Teaching Guide: Caesar Ciphers

With a **Caesar cipher,** you replace each letter in a message with a letter further along in the alphabet. A Caesar cipher shifts the alphabet and is therefore also called a **shift cipher**. The **key** is the number of letters you shift. Caesar cipher is one of the oldest types of ciphers. It is named after Julius Caesar, who is said to have used it to send messages to his generals over 2,000 years ago.

The Caesar cipher is a good cipher to use to introduce cryptography. Students can quickly understand the pattern and they enjoy using cipher wheels to help encrypt and decrypt.

Included in this packet

Opener
Caesar Ciphers: Encrypting and Decrypting
Caesar Ciphers: Cracking
Caesar Ciphers: More Encryption
Caesar Ciphers: More Decryption
Cipher Wheels
Answer key

Introducing the Cipher

Riddle:	What is the clumsiest bee?
Answer:	B C V N C M J O H C F F

Begin by writing this riddle and encrypted answer on the board. The answer (a bumbling bee) has been encrypted with a Caesar Cipher, key = 1. Each letter in the encrypted message is just the next letter along in the alphabet.

This can be displayed as the students come to the classroom. By the time everyone has arrived you will be ready to go with the discussion. Once students have cracked the answer they will want to discuss how they did it. Be sure the discussion includes that the answer was encrypted by shifting the alphabet one letter.

Next pass out the cipher wheels. Students can make these as class is starting or you can have them ready in advance. You can show them how to turn the wheel one letter so that the plaintext letters in the riddle match the ciphertext letters.

Encrypting and Decrypting

Next hand out the page ***Caesar Ciphers: Encrypting and Decrypting.*** You can go over the top of the page with the class. They will see how to substitute letters from the cipher table and how to use the wheel.

To **encrypt** with a cipher wheel, students turn the inner wheel counterclockwise, shifting it the number of letters specified by the key. Then they match plaintext and ciphertext letters as shown on the wheel.

To **decrypt**, students read the wheel backwards: after setting the wheel to the appropriate key, they begin with a ciphertext letter on the inner wheel and match it with the corresponding plaintext letter on the outer wheel.

While students practice decrypting the riddles, you can make sure all the students see how to use the wheel to encrypt and to decrypt.

There are several vocabulary words on this page that may be new to students, such as **encrypt**, **decrypt**, **key**, **plaintext**, and **ciphertext**. Students will pick them up as they work with messages.

Common error: When using a cipher wheel, students sometimes get confused about how to count the shifts.
Solution: Ask them to begin by setting their wheels so that plaintext **a** matches ciphertext **A.** This is a zero shift. Then have them turn their inner wheels *counterclockwise* (according to the arrow), counting the letters as the wheel turns. Matching **B** to **a** is a shift of one. Continue turning to show other shifts.

Common error: There is often a confusion between plaintext and ciphertext.
Solution: Whenever possible follow CryptoClub follows these conventions:
Write plaintext in lowercase and ciphertext in upper case.
Write plaintext on the top line of a message and ciphertext on the bottom line.

Point out to students that these conventions are used in the cipher tables and the sample messages. Show them this convention is also used on the wheel—the lowercase letters on the outer wheel are plaintext and the uppercase letters on the inner wheel are ciphertext. Putting the plaintext on the outer wheel is consistent with the convention of putting it on the top row of a table, since that is where it would be if the wheel were made by wrapping a table around a circle.

More Practice

The ***Caesar Cipher: More Encrypting*** page provides practice with encrypting, while also generating a supply of student-made messages that can be used to play **Cipher Tag** (see next section). Practice with encrypting provides a foundation for understanding how a cipher works. But encrypting is often not as engaging as decrypting, since it is not self-correcting the way decrypting is and it does not give the reward of an interesting message at the end. However, if students know that someone else will decrypt their messages later in a game, they will likely be engaged. Partners can decrypt each other's messages to check for errors before using the messages in the game.

The riddles on the ***Caesar Cipher: More Decrypting*** page provide quick practice with decrypting for those who have more time. Student may want to take these riddles home to enjoy with their families.

Play a Game: Cipher Tag

Games provide a fun way for students to practice their newly learned encrypting and decrypting skills. **Cipher Tag** can be played with all sorts of different messages that students create. You can use the ones they made on the ***Caesar Cipher: More Encrypting*** page.

