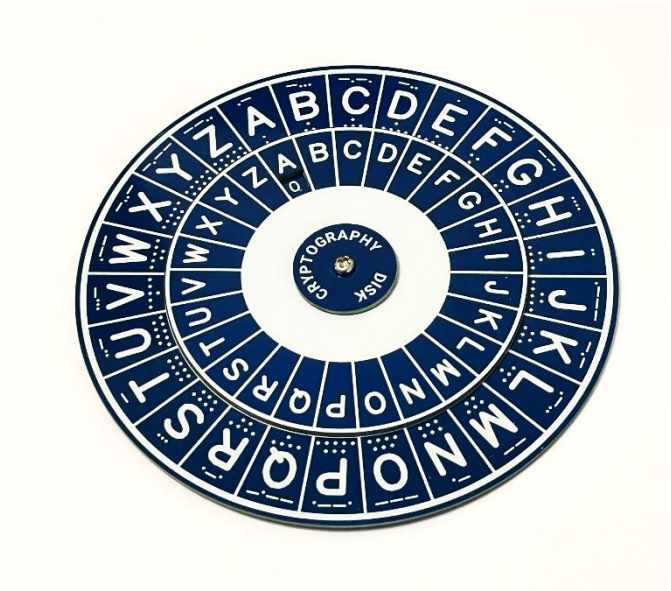
KANGA PRODUCTS

Cryptology Project

‘Hidden Words in plain sight’



This project will give you an introduction to the world of the code breaker, we will look at and use our tools to decode secret messages and we hope you will get an understanding of how interesting this type of work can be. This project is only intended to be a taster of each of the code type we are talking about, the internet is full of much more information on each type of code we are using so which ever code takes your interest do some research on that and learn more about this fascinating topic.

The first examples of hiding messages go back around 4000 years. I’m sure you have seen pictures of pyramids and the hieroglyphs carved out on walls, examples have been found that use none standard symbols that would have been only known by a small select group of people and unreadable to anyone else.

Clay tablets found in Mesopotamia dating back 3500 years contained enciphered writing believed to be secret recipes for ceramic glazes—what might be considered to be trade secrets in today’s world.

For our project we will be starting with a system used about 2000 years ago. A man called Gaius Julius Caesar (100 BC – 44 BC), wanted a way to send secret messages to his army’s and friends. He used one of the first real codes (or correctly called Ciphers). This cipher worked well and was named after

him, it's called Caesar's cipher. It works as well today as it did 2000 years ago. Today you're going to build your own Caesars Cipher disk to allow you to send and receive these hidden messages too.

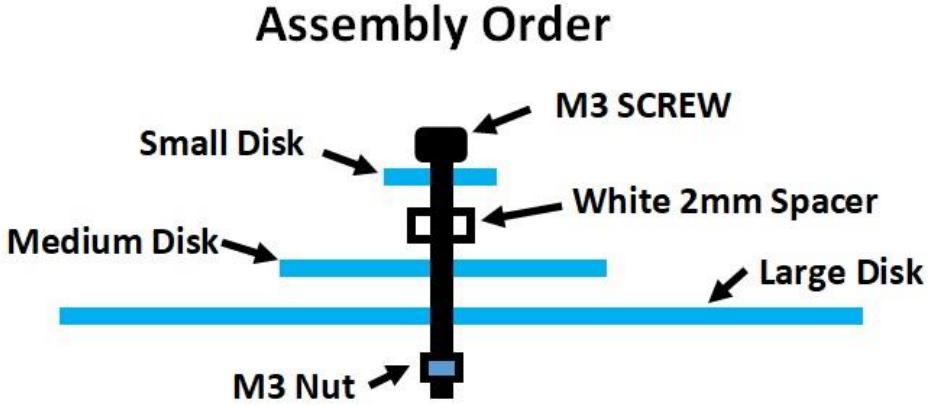
The simple tool we are going to build has two moving disks, each disk is printed with the alphabet running around the edge, the inner disk also has a window that shows a number under the letter 'A' this number is called KEY and this is the secret to decoding messages that use Caesars Cipher. You will also have noticed that the disk as other markings on the front and back, these extra markings will allow us to use other codes too, we will look at them later.

