SECRET MESSAGES

You want to send messages but only if your friend is the ONLY one that can read it. How do you do it?

Hi. This is a secret message. Don't tell anyone the code.

Ij. Uijt jt b tfdsfu nfttbhf. Epo'u ufmm bozpof uif dpef.

⌐⌐. >⌐⌐∨ ⌐∨ ⌐ ∨⌐∟⌐⌐> ⌐⌐∨∨⌐⌐⌐. ⌐
⌐⌐'> >⌐∟∟ ⌐⌐<⌐⌐⌐ >⌐⌐ ∟⌐⌐⌐.

How can you read those messages? What is happening? A cipher! A cipher is writing in disguise.

Here are some secret methods I use. One day you will get a message from me. Be ready to decipher it.

Caesar Cipher
Pigpen Cipher
My very own cipher - I call it the Never Figure Me Out. Because, well....

How a cipher works

It can be easy or complicated. Check it out, I can replace a word with a symbol. So long as you have a key, a sheet that tells you what the symbols mean, then we can talk.

Ice Cream	Underwear	Buy	Store

You	Me	Water	Ok

Me to You: > ⬢ ✚.   You to me: ➡

I wrote, Buy Me Ice Cream, and you wrote, OK. But, it could be better. What happens if someone has our key? Instead, let's say we agree that our letters are going to be shifted 3 spaces or letters from normal. Then

Exb ph Ifh fuhdp.

is "Buy Me Ice Cream", right? Why? If we take our normal letters from A to Z and shift it just 1 time then when we write B we mean A, or if we shift it 2 times then we write C but mean A. So, a shift of 3 makes E mean B. EXB is BUY.
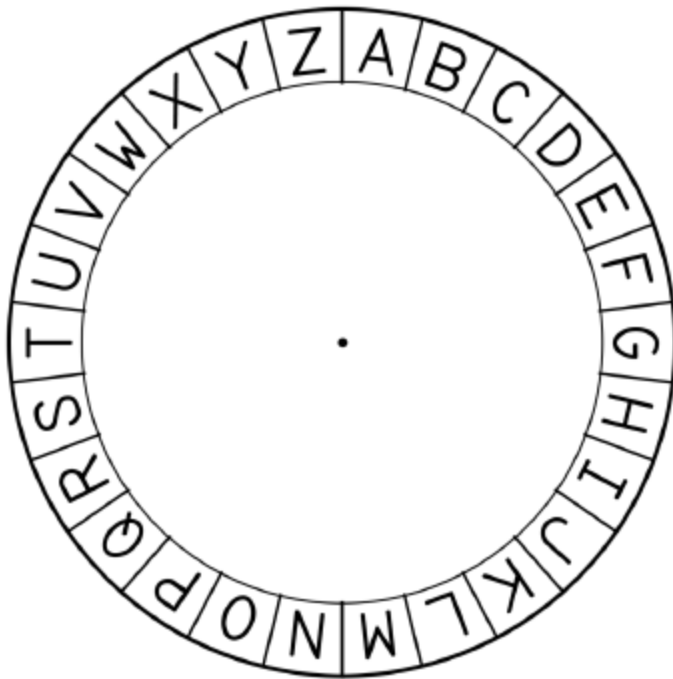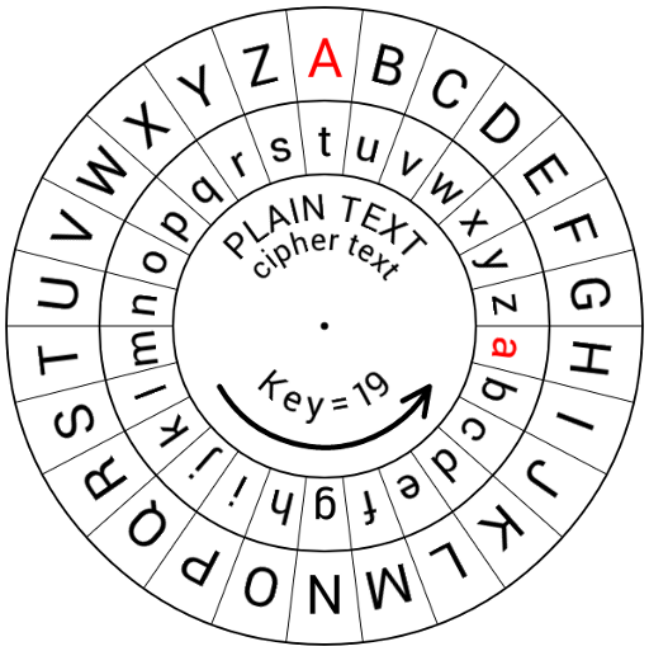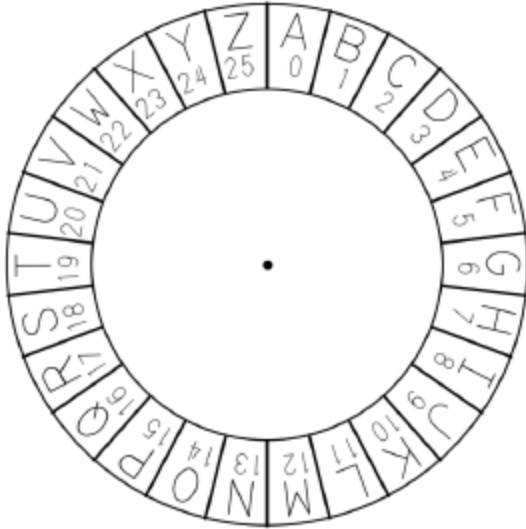
Letters:	A	B	C	D	E	F	G
1 shift	Z	A	B	C	D	E	F
2 shifts	Y	Z	A	B	C	D	E

Caesar cipher

Not too bad if it is a shift of 1 but what about 17 places? Just make a wheel! Move it over the number of shifts you choose between you and your friend, and boom - a cipher and decipher key. This is called a Caesar Cipher. Here is one you can use. Put the small wheel in the center of the big and turn the number of shifts to decipher each letter.

Pigpen cipher

What if we want to use symbols instead of regular letters? We could split the alphabet up into groups of 3, so ABC is a group, DEF is a group, and so on.

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

Now, the symbol will be the lines separating the group, and a dot for which letter in the group we want, like this:

Bracket for the first group and first letter, A:

Bracket for the first group and second letter, B:

So, now I will write what I want to do today:

        S   W   I   M

I want to swim. Cool, right?

Now, that may be a little too easy for someone to steal my secret message. So, I created my own. I call it "the Never Figure Me Out". I shifted the letters 3 places, like a Caesar, but I put them in groups like a Pigpen.

YZ	ABC	DEF
GHI	JKL	MNO
PQR	STU	VWZ

Create your own - 1

Three guys stranded on a desert island find a magic lantern. Inside they find a genie who grants them each one wish.

The first guy wishes he was off the island and back home. Poof! He's gone.

The second guy makes the same wish to go home. Poof!

The third guy looks around the island and sees nothing left. He says:

L dp orqhob. L zlvk pb iulhqgv zhuh edfn.

I choose a Caesar cipher with 3 shifts - What's the third guy say?

OK, so pick a number of shifts and use your wheel to write out what the third guy says using a Caesar cipher. Then take those letters and use the pigpen to encode it one more time. Give your message to someone else and see if they can decipher your message.

CREATE YOUR OWN - 2

Pick any system you want - make one up!... And then write out your favorite joke. Give the joke in a cypher to a friend. Can they figure it out without you telling them the key? Do you have more than one key?

QUESTION

How can math be used to break the code? Even if you don't know someone's key and cipher, you can break the code. How?