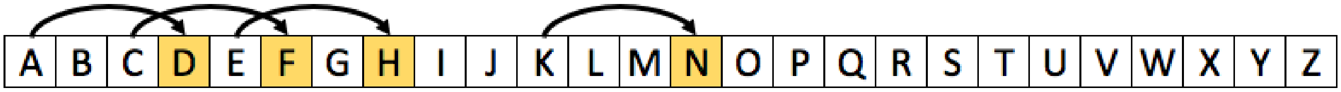
CEMC.UWATERLOO.CA | The CENTRE for EDUCATION in MATHEMATICS and COMPUTING

CEMC Math Circles - Grade 9/10

Wednesday, March 24, 2021
Surprise Party

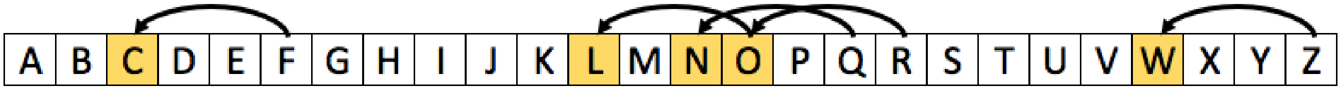
You are planning a surprise party for your friend, Eve. To prevent Eve from finding out about the details of the party, you and the other party planners have agreed to communicate in code. You have chosen to code your messages using a *substitution cipher* known as the *Caesar cipher*. A substitution cipher works by systematically replacing each letter (or symbol) in a message with a different letter (or symbol). A Caesar cipher involves "shifting" the alphabet.

In order to code messages using a Caesar cipher, your group first needs to choose an integer k from 1 to 25, inclusive. This integer k is called the *key* for the cipher, and determines by how many places the alphabet will be shifted. To *encrypt* a message (that is, to change the message from regular text to code) each letter in the message is replaced with the letter that appears k positions to the right in the alphabet. For example, to encrypt the message CAKE using a key of 3, the letter C is replaced with the letter F, which is 3 positions to the right, and the original message CAKE becomes the *encrypted* (or coded) message FDNH.



Note that if you cannot move k places to the right in the alphabet, then you wrap around to the beginning. For example, the letter 3 places to the right of Y is B.

To *decrypt* a message (that is, to change the code back to regular text) each letter in the coded message is replaced with the letter that appears k positions to the left, wrapping around if necessary. For example, to decrypt the message FORZQ using the same key of 3, the letter F is replaced with the letter C, and the coded message FORZQ can be revealed to be the message CLOWN.



For the questions below, consider making your own *Caesar Cipher Decoding Wheel* (see last page) to help you encrypt and decrypt. Alternatively, if you have some programming knowledge you can create a computer program that can encrypt and decrypt messages given some text and a key as input.

Activity 1:

(a) Using a key of 6, encrypt the message PARTY STARTS AT SEVEN.

(b) Using a key of 24, decrypt the message RFC RFCKC GQ DYLRYQW.

(c) The other party planners sent you the following message but the key got lost. Can you still decrypt the message? *Hint: What is the most commonly used letter in the English language?*

PFRPYP HTWW MCTYR ESP NLVP LYO OPNZCLETZYD

More Info:

For a slightly more challenging substitution cipher, check out the Vatsyayana Encryption Scheme.

The Vigènere Cipher

While reading up on the Ceasear cipher, you came across another encrypting technique called the *Vigenère cipher*. Similar to the Ceasear cipher, the Vigenère cipher is a substitution cipher. The Vigenère cipher uses multiple Caesar ciphers and a special table called the Vigenère table.

On the following page, you can find a picture of the Vigenère table. The table consists of 26 copies of the alphabet, where each alphabet is written in a different row. Each row of the table is made by shifting the alphabet in the previous row one place to the left. The table also has the alphabet as the row and column headings. In order to code messages using the Vigènere cipher, your group must first agree on a secret word, which will be your *key* for the cipher. Throughout the encryption process, the Vigenère cipher uses several different rows of the table. The row used at each point in the process depends on the key.

The Vigenère cipher is best illustrated through an example. Say your group chooses PARTY to be the key. The person sending the message repeats the key until it matches the length of the message to be encrypted. For example, to encrypt the message BOB WILL BRING BALLOONS we use the key as follows:

Message:	BOB WILL BRING BALLOONS
Repeated key:	PAR TYPA RTYPA RTYPARTY

We encrypt each letter in the message using the letter in the repeated key directly below it, together with the table. For example, the first letter of the message B is paired with P, the first letter of the repeated key. We encrypt the letter B by replacing it with the letter found at row P and column B of the table. That is, we replace B with Q. Similarly, for the second letter of the message O, we use the letter A of the repeated key. The letter at row A and column O in the table is O, so in this case, the encryption is just the letter O itself. We encrypt the rest of the message in a similar fashion:

Message:	BOB WILL BRING BALLOONS
Repeated key:	PAR TYPA RTYPA RTYPARTY
Encrypted message:	QOS PGAL SKGCG STJAOFGQ

To decrypt a message, we repeat the key until it matches the length of the encrypted message. As above, we pair the letters in the message with letters from the repeated key. For each pair, we use the row corresponding to the repeated key letter. We then find the encrypted letter in this row, and replace it with the letter corresponding to the column that it is in. For example, to decrypt the message RAEWJTS using the key PARTY, the letter R is replaced with the letter C, and the coded message RAEWJTS can be revealed to be the message CANDLES.

Activity 2:

(a) Using the key PARTY, encrypt the message CHOCOLATE CAKE.

(b) Using the key PARTY, decrypt the message

PLZVC LICE ZGIEZ QDMV UMPRU ZYBEJ.

