

# An Introduction to Cryptography

With Max and Freddie

Have a look at the starter activity on your sheet  
while you wait for others to arrive.



**The Royal Institution**  
Science Lives Here

# Starter Activity

What letter of the alphabet is the one which comes eight letters before the letter which comes five letters after the fourth appearance of the first letter to occur four times in this sentence?

**Work backwards**

# Starter Activity

What letter of the alphabet is the one which comes eight letters before the letter which comes five letters after the fourth appearance of the first letter to occur four times in this sentence?

# Starter Activity

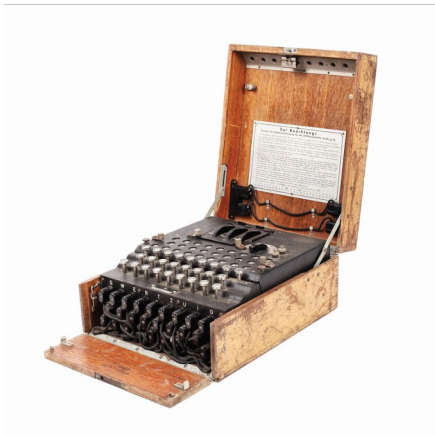
What letter of the alphabet is the one which comes eight letters before the letter which comes five letters after the fourth appearance of the first letter to occur four times in this sentence?

# Starter Activity

What letter **R** of the alphabet is the one which comes eight letters before the letter which comes five letters after the fourth appearance of the first letter to occur four times in this sentence?

The answer is **R**

# A Bit of Background...



# Caesar Cipher



If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others.

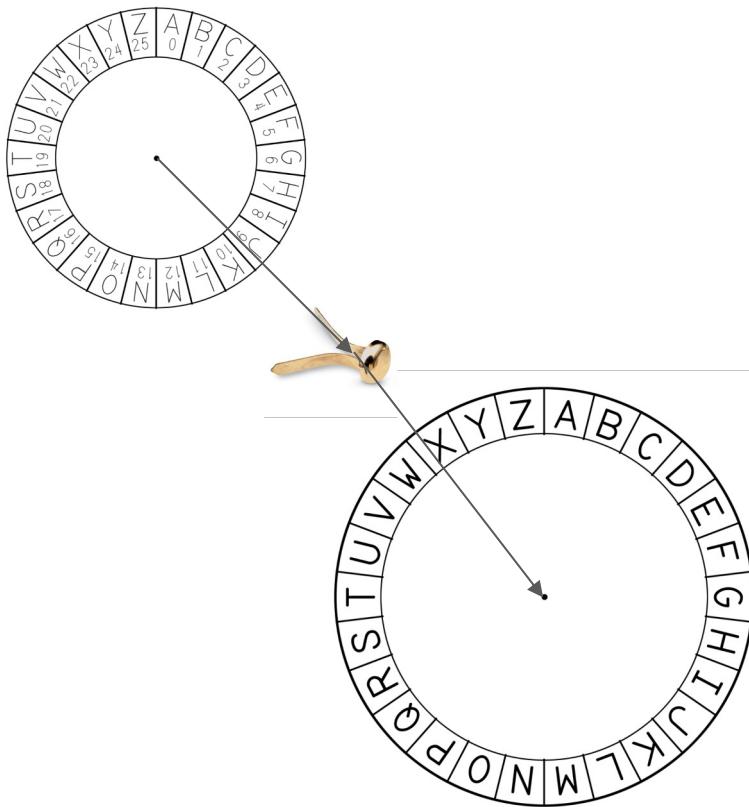
# Caesar Cipher

## Task 1 - Caesar Cipher

Fgct Eqnngciwg,

K owuv yctp aqw vjcv...

Use your cipher wheel to help you.





