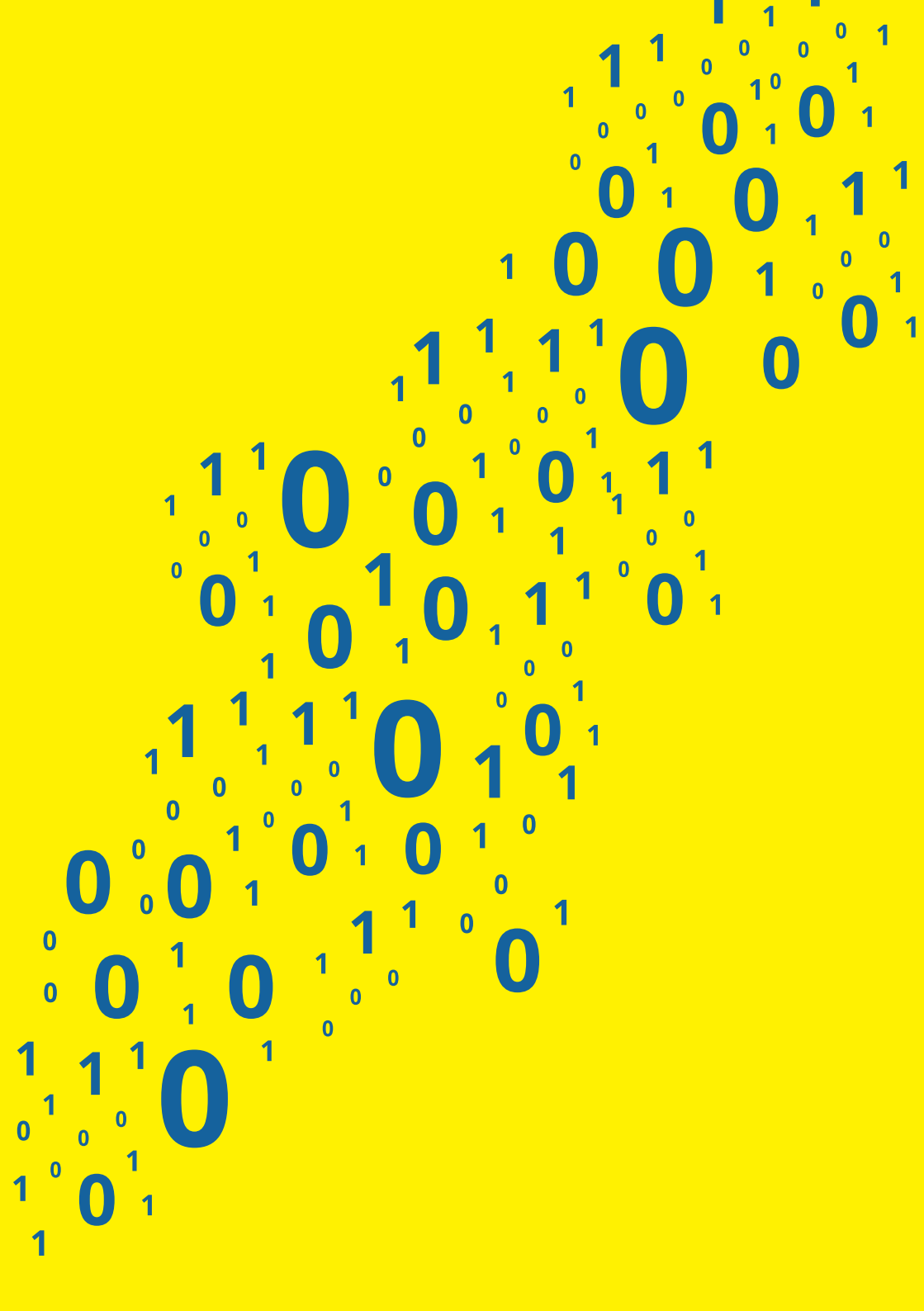
Amiosec

Decode_

PERPLEXING PUZZLES FOR CURIOUS CODEBREAKERS



Decode_

The land of Cyber is huge, fascinating and always growing – just like the amount of information in the world. How do we keep that information safe?

Many top secret keepers would use something called ‘cryptography’ – but what is this?

Simply put, cryptography is a method of protecting secrets by using codes and ciphers.

While people have been using cryptography as far back as ancient Egypt, in today’s digital world our methods of protection and encryption have evolved massively.

