NX

Two matching letters next to each other can make it easy for code breakers to work out an encrypted message. Here we have "LL" and "OO" repeating. Now we replace the second letter with an "X". The Message now reads:

BA LX OX NX

We can now use the rules of the grid and encrypt our message:

Plain Message:
BALXOXNX
Encrypted message:
CBNVNYSX

You can now send your coded messages to your friend if they have the same grid. Using the same rules of the grid, they can decrypt the message. Replacing the "X" becomes obvious once the message is decrypted. If your Grid is discovered, then make a new grid. We use a KEY like in the Caesar cypher. This time we use a word with letters that don't repeat. Like "LIZARD" or "PENCIL". Remember to remove a letter in the alphabet, as we did earlier with the letter "J". Here is the new grid. I have highlighted the KEY as an example:

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

ROYAL AIR FORCE museum



Enigma Machine Cypher

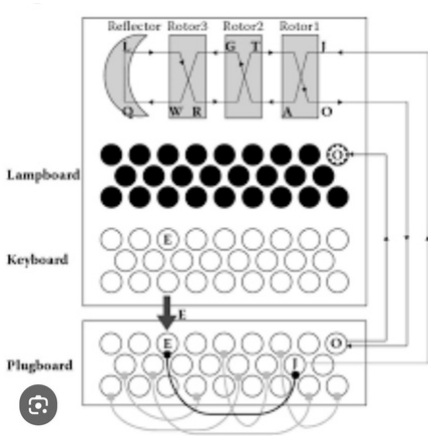


Military Model Enigma I, in use from 1930

The Enigma machine is very complicated to explain and could make over 150 quintillion combinations of encrypted code. That is 158,962,555,217,826,360,000 or 150 million million million combinations.

Each day the combination would change making it very difficult for code breakers.

ROYAL AIR FORCE museum



It uses a keyboard, a plugboard, a lamp board, three rotors and a reflector.

The person using it would type a letter on the keyboard which would send an electrical current through the plugboard. The plugboard had cables which could change the letter typed in, to another letter. The new letter was then sent to the first rotor.

Each day three rotors out of five were selected to go into the enigma machine. The rotors would have three letters set as the starting combination (KEY). When the keyboard letter was pressed the first rotor would rotate one letter down. The electric current would pass to the next rotor and then to the third rotor. After a full turn of the alphabet on the first rotor,

The second rotor would rotate one letter down. After a full turn of the alphabet on the second rotor, the third rotor would roate a letter down. The current would then go into the reflector. The reflector would change the letter again, back through the third rotor, second and finally the first rotor. This give us eleven different letter changes. The current finally goes to the lampboard. The lampboard lights up the letter used for the encrypted message.

And the process continues until the message is typed out. The code was then sent by Morse code, where the person receiving the morse code, would use the enigma machine to decipher the encrypted message. Their Enigma machine would have the same rotors and Key.

Making Your Own Enigma Machine

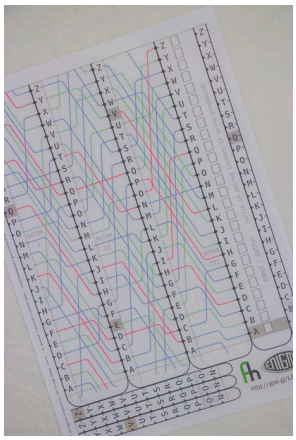
This all sounds very complicated, but we can make a version with a Pringles tube and some pieces of paper.

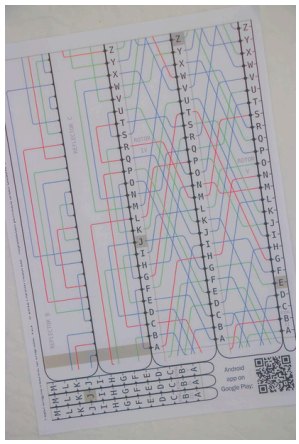
You will need the following:

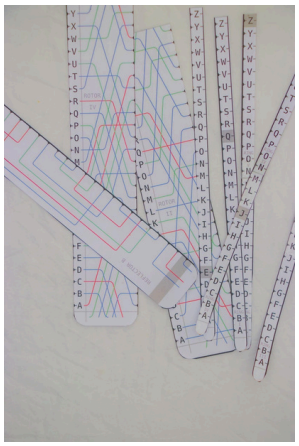
1. Pringles tube (Empty)
2. Sellotape
3. Scissors (Ask an adult to help you) 4. The templates

Step 1.