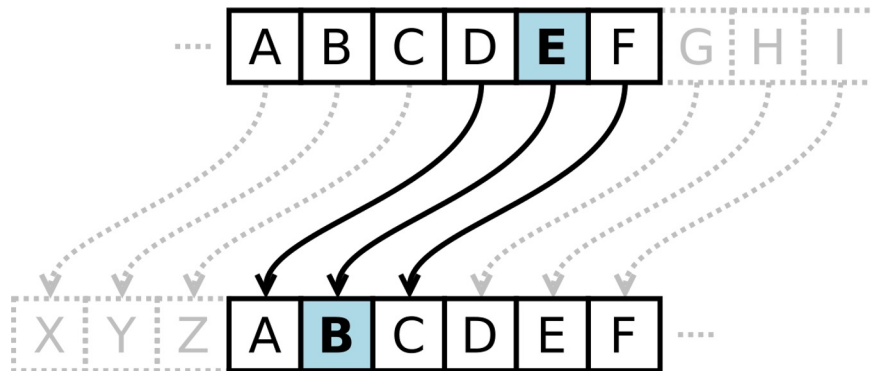
# Caesar Cipher

## Task 1 - Caesar Cipher

Dear Colleague,

I must warn you that...

What did we do with the wheel to allow us to read the message?



# Caesar Cipher Advantages and Disadvantages

What immediate good things do you notice about the cipher and what bad things can you think of when using a Caesar Cipher?

**Advantages**

**Disadvantages**

# Caesar Cipher Advantages and Disadvantages

What immediate good things do you notice about the cipher and what bad things can you think of when using a Caesar Cipher?

## Advantages

Easy to Encrypt/Decrypt

Not immediately readable

Reliable

Used for a long period of time

Easy for a computer to process

## Disadvantages

Easy for an attacker to decrypt

Very basic security

Easy to spot

Can be cracked very quickly by a computer

# Mathematics behind the Ceasar Cipher

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z				
21	22	23	24	25	26				

If we assign a number to each letter, we can then add to each number our **shift**. But what happens when the number sums to beyond 26?!

## A Problem...

It seems common sense to us that after 26 we should just subtract 26 to go back to 1.

We could write this as:

When **shiftednumber** > **26** then we must subtract **26** from **shiftednumber** to make a new **shiftednumber**

The > < <= >= notation is called **inequality**

However there is another way, what happens for example if we go beyond **52** (not that it is possible but let's say it is)

# Modulus

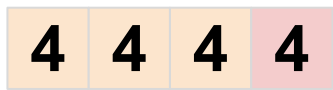
In computing we use the



Sign to indicate mod (modulus)

E.g.  $5 \% 2$  would give 1

**$15 \% 4$**



4    8    12    **16**

$$15 - 12 = 3$$

Here is the result of modulating multiple terms, can you work out what the modulus function does?

$$14 \% 7 = 0$$

$$15 \% 7 = 1$$

$$66 \% 8 = 2$$

$$8 \% 3 = 2$$

The modulus sign means **divide** by and find the **remainder** of.

**So for example  $15 \% 4$ :**

We see how many 4s we can fit into 15.

We realise that 12 is the biggest number before 15 that we can fit 4s into.

Therefore we work out how many units we have to move to 15 and call this the remainder (3).

# Where else do we see Modulus?

We use Modulus without even knowing it when reading 24 hour time.

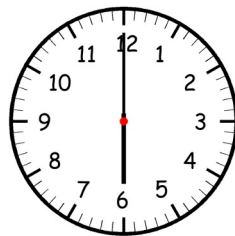
We read clocks in 12 hour cycles, however as there are 24 hours in a day we use 24 hour time to show this.

E.g.

$$16 \% 12 = 4$$

$$22 \% 12 = 10$$

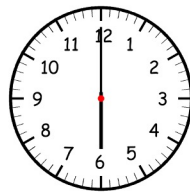
$$18 \% 12 = 6$$



18:00:00

Angle H: 0.0  
Angle M: 180.0

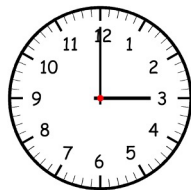
This image was generated at: 2020-01-12 16:34:23 207641



06:00:00

Angle H: 0.0  
Angle M: 180.0

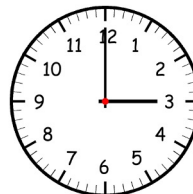
This image was generated at: 2020-01-12 16:34:40 803575



03:00:00

Angle H: 0.0  
Angle M: 90.0

This image was generated at: 2020-01-12 16:35:11 017106



15:00:00

Angle H: 0.0  
Angle M: 90.0

This image was generated at: 2020-01-12 16:35:37 802642

## Clock Math

The sneaky thing about modular math is we've already been using it for keeping time — sometimes called “clock arithmetic”.