Take a trip through time with our curious codebreaker puzzles and see if you can decode our secret messages using some classic cryptography methods.

Difficulty: Easy

Caesar cipher

THE YEAR IS 100 BC...

One of the most famous historical ciphers is a **Caesar cipher**, named after the Roman general **Julius Caesar**.

This type of cipher shifts letters in the alphabet to make our secret message (known as plaintext) unreadable.

Here's an example:

Let's say our plaintext says **'hello world'** and our **shift is 4:**

'H' shifts 4 places I J K (L) The letter 'H' becomes 'L'.
+1 +2 +3 +4

Apply this across all our letters and our encoded message (known as ciphertext) is:

'lipps asvph'

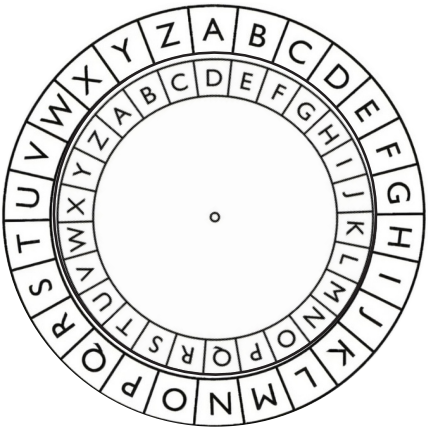
Hmmm... but our original message (our plaintext) could also be shifted 4 letters in the other direction:

What if 'H' shifts back 4 places instead? G F E (D)
-1 -2 - 3 -4

This means the ciphertext could also be 'dahhk sknhz'.

How could someone solve this without the direction???

Using a **Caesar cipher wheel**, a decoder could try various shifts to see which one gives an understandable message.



For long messages the shift could be worked out using 'frequency analysis', where we look at how often certain letters appear in the plaintext language (e.g. English), and compare it to the frequency of the letters in the ciphertext.

See if you can figure out the secret message below. The shift is 3, but is it a shift forward or backward...?

M	X	O	L	X	V		F	D	H	V	D	U		X	V	H	G
D		V	K	L	I	W		R	I		W	K	U	H	H		
W	R		N	H	H	S		K	L	V							
P	H	V	V	D	J	H	V		V	H	F	U	H	W			

Difficulty: Medium

Polyalphabetic cipher

WELCOME TO THE 15th CENTURY...

A polyalphabetic cipher could be seen as an extension of the Caesar cipher – it combines various elements from different substitution alphabets. This type of cipher was essentially a cryptographer's solution to frequency analysis. It is very hard to break since there is a lack of recurring pattern.

The most famous example of this is the **Vigenère cipher**. Here, **each letter** of the plaintext is encoded with a **different** Caesar cipher. The shift for each letter is predetermined by a shared **secret keyword**.

Here's an example:

Our shared secret keyword is **'LEMON'.**
Each letter of 'lemon' determines its own shift.

Let's say we want to secretly code a message:

'Attack at dawn'

Counting from the letter 'A', 'L' is 11 letters away.
This means our shift on the first letter of the message is 11.
'T' is 15 letters from 'E', so the shift on the second letter is 15.
The same theory is applied to the 'M', the 'O' and the 'N'

'Attack at dawn' is longer than the word 'lemon' so we would need to **repeat the phrase** 'lemon' as needed.

For ease, we can use something called a **Tabula Recta**, or a **Vigenère square**.

Our first letter, A , will be paired with the column L (so A gets shifted by 11, to L) and that letter becomes the ciphertext letter. We repeat this until all the letters have been substituted.

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

Can you use our Vigenère square above to encrypt 'attack at dawn' into ciphertext using the keyword 'lemon' below?

Plaintext:	A	T	T	A	C	K	A	T	D	A	W	N		
Keyword:	L	E	M	O	N	L	E	M	O	N	L	E		
Ciphertext:														

Difficulty: Medium

Morse code

THE 1830's CALLED... THEY WANT THEIR CODE BACK...

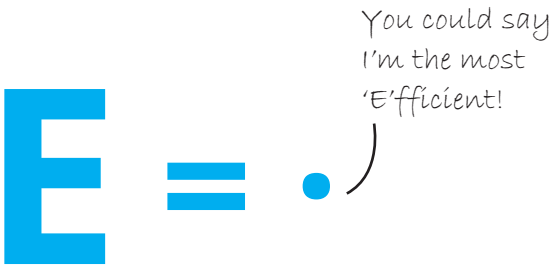
Morse code is another very famous code.