For ***Cipher Tag***, one person is chosen to be "It". Whoever is "It" writes an encrypted message on the board and also announces the key that was used to encrypt the message. The first player to declare that they know the message writes it above the encrypted message, giving everyone a chance to confirm the decryption. If it is correct, this player is the next "It". If the decryption is not correct, another player gets a chance to correct it and to become the next "It". If the next "It" does not have an encrypted message ready to go, he or she can chose another player to be "It".
Advanced option: After a few rounds the students will be ready to add this challenge: the key is not announced when displaying the message. Students will develop their cracking skills as they try to figure out the key.

As students play the game, invite discussion about how they arrive at their answers. You have a chance to check players' efficiency in encrypting and decrypting. Common errors include turning the inner wheel the wrong way and confusing plaintext with ciphertext letters. It is likely that other players will be able to see and correct these errors as the game progresses.

Problem: There is not enough time for everyone to get an opportunity to be "It". Only a few students are getting the answers.
Solution: One way to increase participation is to have two or three games going at once on different sections of the board. Everyone will get to post their message and more will get the answers because students continue to work while winners are posting the next messages.

Cracking

The term "cracking" refers to decrypting a message when you don't know the key (or even the cipher) that was used to encrypt it. Cracking is more challenging than simply following a procedure to decrypt. It can be very satisfying because it involves using one's own ingenuity.

Ask students to try to crack the messages on the ***Caesar Ciphers: Cracking*** page. Caesar ciphers are relatively easy to crack because once you figure out one letter, you know how to set the wheel to decrypt the rest of the letters. The messages progress in difficulty, so students might not get them all on the first try. After they have tried several messages, ask them to discuss the methods they used. Finding their own strategies for cracking and telling others about them is another part of the fun of CryptoClub. The complete *Cipher Handbook* contains a page of tips for Cracking Ceasar Ciphers. It is not surprising for a class to come up with all of them without reference to the book. They may even invent other ways!

Problem: There is not enough time to do the ***Caesar Ciphers: Cracking*** in a one-day lesson.
Solution: Hand out the page for the students to take home. They can teach the Caesar cipher to their friends and family and everyone can work together to crack these messages.

Cryptoclub Website

Problem: Your students want to do more Cryptography!
Solution: Send them to cryptoclub.math.uic.edu or to our new website, cryptoclub.org, that is under development.

Feedback

Problem: Your students want to do more Cryptography!
Solution: Be in touch with the CryptoClub Project to learn how to get materials and training to conduct 20 sessions of Cryptography. Learn more at www.math.uic.edu/CryptoClubProject

CryptoClub want to know about you! If you used these pages, please let us know how it worked for you and your students. Answer the questions on this page and email them to Bonnie Saunders at saunders@math.uic.edu.

Name:

Where are you?

How can we best contact you about CryptoClub?

Tell us something about your program and your students.

How did the Caesar Cipher lesson go for you and your students?

OPENER

What is the clumsiest bee?

B C V N C M J O H C F F

Caesar Ciphers: Encrypting and Decrypting

In a **Caesar cipher,** each letter is replaced by a letter further along in the alphabet. You can think of it as shifting the alphabet to the left. The **key** of a Caesar cipher is the number of places the alphabet is shifted. Here is a Caesar cipher with key 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

Caesar cipher with key 3. Each letter is shifted 3 places to the left.

Example 1: Use the table to encrypt and decrypt with key = 3.

Encrypt

plaintext:	h	i	d	d	e	n
CIPHERTEXT:						

Decrypt

W	U	H	D	V	X	U	H

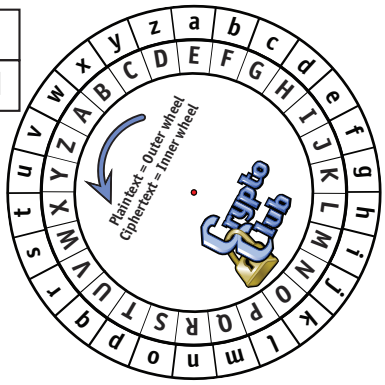
Example 2: Use the cipher wheel with key =4.

Encrypt

plaintext:	s	e	c	r	e	t
CIPHERTEXT:						

Decrypt

Q	I	W	W	E	K	I



Cipher wheel with key = 4

Decrypt the answers to the following riddles. Use a cipher table or a cipher wheel.

1. **Riddle:** What makes a road broad?
   Answer (key 3):

plaintext:														
CIPHERTEXT:	W	K	H		O	H	W	W	H	U		E		

2. **Riddle:** What goes up but not down?
   Answer (key 4):

plaintext:														
CIPHERTEXT:	C	S	Y	V		E	K	I						

3. **Riddle:** What is a tree's favorite drink?
   Answer (key 10):

plaintext:														
CIPHERTEXT:	B	Y	Y	D		L	O	O	B					

Caesar Ciphers: More Encrypting

For each problem, think of an item from the category and write it into the plaintext boxes. Choose a key and encrypt with that key.