Cut out the template. These will be your keyboard, five rotors, two reflectors and some smaller rotors.







Step 2.

Select three rotors, one reflector and the keyboard.

Step 3.

Wrap the reflector around the base of the Pringles tube and Sellotape the ends together. It is best to secure this to the tube for ease of use.

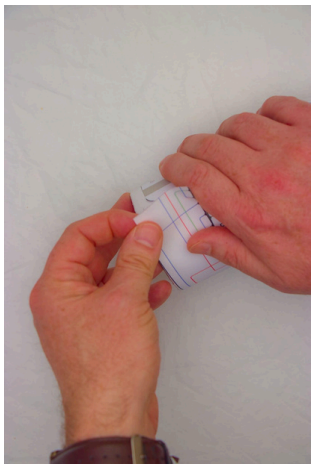
Step 4.

In the same way, wrap the rotor next to the Reflector and Sellotape the ends together. Repeat for the next two rotors, all positioned adjacent to each other.

ROYAL AIR FORCE museum

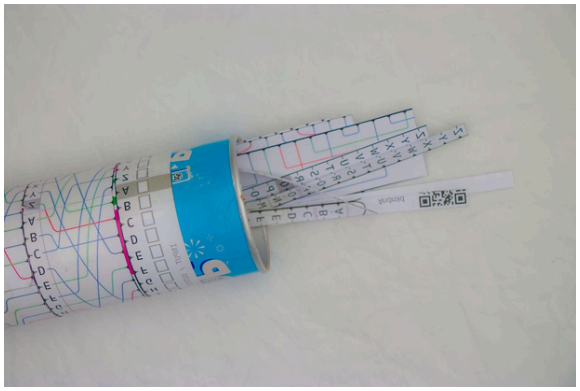
Step 5.

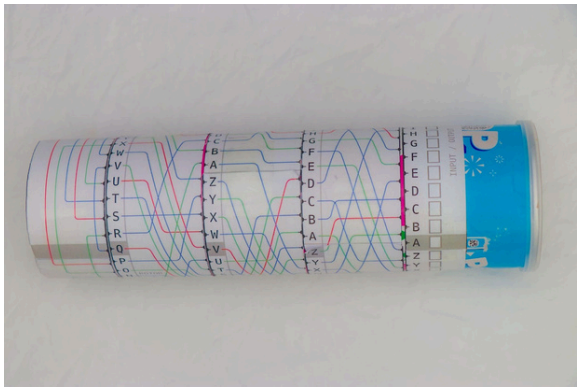
Again, wrap the input board around the Pringles tube and Sellotape the ends. Position it adjacent to the last rotor. IMPORTANT: Secure this down for ease of use, but make sure the grey letter is lined up with the grey letter on the reflector.



Step 6.

Allother pieces go inside the Pringles tube for safekeeping if you want to swap the Rotors or Reflector. In some cases, you may just want to replace the Rotors letter where the grey letter isaltered. For now, just store them in the Pringles tube.





How to Use the Pringles Enigma Machine

Hopefully, your friend has also made the same Pringles Enigma machine with the same Reflector, Rotors and KEY.

ROYAL AIR FORCE museum

Step 1.

You and your friend must have the grey letters all lined up. One of you chooses three letters. Let's say, “B”, “A”, “G”. Turn the rotors so they align from left to right with the grey letter on
the reflector and the keyboard.
KEY = BAG.

Step 2.

In this example, I am using ROTORS I, III and V, and Reflector C.

Plain Message: SPITFIRE

Step 3.

*****Turn Rotor V downwards one letter.**

Find the “S” on the input board. Follow the blue line to the letter “K”.
Follow the letter “K” (Rotor V). Follow the red line to the letter “H”.
Follow the letter “H” (Rotor III). Follow the green line to the letter “V”.
Follow the letter “V” (Rotor I).
Follow the blue line (Reflector C) to the letter “T” (Rotor I).
Follow the letter “T”, blue line to letter “K” (Rotor III).
Follow the letter “K”, green line to letter “B” (Rotor I).
Follow the letter “B”, blue line to letter “V” (Input board).
Now your first letter “S” is encrypted; letter “V”.

