Cryptography [DRAFT]

Summary

There is a large amount of sensitive information stored on computers and transmitted between computers, including account passwords, trade secrets, and personal financial information. To keep this information hidden from third parties who may want access to it, cryptographic techniques must be used to encrypt it, making it difficult or impossible to actually recover the original data for anyone but the intended recipient. Because most modern cryptographic algorithms involve high-level mathematical concepts, this activity will not discuss them. We will, however, investigate the general ideas behind cryptography and introduce the idea of analyzing the strength of different kinds of encryption.

Grade Level: 3rd - 4th

Subject: Computer Science

Length: 50 minutes

CSTA/Common Core Standards Alignment

CSTA - Algorithms and Programming - 1A-AP-08
Model daily processes by creating and following algorithms (sets of step-by-step instructions) to complete tasks.
Ciphers are distinct sets of instruction for how to convert one letter to another letter.

CSTA - Algorithms and Programming - 1B-AP-11
Decompose (break down) problems into smaller, manageable subproblems to facilitate the program development process.
Decompose the frequency analysis problem down into small words before expanding to larger words.

CSTA - Data Analysis - 1B-DA-06
Organize and present collected data visually to highlight relationships and support a claim.
Use diagrams to represent data in the frequency analysis and use those figures to make conclusions about the ciphers.

Cryptography [DRAFT]

Computational Thinking Alignment

Abstraction:
Developing a shift key serves as an abstraction of the entire Cesar Cypher key itself.

Problem Decomposition:
Without knowing a shift key, what strategies could you use to break the deciphering problem down into a simpler problem?

Pattern Recognition:
Use frequency diagrams to recognize patterns in the frequency data.

Objectives

The purpose of this activity is to (1) provide students an introduction into the world of cryptography through the Caesar cipher and (2) help students understand how cryptography is used in computer science. Students will explore data representation and protection by using ciphers to represent the original data in an altered form. Students will learn how patterns can be used to create messages and also read messages.

Timeline

Activity	**Time**	**Activity Location**
Introduction	10 min	Lesson Plan
Making a Cipher Wheel (Optional)	10 min	CipherWheel.pdf
Worksheet - The Caesar Cipher	10 min	CryptographyWorksheets.pdf
Encode Surprise Party	15 min	CryptographyWorksheets.pdf
Decode Surprise Party	10 min	CryptographyWorksheets.pdf
Wrap-Up Discussion	5 min	Lesson Plan
Frequency Analysis Discussion (Optional)	10 min	CryptographySlides.pdf
Total	**>50 min**	

Cryptography [DRAFT]

Materials

❏ CryptographyWorksheets.pdf	one per student
❏ CryptographySlides.pptx	1
❏ Cipher Wheel (Optional)	one per student
❏ Scissors (Optional)	one per student
❏ Paper fastener or split pin (Optional)	one per student

Attachments

- CryptographyWorksheets.pdf
- CryptographySlides.pptx
- CipherWheel.pdf (Optional)

Procedure

Introduction

Cryptography is the study of encryption and decryption of messages. Cryptography is widely used in computer science. For example traffic on the Internet is often encrypted and relies on consistent cipher generation and transmission in order for secure messages to be sent. The principle of encoding a message is to ensure that only the intended receiver understands the message. Thus, when encoding a message, it is important to define a consistent “cipher”, which is known by the recipient beforehand. A “cipher” determines how the message is encrypted.

One of the earliest known ciphers is the Caesar cipher, which Julius Caesar used to send secure messages to generals in the Roman army. The Caesar cipher shifts the alphabet system by a predetermined amount so that the beginning letter of the encrypted messages alphabet is different than that of the original message. For example, a Caesar cipher that translates the message “BAD” into “EDG” is said to have a shift of 3, i.e., each letter in the original message is shifted 3 letters forward in the alphabet. This cipher is relatively easy to break, due to the limited number of ciphers possible (25, to be exact). It is, however. a good example of the basic principles of cryptography.

Lesson Vocabulary

- Cryptography - the study of encryption and decryption of messages
- Encoding- obfuscating a message
- Decoding- determining the original message from the encrypted message

Ask students to think about what kinds of information might need to be kept hidden. What if all of our passwords were transmitted over the internet without any sort of encryption?