For example: it's 7:00 (am/pm doesn't matter). Where will the hour hand be in 7 hours?

Hrm.  $7 + 7 = 14$ , but we can't show “14:00” on a clock. So it must be 2. We do this reasoning intuitively, and in math terms:

- $(7 + 7) \bmod 12 = (14) \bmod 12 = 2 \bmod 12$  [2 is the remainder when 14 is divided by 12]

The equation “ $14 \bmod 12 = 2 \bmod 12$ ” means, “14 o'clock” and “2 o'clock” look the same on a 12-hour clock. They are **congruent**, indicated by a triple-equals sign:  $14 \equiv 2 \bmod 12$ .

Another example: it's 8:00. Where will the big hand be in 25 hours?

Instead of adding 25 to 8, you might realize that 25 hours is just “1 day + 1 hour”. So, the clock will end up 1 hour ahead, at 9:00.

- $(8 + 25) \bmod 12 \equiv (8) \bmod 12 + (25) \bmod 12 \equiv (8) \bmod 12 + (1) \bmod 12 \equiv 9 \bmod 12$

You intuitively converted 25 to 1, and added that to 8.



# Modulus

We can use the modulus to work out which alphabetical character we are referring to after 26

15	15
16	16
17	17
18	18
19	19
20	20
21	21
22	22
23	23
24	24
25	25
26	0
27	1
28	2
29	3
30	4

Modulus is used a lot in advanced cryptography.

**Complete Task 2 on your Worksheet.**

# Checksums

Checksums are used within Cryptography and in all aspects of computing heavily.

They use a mathematical formula to work out whether an item is valid or invalid.

For example, if you were to send a document you might enclose the checksum separately to allow the sender to ensure the file has not been tampered with!

There are lots of different types of checksum such as md5 (although it has some issues), SHA-2, CRC32.

# Hashing

The checksums mentioned towards the bottom of the previous page like MD5 are all examples of a hash.

A hash is a supposedly **irreversible** operation that relies heavily on **prime numbers**.

Some hashes have been broken due to a 'high collision rate'

They are often used to check something has not been tampered with.

For example the md5 for this slide is:

**649595585cdcdb8d35d7996331362f9c**

# Hashing

The checksums mentioned towards the bottom of the previous page like MD5 are all examples of a hash.

A hash is a supposedly **irreversible** operation that relies heavily on **prime numbers**.

Some hashes have been broken due to a 'high collision rate'

They are often used to check something has not been tampered with.

For example the md5 for this slide is:

**558699c045bf48e561706316b1e33226**

Hashing - Even the slightest changes modify the hash

The checksums mentioned towards the bottom of the previous page like MD5 are all examples of a hash.

A hash is a supposedly **irreversible** operation that relies heavily on **prime numbers**.

Some hashes have been broken due to a 'high collision rate'

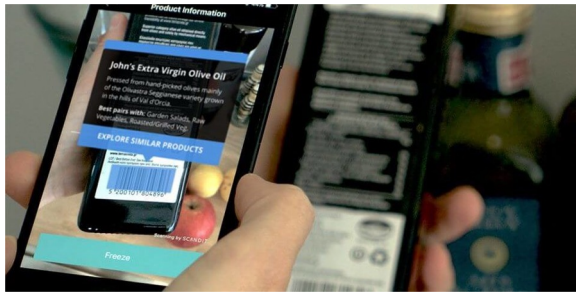
They are often used to check something has not been tampered with.

For example the md5 for this slide is:

**558699c045bf48e561706316b1e33226**

Let's have a go at validating our own checksum

**Universal Product Code** (UPC) is used massively across the world. It is the standard barcode used for most retail products which means it is vital that there is some kind of checksum for computers to be able to check they have read a barcode correctly.