Let's build our tool first and then we will look at how to use it. First check we have all the parts:

1 x Main Large bottom disk
1 x Medium Middle Disk
1 x Small Top disk
1 x Plastic spacer
1 x M3 8mm Screw
1 x M3 Steel nut

To build this kit you will need a small screwdriver and ideally a pair of pilers or a M3 nut spanner.
You have 3 disks, small, medium, and large in size.

First find the small disk, it's about 25mm across and labelled Cryptography disk. Pass the screw though this disk so the screw head is the same side as the writing. Now put the other disks and spacer onto the screw too, follow the order shown below. Don't forget to fit the small white spacer.

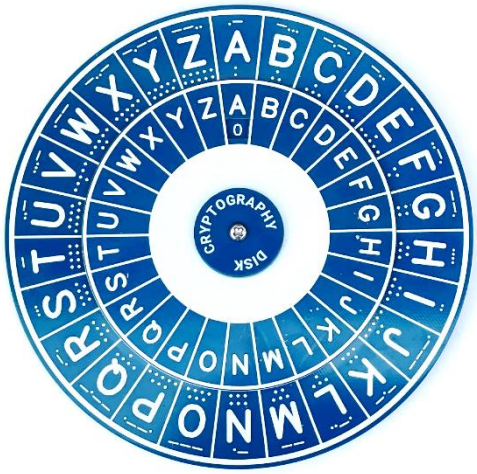


Next tighten the nut on the bottom of the disk. Use a small spanner or a pair of pilers to hold the nut while you tighten the screw. If all correct the middle disk should be free to rotate.

Ok so now we have built our Secret message disk lets see what we can do with it!

Let's look at a 2000 year old code that we can still use today, Ceasars Cipher.

This cipher has all the letters of the alphabet running around the outside of the larger disk and a smaller disk with the same letters on the inside. The disks can be turned so the either the letters line up with each other or are offset, the amount off offset is called the Key, to decode the message we need to set the disk to the same key as was used when the message was encoded.



Start with the two disks set so that the same letters are in line with each other, you will see that the smaller disk is showing a number, in this case it will be Zero (0).

Now to decode a message we need to know the secret Key that was used when the message was encoded.

Let's look at a simple message that I have sent you.

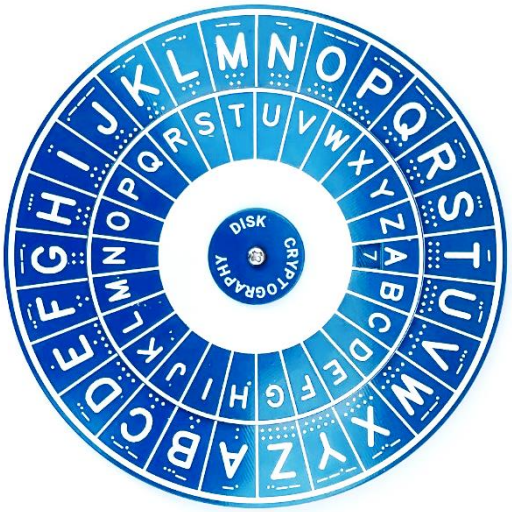
This is an easy one to start with just two words!

Can you decode it?

CODE	A	X	E	E	H		R	H	N
DECODE									

It's hard isn't it! You may work it out but without the secret key it will take some time to work out the message.

If I tell you the Key you will find it easy to decode it.



The secret Key for this message is '7'

Turn the disk so that the number '7' is in the little windows on the smaller disk.

Find the first letter of the code word on the large **outer** letter ring, so for the message above look for the Letter 'A' on the outer ring.

Under this on the smaller wheel you will find a different letter, fill in the box under the first code letter above with this 'New ' decoded letter. Do not change the key, leave it set to 7.

Next find the 'X' on the outer wheel and record the letter under it as before, do this for all the letters in the code word.

Now you should be able to read the secret message!

Here's a few more messages for you to decode

Key '3' (Turn the inner wheel so '3' is in the little cut out window)

G	L	E	K		F	P		X	Q		Q	E	B		O	F	S	B	O		

Key '20'

Z	N	K		S	U	T	K	E		O	Y		A	T	J	K	X		Z	X	K	K

Key ‘11’

H	T	C	S		G	T	X	C	U	D	G	R	T	B	T	C	I					

OK so that’s how we decode words so let’s try and write a message.