Each letter is assigned a combination of **short 'dots' and longer 'dashes'** (. and -) so that messages can be encoded and sent via **telecommunications** such as radio using **beeps and tones**. It can even be communicated with long and short **flashes of light!**

Did you know...?

Morse code was originally **designed to increase efficiency**, so that the length of each symbol was fairly matched to how often its letter appears in the English language.

For example, the letter **E is the most common letter** in the English language. In morse code it is encoded as **one single short dot** to make it **less hard work** to encode and to decode too.



Below is a guide to international morse code:

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

See if you can decode the secret messages below:

- •••• • / •• –• ••–• • –• - ––– •–• / ––– •–•• /

__ __ __ __ __ __ __ __ __ __ __ __ __ __

–– ––– •–• ••• • / –•–• ––– •–• • / ••– •– ••• / •– /

__ __ __ __ __ __ __ __ __ __ __ __ __ __

•––• •– •• –• - • •–•

__ __ __ __ __ __ __

–– ––– •–• ••• • / –•–• ––– •–• • / ••– •– ••• / - •••• • /

__ __ __ __ __ __ __ __ __ __ __ __ __ __ __

•–•• •• •–• ••• - / - • –•• - - / –– • ••• ••• •– ––• •

__ __ __ __ __ __ __ __ __ __ __ __ __ __ __

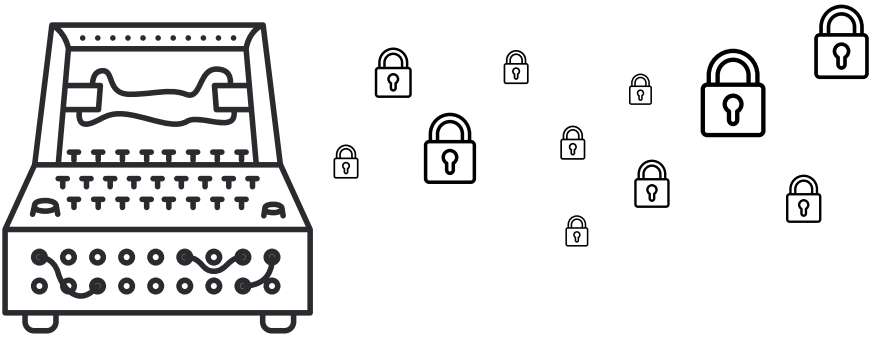
The Enigma Code

WE'VE REACHED THE 1930'S

The **Enigma machine** was developed towards the end of World War One and widely used throughout World War Two by Nazi Germany...

...but what is it?

Essentially it was a very 'fancy' and **sophisticated polyalphabetic cipher**. Some people believed it to be so secure that it could protect even the most secret of messages.



However, when many Nazi **cryptographers** were caught after the war, they expressed that they knew Enigma was not "unbreakable", but did **not believe** anyone would go through the immense effort of **breaking** it...

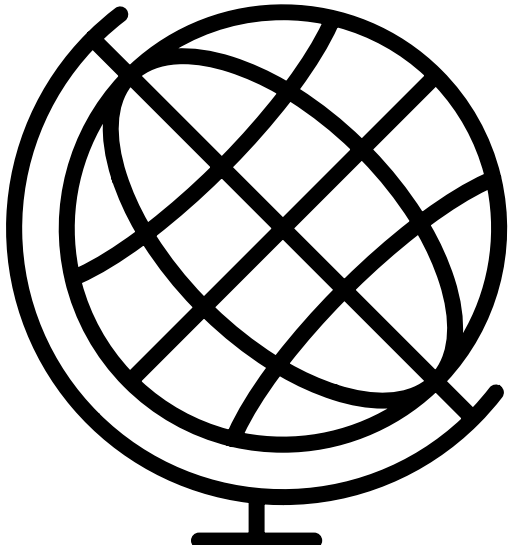
They were very wrong!

Enigma was first broken by Polish mathematician **Marian Rejewski** in around 1932. As the likelihood of war approached, he went on to **share** what he had developed with the **British and French intelligence services**.

It is widely accepted that the majority of the codebreaking was done by Polish cryptographers such as Rejewski, as well as **Alan Turing** and his team at **Bletchley Park**. This breakthrough was an amazing feat for the allies against the Nazis, despite the fact that the break into Enigma was kept secret until 1974.