Let's have a go at validating our own checksum

### **Complete Task 3 on your Worksheet.**

A company has received a batch of electronics parts for the construction of their new mobile phone however they believe a saboteur has tampered with the production line and added fake parts to the production line.

Apparently the saboteur was in too much of a rush to use valid UPC codes. Can you work out which shipments are planted?



UPC	VALID?
036000291452	VALID
075678164125	VALID
012345678905	VALID
823910941850	INVALID
075678164125	VALID
012345678905	VALID
101010101010	INVALID
321951240248	INVALID
786485093088	VALID
011200296908	INVALID
614141003747	VALID
043000181706	VALID
860002973708	VALID
952883929002	INVALID
184295923941	INVALID
820023900295	INVALID
828805829900	INVALID



# Signature Checking with Checksums

Why might signature checking be useful?

Governments and Military plus most of the internet relies heavily on good signature checking. Whenever you visit a page on the internet your page is verified using a complex checking algorithm called **HTTPS** that relies on **Public Key Cryptography**.

Talking on Governments, there is a lot of controversy on the wide availability of military encryption and whether they should be allowed to have a backdoor.

# Australia data encryption laws explained

🕒 7 December 2018



GETTY IMAGES

Australian police can now order tech firms to access the encrypted messages of suspects

**Australia has passed controversial laws designed to compel technology companies to grant police and security agencies access to encrypted messages.**

# Affine Cipher

This is another way to encrypt a cipher. Can you notice how it works?

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

# Affine Cipher

This is another way to encrypt a cipher. Can you notice how it works?

What if I highlight A, B and C?

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

# Affine Cipher

The affine cipher works by placing the letter A in a place in the alphabet and then placing the letters afterwards a set number of places after. Eg. every three letters.

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

# Let's try one

Umx nvj wzlaxs vexk umx lvvq.

Do you notice that umx comes up twice?

What word in English could this be?

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

# Let's try one

Umx nvj wzlaxs vexk umx lvvq.

Do you notice that umx comes up twice?

What word in English could this be?

How many spaces are there between E and H in the English alphabet and also in our table?

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

# Let's try one

Umx nvj wzlaxs vexk umx lvvq.

Do you notice that umx comes up twice?

What word in English could this be?

How many spaces are there between E and H in the English alphabet and also in our table?

$$15 / 3 = 5$$

Ciphertext	Plaintext	Ciphertext	Plaintext
A	3	N	
B	4	O	
C	5	P	
D	6	Q	
E	7	R	
F	8	S	
G	9	T	
H	10	U	T
I	11	V	
J	12	W	
K	13	X	E
L	14	Y	1
M	H	Z	2



# Let's try one

Umx nvj wzlaxs vexk umx lvvq.

Do you notice that umx comes up twice?

What word in English could this be?

How many spaces are there between E and H in the English alphabet and also in our table?

$$15 / 3 = 5$$

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

# Let's try one

Umx nvj wzlaxs vexk umx lvvq.

Do you notice that umx comes up twice?

What word in English could this be?

How many spaces are there between E and H in the English alphabet and also in our table?

$$15 / 3 = 5$$

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

# Let's try one

Umx nvj wzlaxs vexk umx lvvq.

Do you notice that umx comes up twice?

What word in English could this be?