If you are building this in a group you write a message for someone else, give them the secret key and see if they can decode it, give the same message to someone else but don’t give them the key and see if they can work it out.

To write your message first choose a key number, let’s say number 4.
turn the **inner** wheel so the number ‘4’ is showing.
Now write down your message/word on paper, its better if you can write it in a table format like below

Word	T	I	M	E		IS		UP	
ENCODE									

Now you have set your Key to 4 look at the letters on the **inner** wheel this time, find the letter ‘T’ (in our example above), now write down the letter that is **above** it , in this example it would be ‘P’. Now don’t reset the wheel, leave it set to your key of ‘4’ and find the next letter, above the letter ‘I’ you will see ’E’ so write that down, do this for all the remaining letters. When finished in our example you should have the encode message as below.

PEIA EO QL

Although Caeser’s Cipher works well there is an only a small number of options for the key so its possible to try each key in a relatively short time if you really needed to read the message.

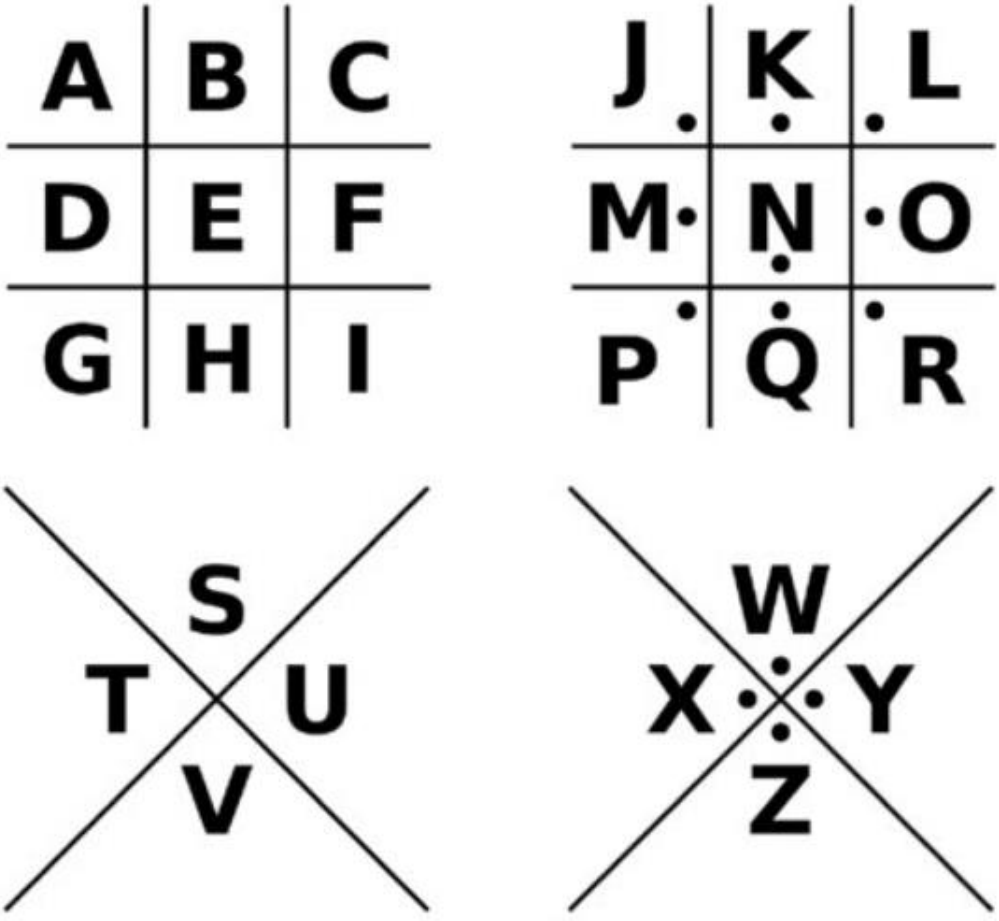
Back 2000 years ago not many people could read well so even a simple cipher like this would make it harder for people to decode.

