

Vigenère Cipher

Teacher Materials

Students will understand the basics of how Vigenère Ciphers work and are created, decode various messages using a shift cipher, and encode messages using a shift cipher.

Acknowledgements and License

This activity was contributed by Crista Goehring, Westside Middle School for UNO's TED 8006 course. Activity introduction taken from Wikipedia, https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher.

Lesson Details

Grade Level: 6th-10th graders

Activity Length: 20-30 minutes

Format: Students working in pairs, materials for 3 pairs

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

#	Description
3	Vigenère squares
3	Dry erase markers
3	Pencils
2	Eraser rags
3	Activity cards

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 Vigenère Ciphers. For the students to have hands-on practice decoding and encoding messages using the Vigenère 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

One of the things computers can do really well is *encryption* or converting plain text into secret text. Encryption can be used to keep secret things secret, like passwords and bank account information. This is particularly important for data that is transmitted over networks where others might be listening.

The Vigenère Cipher is a more complex version of the Caesar Cipher. The Caesar Cipher, like all simple substitution ciphers, is fairly straightforward to break using simple frequency analysis - knowing the most frequently-used letters can lead to decoding the text. A Vigenère Cipher is a polyalphabetic substitution cipher, where any letter can be represented by any other rather than just by one. However, modern computers can still break a Vigenère Cipher fairly quickly.

The use of a shared key to decode the Vigenère Cipher is a notable feature which is a building block to modern public key encryption.

Further Related Resources

- https://en.wikipedia.org/wiki/Vigenere_cipher
- <http://www.counton.org/explorer/codebreaking/vigenere-cipher.php>

Answer Key

Key	G	O	O	D	G	O	O	D	G	O	O	D
Plain Text	T	H	E	D	A	B	I	S	D	E	A	D
Coded Message	N	T	Q	A	U	N	U	P	X	Q	M	A

Key: GOOD

Decoded Message: THE DAB IS DEAD

Key	C	A	K	E	C	A	K	E	C	A	K	E	C	A	K	E	C	A	K	E	C	A	K	E
Plain Text	H	A	P	P	Y	B	I	R	T	H	D	A	Y	G	R	A	C	E	H	O	P	P	E	R
Coded Message	F	A	F	L	W	B	Y	N	R	H	T	W	W	G	H	W	A	E	X	K	N	P	U	N

Key: CAKE

Decoded Message: HAPPY BIRTHDAY GRACE HOPPER

Key	D	O	G	D	O	G	D	O	G	D	O	G	D	O	G	D
Plain Text	P	R	O	G	R	A	M	M	I	N	G	I	S	F	U	N
Coded Message	M	D	I	D	D	U	J	Y	C	K	S	C	P	R	O	K

Key: DOG

Decoded Message: PROGRAMMING IS FUN

Vigenère Cipher

Student Instructions

Background:

The **Vigenère Cipher** is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of poly-alphabetic substitution. Though the cipher is easy to understand and implement, for three centuries it resisted all attempts to break it; this earned it the description **le chiffre indéchiffrable** (French for 'the indecipherable cipher'). Many people have tried to implement encryption schemes that are essentially Vigenère Ciphers. Friedrich Kasiski was the first to publish a general method of deciphering a Vigenère Cipher, in 1863.

Challenge:

For this challenge you will be using a Vigenère square. To encode a message with a Vigenère square you first decide on a “key”, a word that will be used to encode and decode the message. Write that key word over the message and repeat it until each letter in the message has a letter in the key word above it.

Then, using the Vigenère square, look in the *top row of letters to find the letter in your key*. Find the *letter from your message in the first column*. Find where that row and column intersect and write that letter (that is the encoded character). Keep repeating this process until the whole message is encoded.

For example let's encode the message “hello world” using the key “pizza”

key	P	I	Z	Z	A	P	I	Z	Z	A
message	H	E	L	L	O	W	O	R	L	D
encoded message	W	M	K	K	O	L	W	Q	K	D

Look in the box to find the challenge cards. The cards have the key and the encoded message, your task is to use the information above and the Vigenère square below to try and decode the messages. Write the decoded letters in the blank squares using the dry erase markers in the box and show a teacher when you're done. (**Hint:** you have to work backwards to decode a message).

Hand-Outs

	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

Key												
Plain Text												
Coded Message	N	T	Q	A	U	N	U	P	X	Q	M	A

Key: GOOD

Decoded Message: _____

Key																								
Plain Text																								
Coded Message	F	A	F	L	W	B	Y	N	R	H	T	W	W	G	H	W	A	E	X	K	N	P	U	N

Key: CAKE

Decoded Message: _____

Key																		
Plain Text																		
Coded Message	M	D	I	D	D	U	J	Y	C	K	S	C	P	R	O	K		

Key: DOG

Decoded Message: _____



Resupply

- Test dry erase markers to make sure they still work
- Replace eraser rag if needed