Cryptography Worksheet — The Caesar Shift

Wkh Fdhvdu Vkliw

Julius Caesar used a simple **Substitution Cipher** to send messages to his troops. He used a very simple rule to replace each letter with another letter from the alphabet. He substituted each letter by the letter that was 3 places further along in the alphabet, so that "a" was replaced with "D", "b" with "E" and so on. *Complete the table below to show what each letter is enciphered as using this system.*

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
D	E	F																							

Using the Caesar Cipher, encode the name of your school. Check that you get the same code as the person sat next to you.

How easy is it for someone who intercepts a secret message written using this cipher to work out the original message? Is there anyway to make it harder to work out?

Although Caesar substituted each letter with the letter 3 places ahead, there are other variations of this cipher. You could shift each letter by 4 or 5 or 6 etc. This is called a **key**, and depending on which key you use, you will get a different message.

Cut out and make a Caesar Shift wheel. Use the wheel to encipher your name using three different keys. Pass your encoded names to the person next to you, and ask them to work out what keys you used.

How many different keys are there?

Decode this message, which was enciphered using a Caesar Shift: ZKHQ BRX KDYH GHFRGHG WKLV ZRUN RXW WZHQWB VHYHQ WLPHV QLQH DQG WHOO BRXU WHDFKHU.

Write a message of your own, and encipher it using the Caesar Wheel. Hand the secret message to your partner, and get them to decipher it.

In pairs, discuss how good this cipher is at protecting messages. Can you think of any ways to improve it?

Teacher's Notes — The Caesar Shift

The Caesar Shift Cipher has a long history of usage, dating back to Julius Caesar (100BC—44BC). He used the cipher to protect messages of military importance, and it is believed that he used many other substitution ciphers as well (although this is the only one we have evidence of him using, as quoted by Suetonius). The cipher works by substituting for each letter the letter that is *k* letters further along the alphabet, where *k* is the key. Below is the completed table for a shift of 3.

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
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

If a shift of 3 is always used, as it is thought was the case with Caesar, then it is fairly easy for an interceptor to break the code. However, the huge benefit of this cipher over the Atbash or Pigpen is that there is a key. This key allows the user of the cipher to change a very small detail of the encryption process, which does not make it any harder to encipher or decipher if you know the key, but makes it a lot harder to break the code for someone who intercepts the message. Discuss the use of keys in cryptography as being integral to creating a more secure cipher, by giving the person using the cipher a choice, it makes it harder to work out the original message for an interceptor. Also note the important fact that, for a good cipher, the intended recipient knows the key, and so it is also easy for them to decipher the original message.

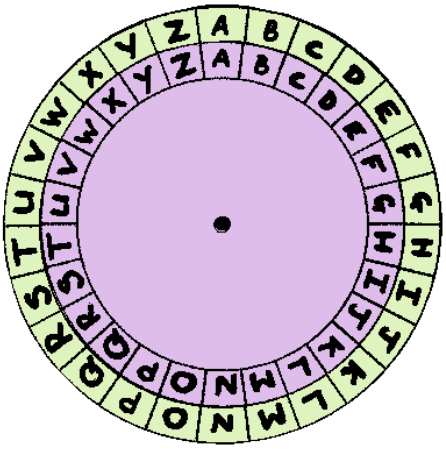
Give each pupil a copy of the Caesar Wheel Template, and they need to cut it out, and fasten the two wheels together using a clip. It works by matching "a" on the inner wheel to the appropriate shift letter on the outer wheel: so for a shift of 3, "a" would be lined up with "D". Explain that this was a very early machine used to help in the process of enciphering and deciphering secret messages.

There are 26 different keys for this cipher: "a" -> "A" (shift of 0); "a" -> "B" (shift of 1); "a" -> "C" (shift of 2); etc. Note that the identity shift is a key, but that it is pretty useless as it just returns the original message. Also note that a shift of 26 is the same as a shift of 0, and can introduce some modular arithmetic. Also, a shift of –1 (or 1 to the right) is the same as a shift of 25.