The next code we will look at is an interesting one with a strange name

PigPen Cipher

The Pigpen Cipher is also known as the Freemason Cipher has it is well known to be used by the Freemasons. The Cipher works by replacing the letters with an image. Not much memorization is required since the letters are distributed over two repeating grids. To mark the difference in the repetition, a dot is used. The cipher symbol is the gridline with or without the dot. The letters could be juggled and moved around to make the cipher more difficult for people that know how it works but the standard grid of letters is most commonly used as shown below.

This cipher is called the pigpen code because the “boxes” look like the fences of pigpens and the dots look like little pigs in their pigpens.



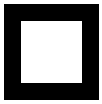
You will find this grid on the back of your decoding disk.

Lets see how to use it, lets look at a simple message ‘HELLO WORLD’

Find the letter ‘H’ in the grid

And write down the shape around it 

Repeat the process for the other letters too

So next we have ‘E’ which is 

Carry on with the rest of the letters

L = 

L = 

O= 

If you continue for the full message you should end up with

Easy isn’t it!

Right encode the following into Pigpen

S	E	C	R	E	T	C	O	D	E

Decoding PenPen is just as easy,

Try decoding these, look at the shape and write down the letter inside of it on the disk

The next cipher we will look at is still used today by thousands of radio hams every day, until recently it was also still used by the military around the world.

Morse Code

An inventor named Samuel F.B. Morse created Morse Code in the 1830s. Before his invention, an important message could take weeks to reach its destination. Morse Code allowed messages to be sent across cities and counties instantly.

It can be sent by radio, telegraphy wire, or even flashed with a hand torch.

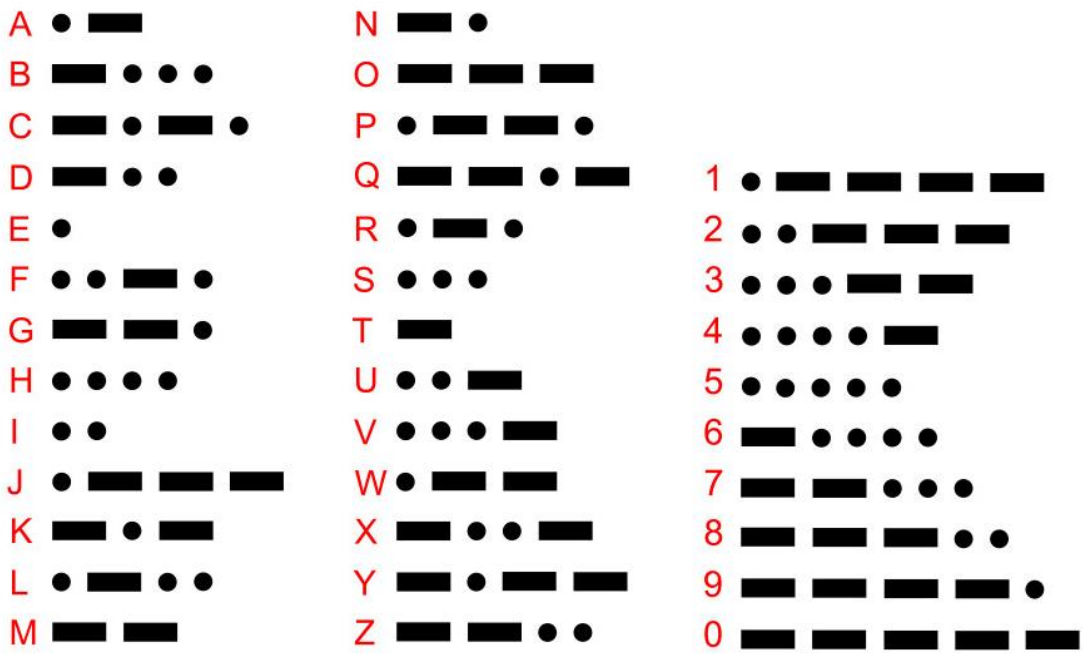
It's relatively easy to learn the code and up to recently it was standard practice for all military organisations to teach it to their radio operators. Even now many people still learn the code, if everything else fails in this digital world Morse will still work as an effective communications method.

Morse is made up from a series of Dots and Dashes, the length of a Dash is three times longer than a Dot.