Why is this such an important part of the history of cryptography?

Firstly, it was a significant step towards the **defeat of the Nazis** during World War 2, but also, due to its **importance and impact around the globe**, the general public saw how important cryptography and cryptanalysis (the breaking of cryptosystems) are to the world.



Protecting information today

WE'VE RETURNED TO THE 2020's

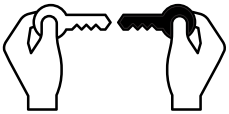
Making and breaking codes and cryptosystems has been around for thousands of years, and will continue to be around for many more. It plays a crucial part in protecting our way of life.

In today's **digital age**, this is more important than ever, and the methods of encryption we use are more advanced than those we've explored throughout our puzzles and challenges. From protecting credit **card transactions**, to **protecting messages** sent over public networks, there is an encryption method out there for **everything!**

Some of today's common ciphers and cryptosystems are:

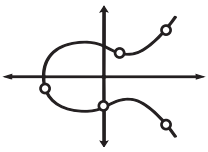
AES

A symmetric block cipher, so data can be encrypted and decrypted the same way



RSA

A public-key cryptosystem, using both a public key and (secret) private key



ECC

Based on elliptical curves, ECC is like having a very strong lock that's hard to break

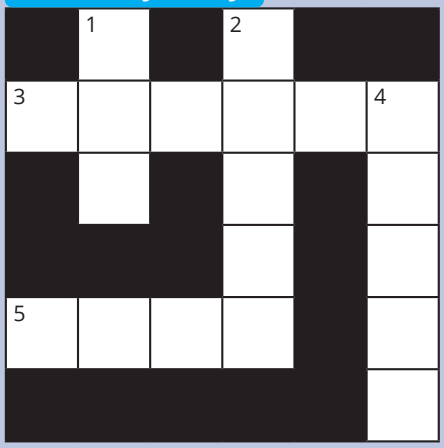
There are many other cryptosystems out there being used and new ones being developed every day!

Cyber Crosswords

We've cracked codes, we've encoded secret messages and we've learned about encryption through the ages.

Can you now put your puzzle-busting pens to paper and take on our Cyber Crosswords?

Difficulty: Easy



Across

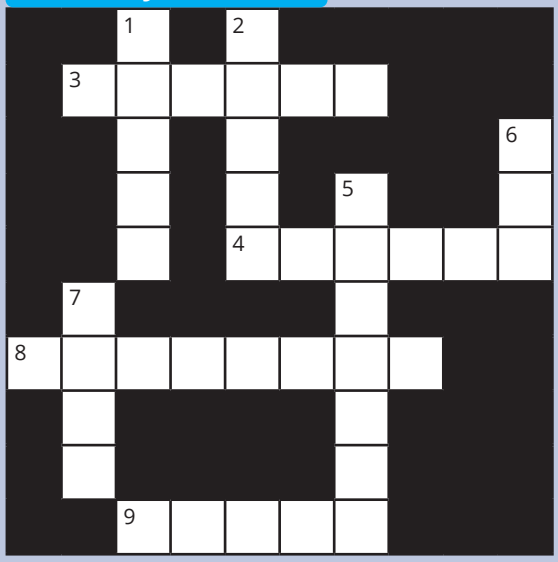
3. Apple's mobile phone
5. Tall plant with a trunk