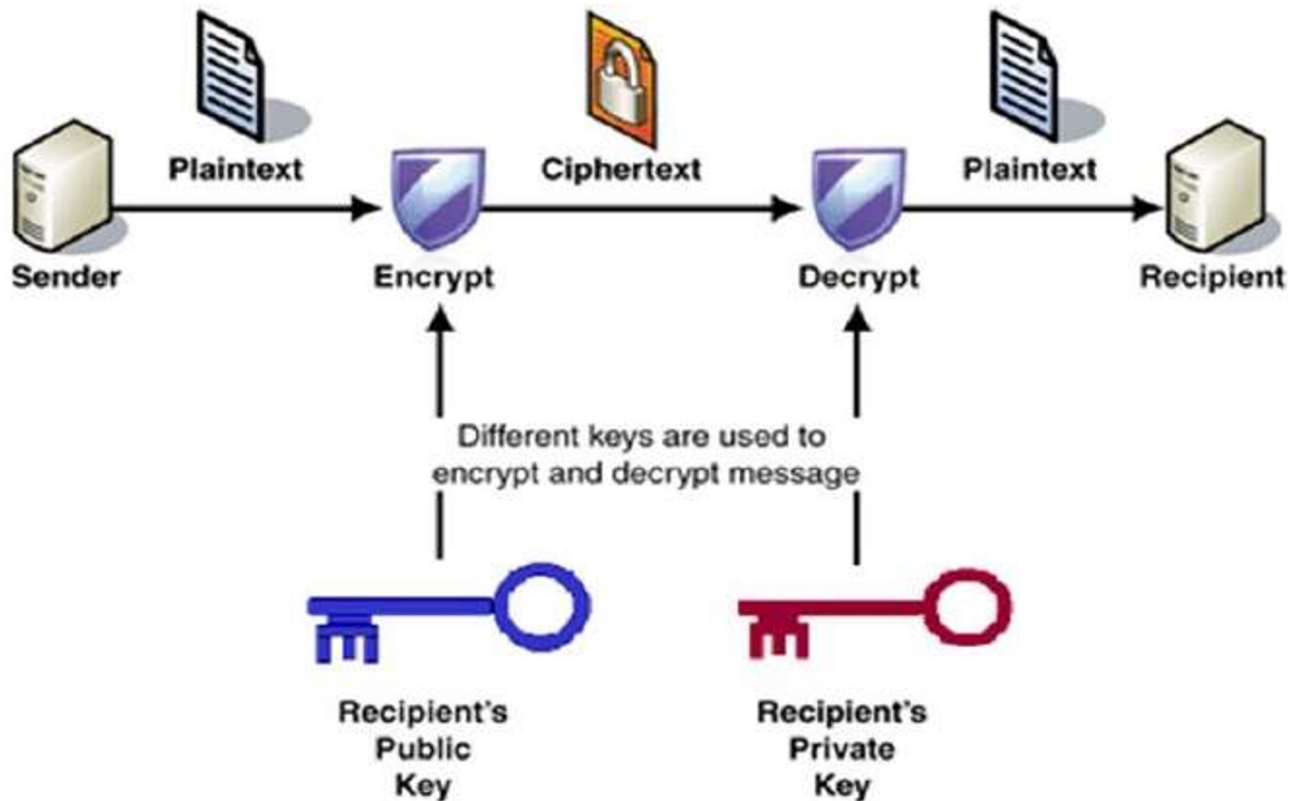
How many spaces are there between E and H in the English alphabet and also in our table?

$$15 / 3 = 5$$

THE COW JUMPED OVER THE MOON.

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

# Public Key Cryptography



# Trying our own Pubkey Crypto

Complete Task 6 on your  
Worksheet

Find the code around the room with your public key.

Use your private key to decrypt the message:

Get code off  
sheet

Convert your  
private key to  
numbers using  
alphabet sheet

Subtract your  
private key numbers  
from code numbers  
to get decrypted  
version as numbers.

25	24	31	18	24
F	I	R	E	S
6	9	18	5	19
19	15	13	13	5
S	O	M	M	E

Convert back into  
letters.

# Hexadecimal

**Hexadecimal** is used heavily within computing and cryptography due to it being able to store more data in a shorter space. It goes from 0-F (4 bits \* 16).

Denary	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

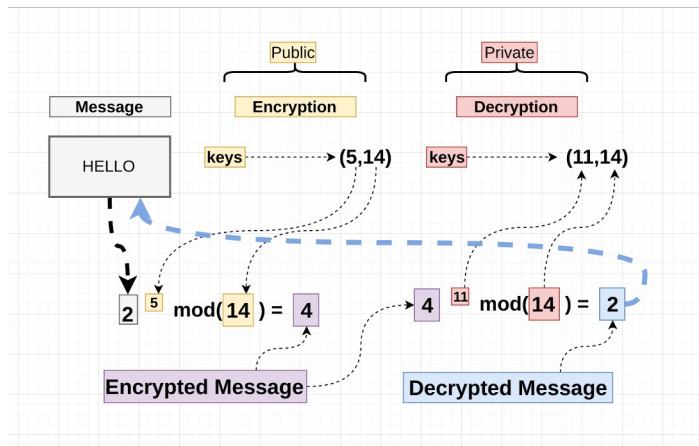
**Complete the final activity 7 on your worksheet.**

Each letter maps back to the 0-26 system we used for the alphabet earlier.

