

Caesar Cipher

Teacher Materials

Students will be able to understand the basics of how shift or Caesar Cipher works and is created, decode various messages using a simple shift cipher, and encode messages using a simple shift cipher.

Acknowledgements and License

This activity was contributed by Randy Henderson, McMillan Magnet School and Crista Goehring, Westside Middle School for UNO's TED 8006 course. Background information taken from Wikipedia, https://en.wikipedia.org/wiki/Caesar_cipher.

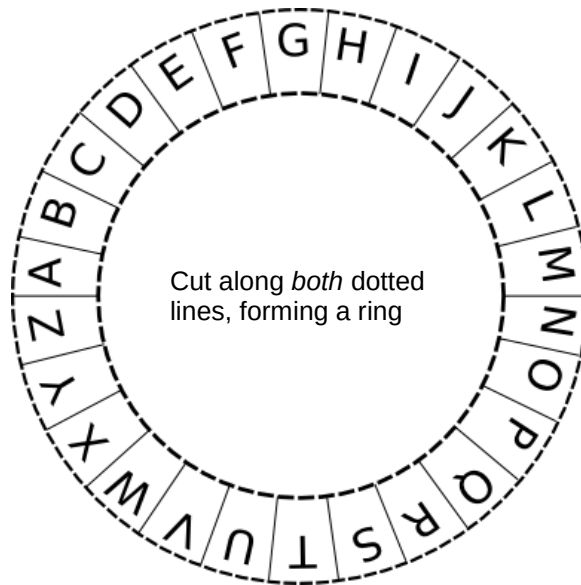
This activity is based off an activity from Crypto Corner,
<http://crypto.interactive-maths.com>.

To create your own Caesar Cipher, visit <http://www.raftbayarea.org/ideas/resources/730/Caesar%20Cipher%20Disc%20-%20Blackline%20Master.pdf>

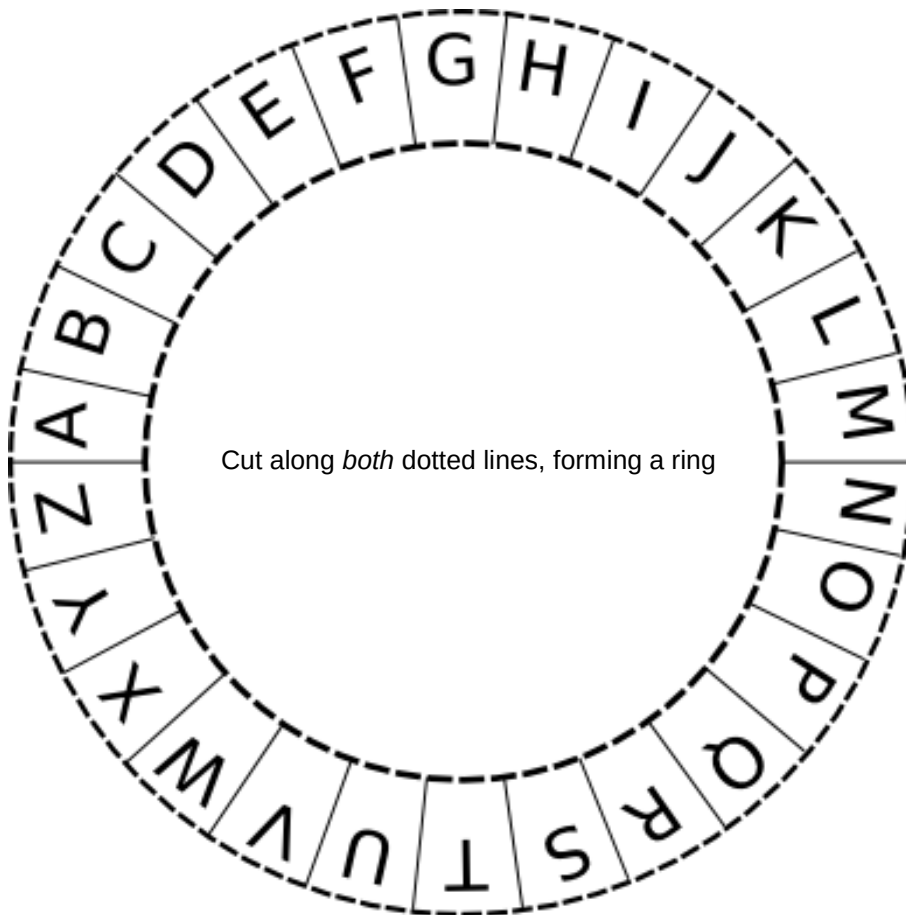
You can 3D print Caesar Ciphers using <https://www.thingiverse.com/thing:14891> or <https://www.thingiverse.com/thing:18315> or <https://www.thingiverse.com/thing:1706210>.