Down

1. Gorilla; an animal similar to humans
2. Computer item; a rodent
4. The planet that we live on

Cyber Crosswords

Difficulty: Medium



Across

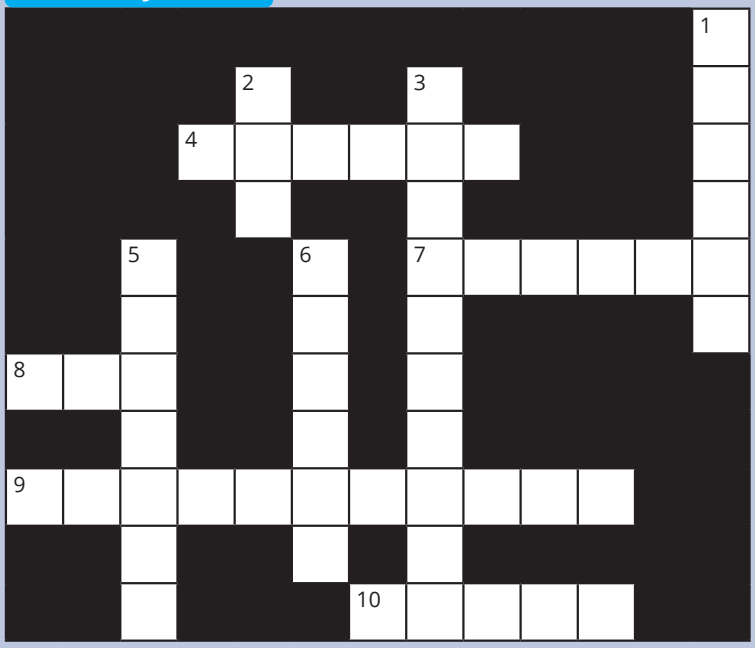
3. 01100010 01101001 01101110 01100001 01110010 01111001 ; a collection of 1s and 0s (6)
4. Something to be kept hidden or private (6)
8. A device for working with information; common electronic machine (8)
9. Item to move your cursor on screen (5)

Down

1. A square on a screen of an image (5)
2. The M in STEM (5)
5. The first letter of STEM (7)
6 . A basic unit of information; binary integer (3)
7. A programmer writes _____ (4)

Cyber Crosswords

Difficulty: Hard



Across

4. Kept secret (6)
7. A person who wants to break into a system (6)
8. A digital error (3)
9. The roadmap connecting all computer components (11)
10. Related to computers and technology (5)

Down

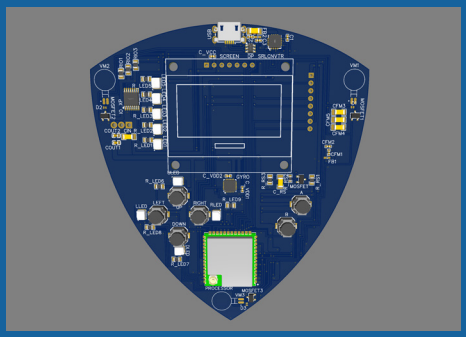
1. Information storage (6)
2. Binary integer (3)
3. Knowledge, equipment, and methods that are used in science and industry (10)
5. Processes data in the form of numbers (7)
6. Base 2 (6)

Amiosec Challenge Board

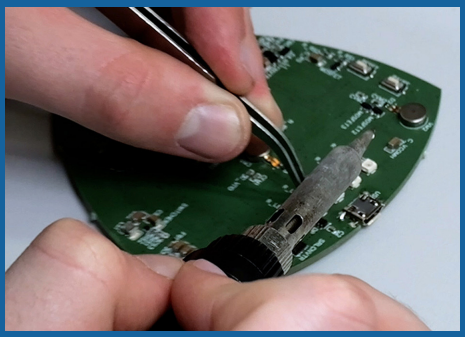
FROM CODEBREAKING TO GAME MAKING

Coding isn't just used for protecting data, it can be used to build software - even computer games! Read on to find out how our talented team of apprentices designed, developed and built the **Amiosec Challenge Board...**

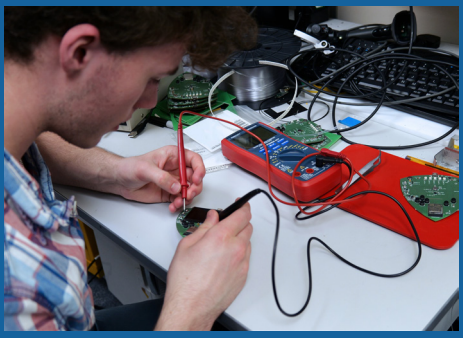
Our apprentices joined Amiosec in September 2023 and within the first few weeks were assigned the task to **create a gaming device** for Cheltenham Science Festival...



The first thing to do was **design the hardware** and case, then research and decide what games and challenges would be programmed...



Once the design for the **Hardware PCB** (Printed Circuit Board) was complete, the boards were ordered and **components were soldered** into place...



After all of the components had been soldered on, it was time to grab a mutlimeter and **start testing** each of the challenge boards...

In the meantime, **software development** was ongoing; creating new games, a scoreboard and title screens for all of the challenges.