If you look at the front of your code wheel you will see that the larger disk of letters has a dots and dashes **ABOVE** each letter. (We will talk about the dots under each letter shortly). These Dots and Dashes are the Morse code for each letter.

Here's a chart showing the letters

MORSE CODE



Can you decode this message?

Now write your name in Morse Code below

The finial cipher we are looking at with our disk is one with an interesting history.

Tap Code

You must have seen films where people send message to each other by tapping pipes or walls ? well the way this is done is Tap code, like many things in films they get it wrong and say its Morse code but if you tap a wall or a pipe you cant tell the difference between a Dot and a Dash!

How did Tap Code come about?

Well there is some evidence that it dates back long into history but seems to be often credited to a group of Prisoners of war. Four American POWs who were imprisoned in North Vietnam beginning in 1965, it is made up from a 5x5 grid system is separated by rows and columns. The letter C is used for both C and K. The first series of taps indicates the row number, the second series of taps indicates the column.

It doesn't take long to learn and prisoners quickly taught each other how to use it, messages got sent tapping walls, pipes and even tapping brooms on the floor while they were forced to work.

Let's look at this code in its 5 x 5 grid form. Its important to note each letter is made up with two groups of taps.

	1	2	3	4	5
1	A	B	C/K	D	E
2	F	G	H	I	J
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

So if we wanted to send the word AND

What would we do?

Well start with the letter ‘A’

You will see it’s in the first Row so the first Tap group would be 1 short Tap (that tells us the ROW number) next we can see it’s the first letter in that Row so the second Tap group is also just one. So ‘A’ would be TAP (a small gap) TAP.

We leave a short gap between each tap group and a longer gap between each letter.

Next letter is ‘N’ so that’s on the 3rd ROW and just happens to be the 3rd letter in that Row. To send the ‘N’ we would first make three Taps, a short gap and then 3 more taps so TAP, TAP, TAP (gap) TAP, TAP, TAP

The last letter is ‘D’

So D is in the first Row and is the fourth letter,

To send a ‘D’ we would tap once (first row), then a gap, then four taps.

So ‘D’ Would be TAP, (gap) TAP, TAP, TAP, TAP

Tap code is certainly not a fast way to send a message but it does work, an interesting note about this, since it took a long while to send messages people started to use many of the abbreviations that get used in modern text messages like GBY , God Bless You or GN, Good Night.

Our disk shows the Tap code under each letter on outer wheel. There are two lines of Dots, the top line is the Row number and the bottom Dots are the position on that line, of course if you want to send Tap code just find the Letter you want to send on the outer wheel and look below it to see how many taps to make, remember each letter is made from two groups of taps, the first tap is the Row and the second is the position on the Row.

Other Ciphers

There are many other ciphers that look simple but are much harder to solve, one of my favourites is called Book Code, let me give you an example.

To start with we need a book or a section of text, both the sender and the receiver need to agree on the book or text first and have copies, any book that is likely not to attract attention is a good choice, maybe the bible or a Charles Dickens novel.

For this example I will use a section of text from Lord of the rings.

Three Rings for the Elven-kings under the sky,

Seven for the Dwarf lords in their halls of stone,

Nine for Mortal Men doomed to die,

One for the Dark Lord on his dark throne,

In the Land of Mordor where the Shadows lie,

Of course we really need a larger section of text but to give you an idea of how this works the message I want to send is

'The three men in Mordor lie'

So we find the word **The** in the passage and write down the row and place location so 'The' is Row 1: position 4, 'three' is Row 1, position 1, 'men' is 3:4, 'in' is 2:6, 'Mordor' is 5:5, 'Lie' is 5:9

So the code would be 1:4;1:1;3:4;2:6;5:5;5:9

Without knowing the text its going to be VERY hard to decode!

It's a simple code that does its job very well.

The Codes shown here are simple codes but all have been or are still used today. Many much more complex codes have been made such as the Enigma Code that Bletchley Park is famously associated with breaking. Today the world is using very complex coding systems and large government organisations such a GCHQ and MI6 employ thousands of people, the world of cryptography is still very much alive!

If you find this topic interesting then look out for the Christmas GCHQ challenges that they put out each year. If you look on their web site you can look at all the past challenges they have created.

https://www.gchq.gov.uk/section/news/puzzles

Hppe mvdl !