Caesar Cipher Disc - Black Line Master

Small template



Large template



Lesson Details

Grade Level: 6th-10th graders

Activity Length: 10-20 minutes

Format: Students working in groups, materials for 2 groups

Connection to Standards

This activity contains content and practices addressing elements of the following CSTA K-12 Computer Science Standards (2017):

CSTA Std	Description
1A-AP-09	Model the way programs store and manipulate data by using numbers or other symbols to represent information.
2-NI-06	Apply multiple methods of encryption to model the secure transmission of information.
2-DA-07	Represent data using multiple encoding schemes.
2-IC-23	Describe tradeoffs between allowing information to be public and keeping information private and secure.

This activity contains content and practices addressing elements of the following Nebraska K-12 Technology Scope & Sequence Standards:

NE Tech Standard	Description
Computational Thinking 1	Create algorithms, or series of ordered steps, to solve problems.
Computational Thinking 3	Collect, analyze, and represent data effectively.
Computational Thinking 4	Demonstrate and understanding of how information is represented, stored, and processed.

Bin Materials Checklist

bin materials checklist

#	Description
2	Laminated Caesar Cipher wheels OR printed Caesar Cipher wheels
1	Notepad
4	Pencils
	Question Worksheets
1	Pencil Sharpener

Lesson Vocabulary Words

cipher a secret or a disguised way of writing; a code

cryptography the practice and study of techniques used for securing communication and information from unattended readers, enemies or adversaries.

decoding/ decryption returning the encoded/ encrypted message back to its plain text form

encoding/ encrypting converting information or data into another system

key the word or letter that lets the receiver of the encrypted message decode the message correctly

plain text text that is not written in code. Messages before they have been encoded or encrypted are in plain text

shift the amount of numbers (+ or -) used offset the alphabet and create the cipher

substitution the action of replacing something with another thing. In this case- letters

Lesson Setup / Introduction

This CS activity shares the theme of ciphers and encryption and would fit in any lesson involving cyber security or cryptography.

Students learn about the history and uses of cryptography and practice their math skills as they decode and encode Caesar Ciphers (Shift Cipher). The students will have hands-on practice decoding and encoding messages using the Caesar Cipher. All Activities would work for middle level or higher and work from the least challenging to most challenging in the order they are presented.

Connection to Computing

This activities introduces cryptography. Students practice encoding and decoding of plain text using a cipher key. Cryptography is an important component of cybersecurity; cryptography keeps information private and secret by converting it into a secret code. A Caesar Cipher was one of the earliest ciphers, but it is fairly easy to break, particularly for computers, because it is easy to use information about letter frequency - e.g. E is the most common letter in English - to use brute force to figure out what a message says.

Answer Key

Challenge Answers

1. Using a *shift of 4* decode this message:

Message:

GSQTYXIV WGMIRGI MW GSSP!