# Ciphers used today and their complexity

The Caesar Cipher is seen as a joke in today's crypto world and is mainly used for educational activities like this.

Real cipher can get super complex, for example RSA which uses the same public key cryptography that we mentioned earlier. There are worries that the introduction of Quantum Computing may mean that we may eventually be able to crack them!



# Prime Numbers

Have you heard of Prime Numbers before?

Can you list any of them?

What is the definition of a Prime Number?

**Prime Numbers are used a lot in advanced Cryptography as they are very hard to go back from due to their limited factors (only 2!).**



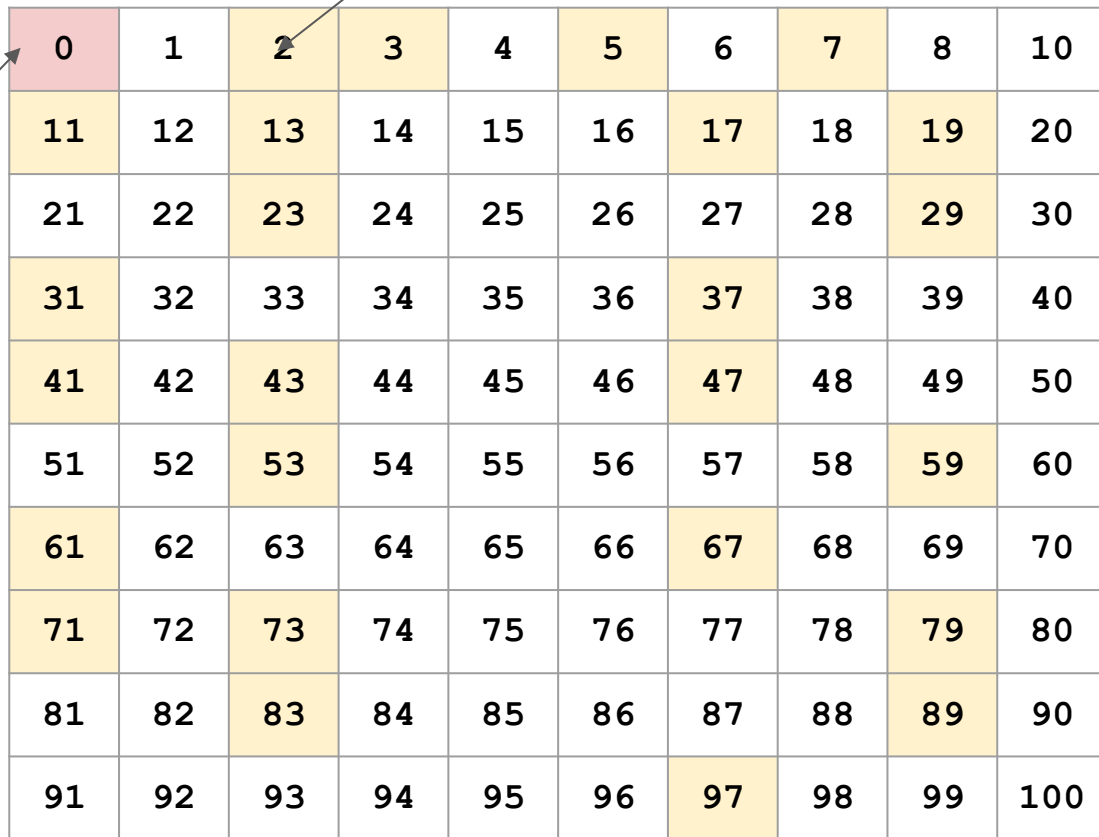
# Prime Numbers

0	1	2	3	4	5	6	7	8	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

# Prime Numbers

2 is the only  
discovered even  
prime number, why?

0 is not a  
prime  
number!



0	1	2	3	4	5	6	7	8	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

# Where to test your skills...