Take ideas about how we might protect sensitive information.

Next, explain the idea of encrypting a message (i.e., modifying it to be unrecognizable) before transmission in order to make it hard for someone who intercepts the message to actually read the message (unless they can determine how to decode the message).

The following example provides students with the idea of cryptography. Tell the students you are going to encrypt a message using a cipher or “key” of size 2. Ask the students if they can decrypt the following message: eqorwvgt [**answer**: computer]

Body of Lesson and Activities

Making a Cipher Wheel (Optional)

A cipher wheel can make encoding and decoding easy! Use the CipherWheel worksheet to create cipher wheels to use with the remaining activities (not required). A cipher wheel consists of two disks, both of which have the alphabet around the perimeter. The larger disk will be the “stationary” disk and will not move. This represents our original alphabet. The second disk will be moved the number of times necessary to represent the cipher key. For example, if we are using the key 3, rotate the disk 3 letters counter clockwise so that the ‘D’ and ‘A’ are aligned. Now you can easily encode and decode messages!

To construct a cipher wheel:

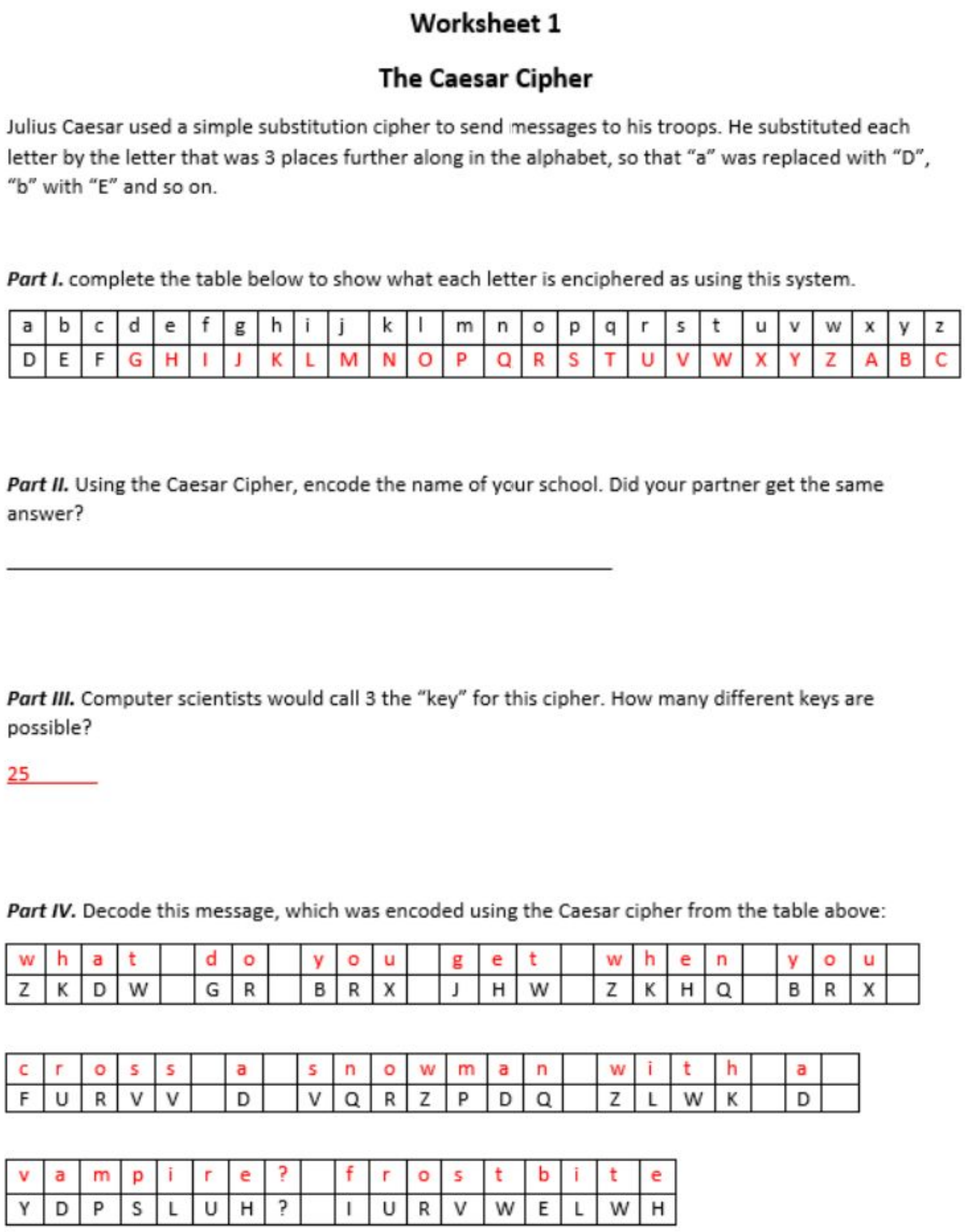
1. Have the students carefully cut out each of the disks in the cipher wheel worksheet. If you are not comfortable having the students do this themselves, you may precut the disks for them
2. Use a pencil to CAREFULLY make a hole in the center of each disk.
3. Push a paper fastener or split pin through the hole you created. Bend the legs of the split pin so that the wheels stay together and the wheel lies flat on the table.