Example: Something you might put on your head.

Key = 7

plaintext:	f	e	d	o	r	a											
CIPHERTEXT:	M																

1. Something you might put on your head.

Key =

plaintext:																	
CIPHERTEXT:																	

2. An animal that is bigger than a breadbox.

Key =

plaintext:																	
CIPHERTEXT:																	

3. A president of the United States.

Key =

plaintext:																	
CIPHERTEXT:																	

4. Something that is red.

Key =

plaintext:																	
CIPHERTEXT:																	

Caesar Ciphers: More Decrypting

Decrypt **Answers A**, **B**, **C**, and **D**, which have been encrypted with Caesar ciphers. Match each riddle with its answer.

Riddles:

1. Why can't you tell an egg a joke? Answer _____
2. What do call a snail on a ship? Answer _____
3. Why was Cinderella bad at soccer? Answer _____
4. What did one eye say to the other? Answer _____

Answer A. Encrypted with key = 13.

plaintext:														
CIPHERTEXT:	N		F	A	N	V	Y	B	E					

Answer B. key = 18

plaintext:																	
CIPHERTEXT:	T	W	L	O	W	W	F		Q	G	M		S	F	V		E	W
plaintext:																	
CIPHERTEXT:	K	G	E	W	L	Z	A	F	Y		K	E	W	D	D	K	!	

Answer C. key = 23

plaintext:																	
CIPHERTEXT:	F	Q		J	F	D	E	Q		Z	O	X	Z	H		R	M	.

Answer D. key = 12

plaintext:																	
CIPHERTEXT:	N	Q	O	M	G	E	Q		E	T	Q		D	M	Z			
plaintext:																	
CIPHERTEXT:	M	I	M	K		R	D	A	Y		F	T	Q		N	M	X	X

Caesar Ciphers: Cracking

What if you find a secret message but you don't know how it was encrypted? Maybe you know the Caesar cipher was used, but you don't know the key. In that case, you only have to figure out one letter to know how much the alphabet was shifted.

If you guess one letter, you can set your Caesar wheel to correctly decrypt that letter and then use that setting to decrypt the rest of the message. Or, you can find the row that correctly decrypts that letter in the Vigenère square and use it to decrypt the rest.

Crack the following, which were encrypted with Caesar ciphers. You will know you are on the right track when you get something that makes sense.

1. D R E P T C L V J Y V C G U V T I P G K R T R V J R I

T Z G Y V I .

2. E S P D X L W W H Z C O D L C P G P C J S P W A Q F W .

3. U ' X X F T U Z W M N A G F F T M F .

4. C Q R B F J B Q J A M N A K N L J D B N C Q N A N F N A N W X B Y J L N

B K N C F N N W F X A M B .

5. Z X Z F Q Q D Y M J R T X Y H T R R T S Q J Y Y J W N X J

G Z Y S T Y F Q B F D X .

Answers

Caesar Ciphers: Encrypting and Decrypting

In a **Caesar cipher,** each letter is replaced by a letter further along in the alphabet. You can think of it as shifting the alphabet to the left. The **key** of a Caesar cipher is the number of places the alphabet is shifted. Here is a Caesar cipher with key 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

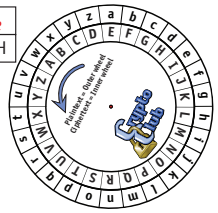
Caesar cipher with key 3. Each letter is shifted 3 places to the left.

Example 1: Use the table to encrypt and decrypt with key = 3.

Encrypt							Decrypt							
plaintext:	h	i	d	d	e	n	*t*	*r*	*e*	*a*	*s*	*u*	*r*	*e*
CIPHERTEXT:	*K*	*L*	*G*	*G*	*H*	*Q*	W	U	H	D	V	X	U	H

Example 2: Use the cipher wheel with key =4.

Encrypt							Decrypt							
plaintext:	s	e	c	r	e	t	*m*	*e*	*s*	*s*	*a*	*g*	*e*
CIPHERTEXT:	*W*	*I*	*G*	*V*	*I*	*X*	Q	I	W	W	E	K	I



Cipher wheel with key = 4

Decrypt the answers to the following riddles. Use a cipher table or a cipher wheel.