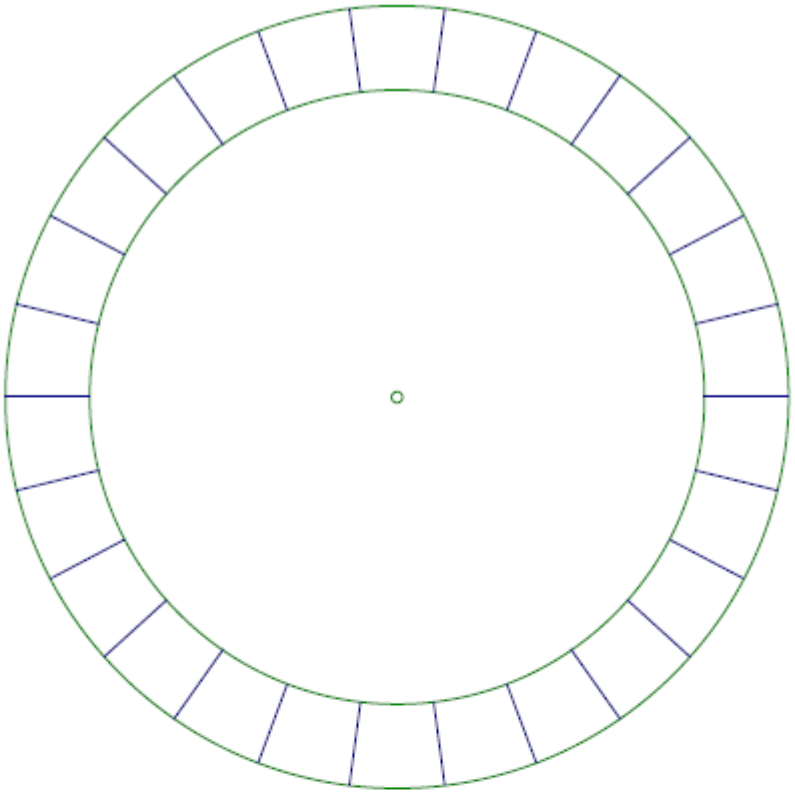
The message decodes as: *'When you have decoded this work out twenty seven times nine and tell your teacher'*.

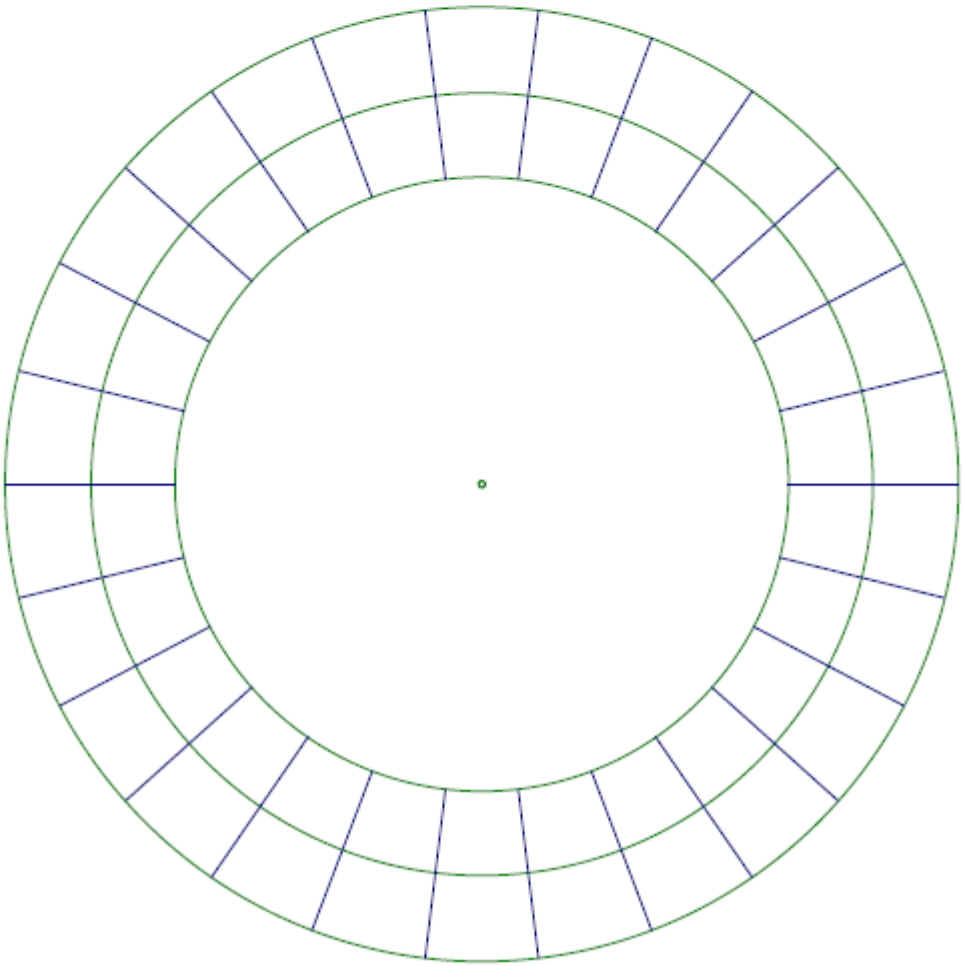
In discussions of how good the cipher is, expect to hear that it is better than the Atbash and Pigpen Ciphers, and ask why (because it has a key).

Extension: How could we make this cipher even more secure? One way would be to jumble up the alphabet first, before you write it on the two wheels.



Caesar Wheel Template





Caesar Wheel

Directions:

1. Paste this whole page onto thin card
2. Carefully cut around the two circles
3. Write the alphabet in **RED** around the SMALL circle
4. Write the alphabet in **BLACK** around the LARGE circle
5. Fix the small circle onto the big circle using a paper fastener through the centre (marked with a dot)

You are ready to use your Caesar Wheel

REMEMBER the plaintext letters are written in **BLACK**, the ciphertext letters are written in **RED**

ENCIPHERING = **BLACK** to **RED**

DECIPHERING = **RED** to **BLACK**