Worksheet - The Caesar Cipher

This worksheet introduces a very simple kind of encryption which was used by Julius Caesar. The worksheet walks the students through the mechanics of the cipher, and lets them practice using it on their own. In other words, the worksheet allows students to sharpen their skills in encoding and decoding a variety of messages using keys.

Cryptography [DRAFT]

The Caesar Cipher Answer Key:



Worksheet 1

The Caesar Cipher

Julius Caesar used a simple substitution cipher to send messages to his troops. 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.

Part I. 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	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Part II. Using the Caesar Cipher, encode the name of your school. Did your partner get the same answer?

____

Part III. Computer scientists would call 3 the "key" for this cipher. How many different keys are possible?

25

Part IV. Decode this message, which was encoded using the Caesar cipher from the table above:

w	h	a	t		d	o		y	o	u		g	e	t		w	h	e	n		y	o	u	
Z	K	D	W		G	R		B	R	X		J	H	W		Z	K	H	Q		B	R	X	

c	r	o	s	s		a		s	n	o	w	m	a	n		w	i	t	h		a	
F	U	R	V	V		D		V	Q	R	Z	P	D	Q		Z	L	W	K		D	

v	a	m	p	i	r	e	?		f	r	o	s	t	b	i	t	e
Y	D	P	S	L	U	H	?		I	U	R	V	W	E	L	W	H

Activity - Team Worksheet

Divide the class into groups of four. Explain that each group is trying to organize a surprise party without the lucky person finding out. The team will need to make up the details - who will the surprise party be for? Where? What game or activity will you do at the party? What gift will you bring? You may want to encourage students to use answers that are fairly short (e.g., 1-3 words, not entire sentences).

Packet Villain: The first part of the worksheet is to practice encoding/decoding when the exact cipher is not specified (but limited to one of 3, to keep it fairly simple). This exercise is called Packet Villain. This small practice should not take long, and gives practice encoding a known message (the partner's name).

Surprise Party: Next the teams should encode the details of the party. Each person should encode ONE detail. After the encoding is done, have the teams swap and see if they can determine the details. Note that this will be harder than the previous example, as students won't know a) which cipher was used or b) what the answer is. If a team is really struggling, you might ask the other team to tell which cipher they used. As teams finish the decoding, share some of the party details with the entire class.

Discussion

People often rely on encryption when using the internet. Some of the uses of encryption include:

- Protecting credit card details or other sensitive information in online transactions.
- Protecting email communication from eavesdropping third parties.
- Verifying the authenticity of software updates to prevent installation of malicious software.

Without strong cryptographic algorithms, most modern Internet infrastructure would fail.

A simple substitution cipher can be broken quickly by a modern computer. Modern cryptography uses the idea of computational intractability (problems which take unreasonable amounts of time to solve).

Many algorithms are based on large prime numbers because:

- To multiply two large primes can takes approximately one millionth of a second
- To recover the original two factors when unknown would take approximately 200,000 years

Frequency Analysis Discussion (Optional)

Modern decryption methods often use the context of encrypted words (i.e., what words typically come before or after this word?). Also decryption methods use the frequency that different letters tend to occur in the English language. This material is covered in CryptographySlides.pdf.