1. **Riddle:** What makes a road broad?
   Answer (key 3):

plaintext:	*t*	*h*	*e*		*l*	*e*	*t*	*t*	*e*	*r*		*b*		
CIPHERTEXT:	W	K	H		O	H	W	W	H	U		E		

2. **Riddle:** What goes up but not down?
   Answer (key 4):

plaintext:	*y*	*o*	*u*	*r*		*a*	*g*	*e*						
CIPHERTEXT:	C	S	Y	V		E	K	I						

3. **Riddle:** What is a tree's favorite drink?
   Answer (key 10):

plaintext:	*r*	*o*	*o*	*t*		*b*	*e*	*e*	*r*					
CIPHERTEXT:	B	Y	Y	D		L	O	O	B					

Caesar Cipher: More Encrypting

For each problem, think of an item from the category and write it into the plaintext boxes. Choose a key and encrypt with that key.

Example: Something you might put on your head.

Key = 7

plaintext:	f	e	d	o	r	a											
CIPHERTEXT:	M	*L*	*K*	*V*	*Y*	*H*											

1. Something you might put on your head.

Key =

plaintext:																	
CIPHERTEXT:																	

2. An animal that is bigger than a breadbox.

Key =

plaintext:																	
CIPHERTEXT:																	

3. A president of the United States.

Key =

plaintext:																	
CIPHERTEXT:																	

4. Something that is red.

Key =

plaintext:																	
CIPHERTEXT:																	

Answers

Caesar Cipher: More Decrypting

Decrypt **Answers A**, **B**, **C**, and **D**, which have been encrypted with Caesar ciphers. Match each riddle with its answer.

Riddles:

1. Why can't you tell an egg a joke? Answer ____*C*
2. What do call a snail on a ship? Answer ____*A*
3. Why was Cinderella bad at soccer? Answer ____*D*
4. What did one eye say to the other? Answer ____*B*

Answer A. Encrypted with key = 13.

plaintext:	*a*		*s*	*n*	*a*	*i*	*l*	*o*	*r*					
CIPHERTEXT:	N		F	A	N	V	Y	B	E					

Answer B. key = 18

plaintext:	*b*	*e*	*t*	*w*	*e*	*e*	*n*		*y*	*o*	*u*		*a*	*n*	*d*		*m*	*e*
CIPHERTEXT:	T	W	L	O	W	W	F		Q	G	M		S	F	V		E	W
plaintext:	*s*	*o*	*m*	*e*	*t*	*h*	*i*	*n*	*g*		*s*	*m*	*e*	*l*	*l*	*s*	*!*	
CIPHERTEXT:	K	G	E	W	L	Z	A	F	Y		K	E	W	D	D	K	!	

Answer C. key = 23

plaintext:	*i*	*t*		*m*	*i*	*g*	*h*	*t*		*c*	*r*	*a*	*c*	*k*		*u*	*p*	*.*
CIPHERTEXT:	F	Q		J	F	D	E	Q		Z	O	X	Z	H		R	M	.

Answer D. key = 12

plaintext:	*b*	*e*	*c*	*a*	*u*	*s*	*e*		*s*	*h*	*e*		*r*	*a*	*n*			
CIPHERTEXT:	N	Q	O	M	G	E	Q		E	T	Q		D	M	Z			
plaintext:	*a*	*w*	*a*	*y*		*f*	*r*	*o*	*m*		*t*	*h*	*e*		*b*	*a*	*l*	*l*
CIPHERTEXT:	M	I	M	K		R	D	A	Y		F	T	Q		N	M	X	X

Caesar Ciphers: Cracking

What if you find a secret message but you don't know how it was encrypted? Maybe you know the Caesar cipher was used, but you don't know the key. In that case, you only have to figure out one letter to know how much the alphabet was shifted.

If you guess one letter, you can set your Caesar wheel to correctly decrypt that letter and then use that setting to decrypt the rest of the message. Or, you can find the row that correctly decrypts that letter in the Vigenère square and use it to decrypt the rest.

Crack the following, which were encrypted with Caesar ciphers. You will know you are on the right track when you get something that makes sense.

1. *many clues help decrypt a caesar*
DREP TCLVJ YVCG UVTIPGK R TRVJRI

cipher *(key = 17)*
TZGYVI.

2. *the small words are very helpful (key=11)*
ESP DXLWW HZCOD LCP GPCJ SPWAQFW.

3. *i'll think about that (key = 12)*
U'XX FTUZW MNAGF FTMF.

4. *thiswasharderbecausetherewerenospace*
CQRBFJBQJAMNAKNLJDBNCQNANFNANWXBYJLN

sbetweenwords (key=9)
BKNCFNNWFXAMB.

5. *usually the most common letter is e*
ZXZFQQD YMJ RTXY HTRRTS QJYYJW NX J

but not always (key = 5)
GZY STY FQBFDX.

Cipher Wheels