Plain Message: SPITFIRE
Encrypted Text: V

Step 4.

Repeat from ***** We turn Rotor V downwards one letter** for each letter of the Plain text. Each time, the letters will be different. Be careful to follow the lines.

If the rotors show a grey letter, the next rotor to the left needs to rotate one letter downwards before encrypting the letter.

Plain Message: SPITFIRE
Encrypted Text:
VZDZGPOI

ROYAL AIR FORCE museum

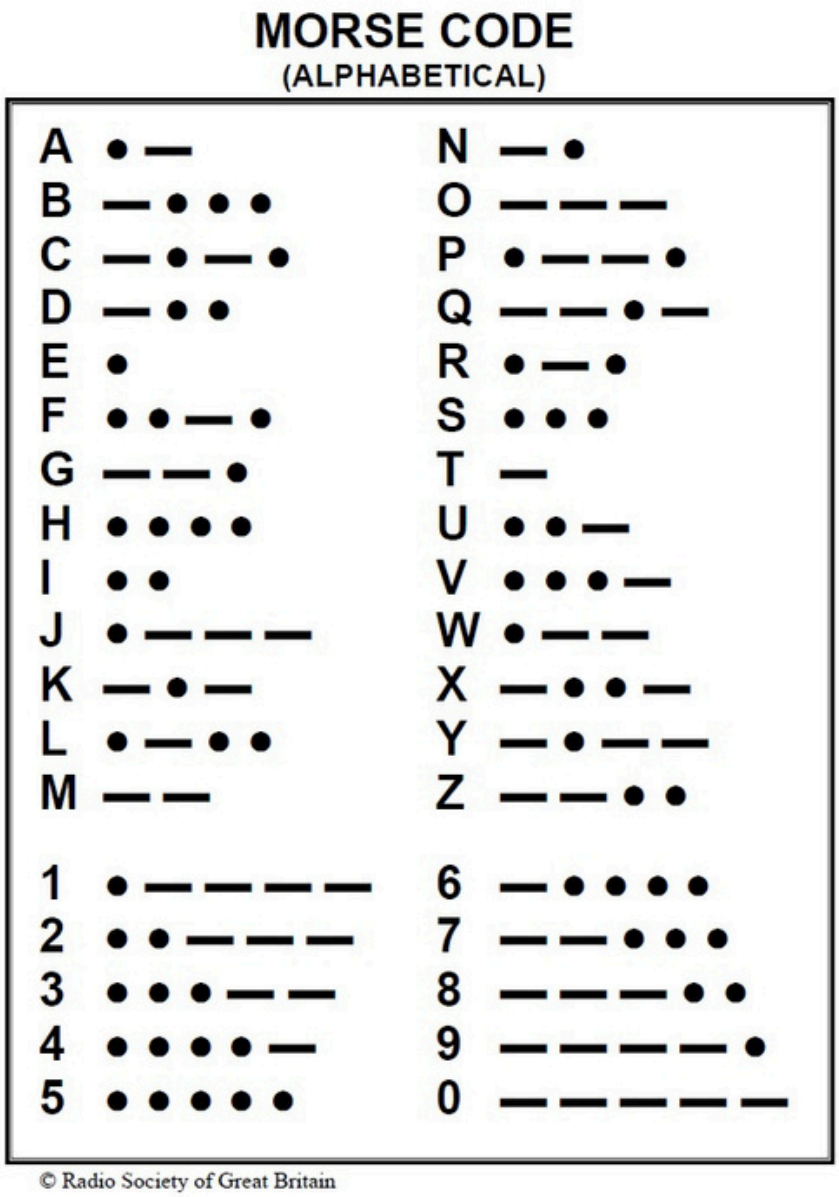
Final Check:

Check your encrypted text by resetting your enigma machine and setting the KEY again to “B”, “A”, “G”. Follow the same steps but input the encrypted message. You shoul get the following:

Encrypted Text received: V Z D Z G P O I
Decrypted Message: S P I T F I R E

Morse Code

The encrypted messages would be sent by Morse Code. Signals were sent with dots and dashes. Here is the Morse code alphabet.



ROYAL AIR FORCE museum