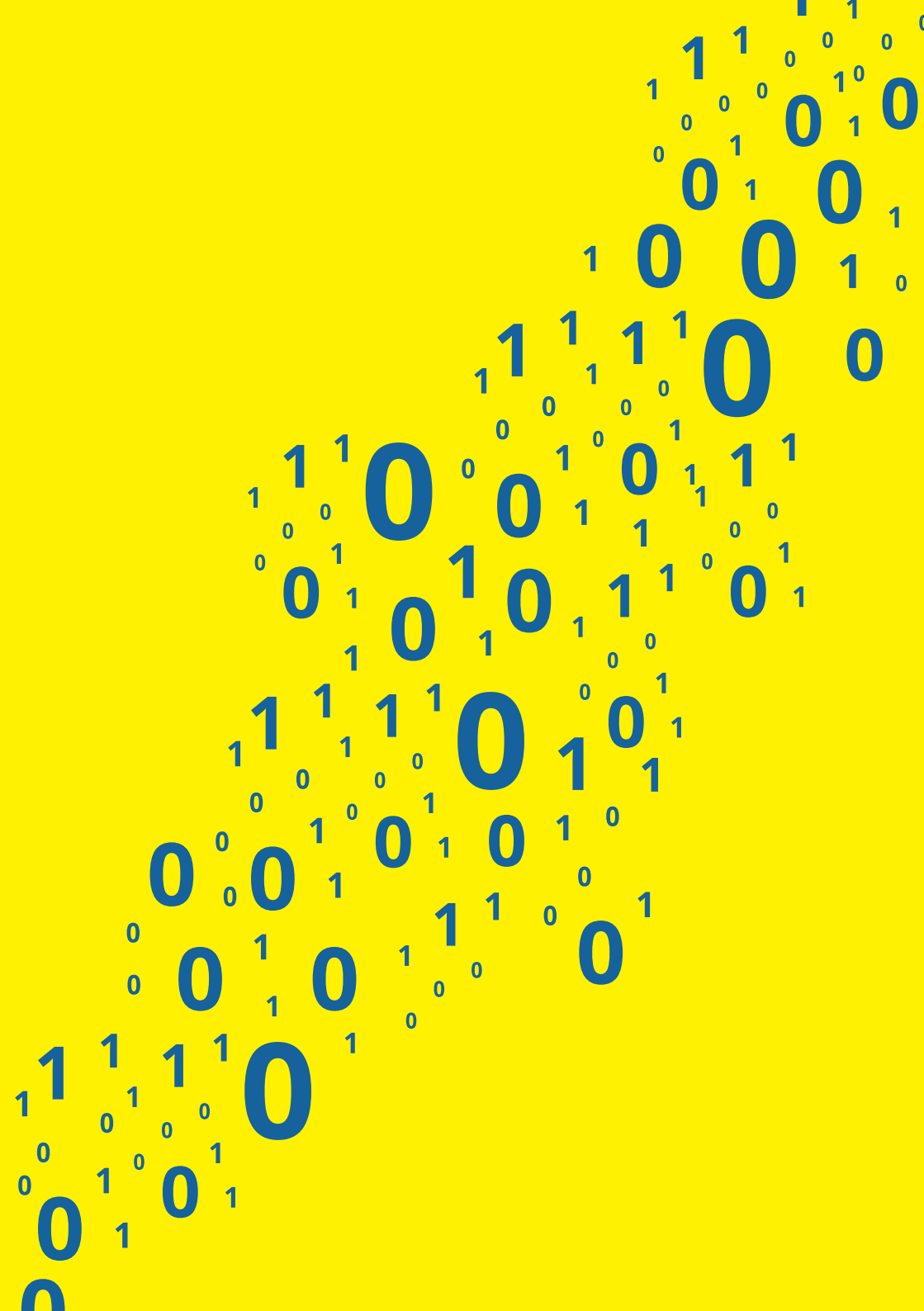
The apprentices learnt a lot during this seven month project and were **incredibly proud** to showcase their final Challenge Boards at **Cheltenham Science Festival!**

Amiosec

Amiosec is an exciting and growing technology company headquartered in Tewkesbury, Gloucestershire, with a vision to focus on research and development of new technologies that enable secure communications.

We are passionate and committed to growing new talent within cyber security. As such, we run an apprenticeship and graduate scheme, and have an active STEM outreach programme, collaborating with schools, universities and the NCSC CyberFirst program.

Please feel free to get in touch and find out more about what we do as a business: www.amiosec.com



Decode: Perplexing puzzles for curious codebreakers
05/2024