Answer: **COMPUTER SCIENCE IS COOL!**

2. Using a *shift of 11* decode these two messages:

Message: **"T'X DZCCJ, TQ JZF HPCP CTRSE, T'O IRCPP HTES JZF."**

Answer: **"I'M SORRY, IF YOU WERE RIGHT, I'D AGREE WITH YOU."**

Message: **"ESP TYEPCYPE? TD ESLE ESTYR DETWW LCZFYO?"**

Answer: **"THE INTERNET? IS THAT THING STILL AROUND?"**

3. Using a *shift of 18* decode this message:

Message: **"UGEHMLWJK SJW MKWDWKK. LZWQ USF GFDQ YANW QGM SFKOWJK."**

Answer: **"COMPUTERS ARE USELESS. THEY CAN ONLY GIVE YOU ANSWERS."**

4. Using a *shift of 20* decode this message:

Message: **NLOMN SIOL WUFWOFUNIL. CN'M MIGNYBCHA NI WIOHN IH.**

Answer: **TRUST YOUR CALCULATOR. IT'S SOMETHING TO COUNT ON.**

5. Using a *shift of 23* decode this message:

Message: **F'J KLQ XKQF-PLZFXI; F'J GRPQ KLQ RPBO COFBKAIV.**

Answer: **I'M NOT ANTI-SOCIAL; I'M JUST NOT USER FRIENDLY.**

Extension 2 Answers

1. Key: **Shift + 3**

Coded message: **AIK'QD FSBRM QEBPE FM!**

Answer: **DON'T GIVE UP THE SHIP!**

2. Key: **Shift + 4**

Coded message: **WJEHH SEJZX HKSOJ KCKKZ**

Answer: **AN ILL WIND BLOWS NO GOOD**

3. Key: **Shift + 6**

Coded message: **XIH'NF IIEUA CZNBI LMYCH NBYGI ONB**

Answer: **DON'T LOOK A GIFT HORSE IN THE MOUTH**



4. Key: **Shift + 5**

Coded message: **BZOOD IBVIV DNVWM ZZUZ, IJO!**

Answer: **GETTING AN N IS A BREEZE, NOT!**

5. Key: **Shift + 7**

Coded message: **UNLRT LTUXT OXK LE RTLTY HQPBL XTLTG
HPEUN MPAHZ BOXLT AHM?**

Answer: **BUSY AS A BEAVER, SLY AS A FOX, WISE AS AN OWL,
BUT WHO GIVES A HOOT?**

Caesar Cipher

Student Instructions

Background

The earliest and simplest form of ciphers is known as “mono-alphabetic substitutions”. This is a system of encryption where every occurrence of a particular plaintext letter in the alphabet is replaced by a ciphertext letter. This will generate a second alphabet where the 26 letters are in different positions. Pairing the two alphabets together will yield a one-to-one mapping of the plaintext letter to its encrypted counterpart.

The Caesar Cipher is an example of such a substitution cipher. It is attributed to Julius Caesar who used it to communicate with his generals. Also known as a shift cipher, it replaces each plaintext letter with a letter that is a fixed number of places down the alphabet. For example, with a shift of three, a B in the plaintext alphabet becomes an E in the ciphertext one. -Wikipedia (https://en.wikipedia.org/wiki/Caesar_cipher)

As such, this is the full cipher alphabet with 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

Hand-Outs

Caesar Challenge 1: Using the Caesar Cipher wheels try to break the following ciphers.

1. Using a *shift of 4*, decode this message:

GSQTYXIV WGMIRGI MW GSSP!

Plain Text Answer:

2. Using a *shift of 11*, decode these two messages:

"T'X DZCCJ, TQ JZF HPCP CTRSE, T'O LRCPP HTES JZF."

Plain Text Answer:

"ESP TYEPCYPE? TD ESLE ESTYR DETWW LCZFYO?"

Plain Text Answer:

3. Using a *shift of 18*, decode this message:

"UGEHMLWJK SJW MKWDWKK. LZWQ USF GFDQ YANW QGM SFKOWJK."

Plain Text Answer:

4. Using a *shift of 20*, decode this message:

NLOMN SIOL WUFWOFUNIL. CN'M MIGNYBCHA NI WIOHN IH.

Plain Text Answer:

5. Using a *shift of 23*, decode this message:

F'J KLQ XKQF-PLZFXI; F'J GRPQ KLQ RPBO COFBKAIV.

Plain Text Answer:

Extension 1:

Using the Caesar Cipher wheel, try to break additional ciphers. See how fast you can decrypt and figure out the message.

Ask your teacher for the Caesar Cipher Extension 2 worksheet.

Extension 2:

Using the Caesar Cipher wheel, create your own secret messages for others to decode. Remember to provide the key (shift)

Ideas:

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

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.

Enciphered message 1:

Enciphered message 2:

Extension 2- Caesar Cipher Worksheet

1. Key: **Shift + 3**

Coded message: **ALK'QD FSBRM QEBPE FM!**

Answer:

2. Key: **Shift + 4**

Coded message: **WJEHH SEJZX HKSOJ**

Answer:

3. Key: **Shift + 6**

Coded message: **XIH'NF IIEUA CZNBI LMYCH NBYGI ONB**

Answer:

4. Key: **Shift + 5**

Coded message: **BZOOD IBVIV DNVWM ZZUZ**

Answer:

5. Key: **Shift + 7**

Coded message: **UNLRT LTUXT OXK LE RTLTY HQPBL XTLTG
HPEUN MPAHZ BOXLT AHHM?**

Answer:



Resupply

- Sharpen Pencils