(c) You received the following message, but forgot what the key is! You only remember that the key is 4 letters in length and ends with a G. Can you still decrypt the message? *Hint: Sort the letters into* 4 *different groups.*

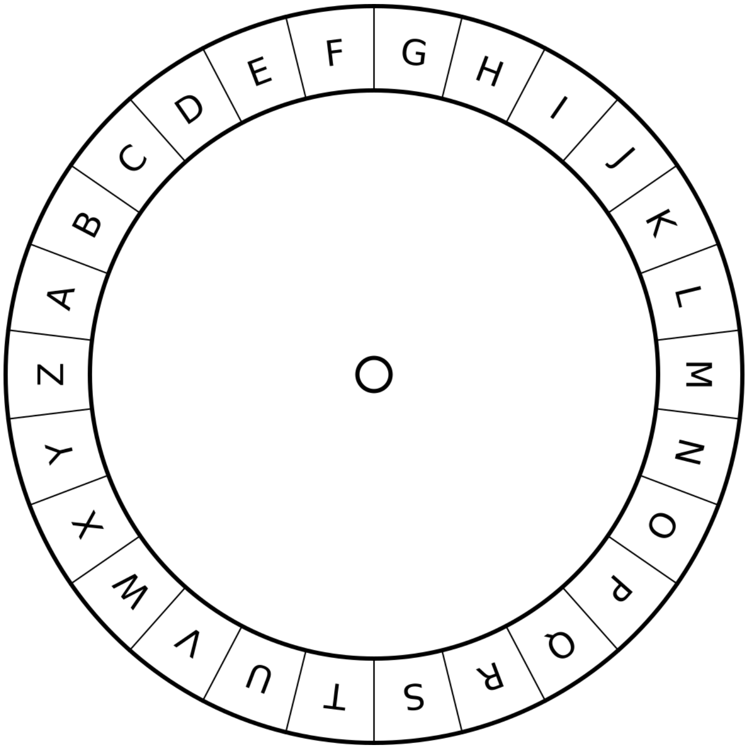
WTVFSJRZZ EVRD JEOFO PGFLYKK NBX LPR ISSR

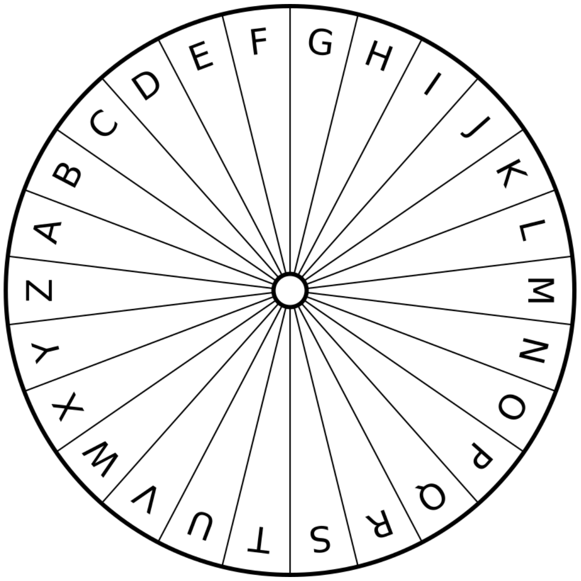
The Vigènere Table

	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

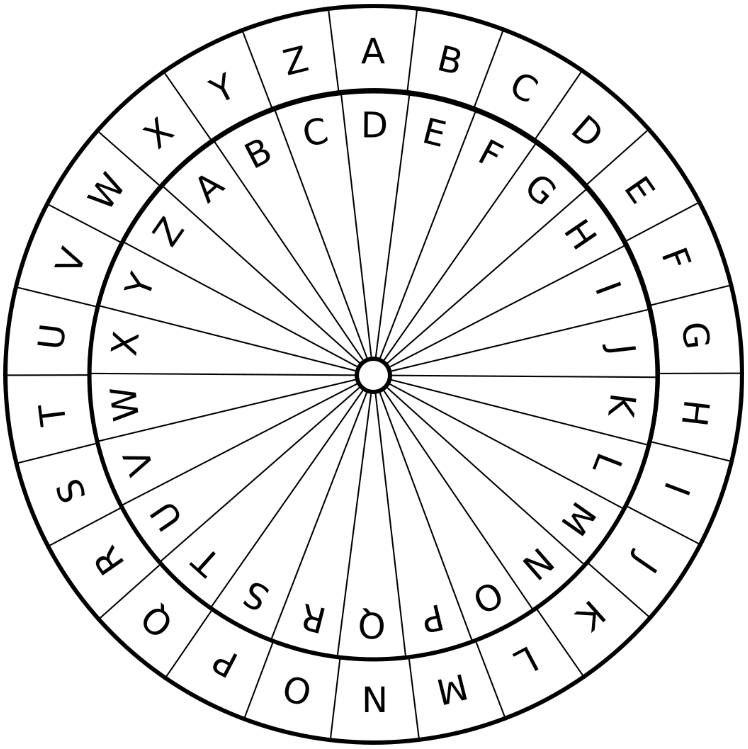
Caesar Cipher Decoding Wheel

Print and cut out the following two circles. Place the smaller circle on top of the larger circle and attach them through the middle using a paper fastener (brad).





Rotate the circles so that the `A`'s are aligned. Then set your key by rotating the inner circle **counter clockwise**. In the diagram below the key is set to 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

You are now ready to encrypt and decrypt! To encrypt, replace each letter on the outer circle with the corresponding letter on the inner circle. To decrypt, replace each letter on the inner circle with the corresponding letter on the outer circle.