ROI

INDIANA UPLANDS | PROUD PARTNER

Grade 6-8 STEM Challenge

Cryptography

Inspired by Barry, an Information Assurance Analyst in the Indiana Uplands.

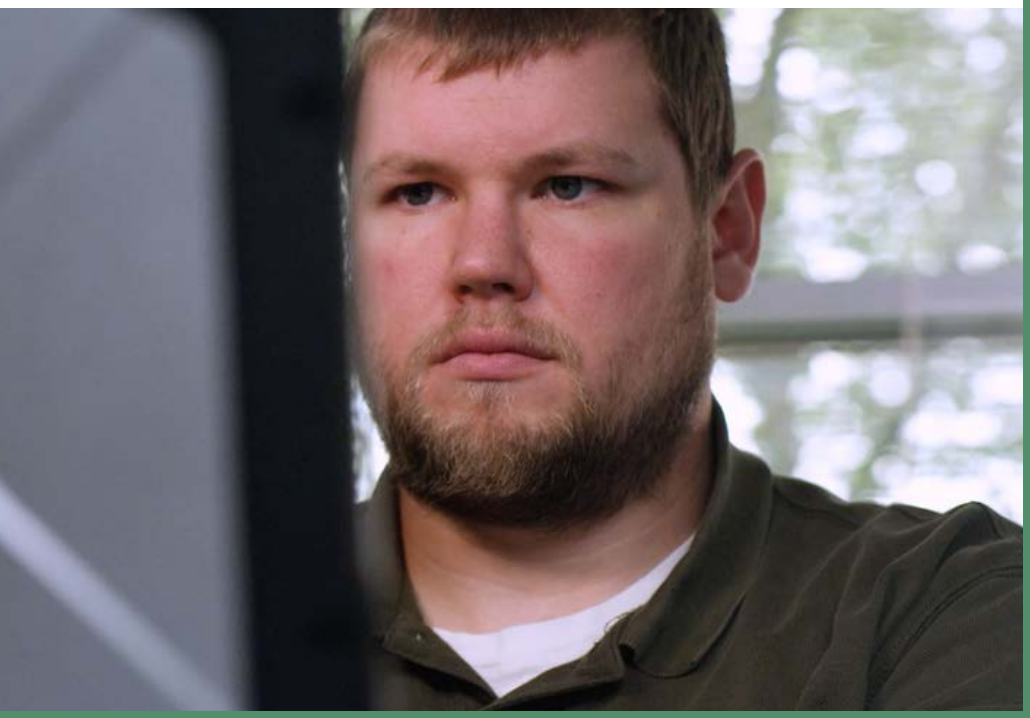
Published by Regional Opportunity Initiatives, Inc.

GRADE 6-8 STEM CHALLENGE

Cryptography

Inspired by Barry, an Information Assurance Analyst in the Indiana Uplands.

Students will learn how ciphers and encryption are used to protect information from prying eyes.



LESSON TIMELINE

DAY 1

- View the job shadow video, "Barry - Information Assurance Analyst"
- Introduce the challenge (10 minutes)
- Cipher Practice (20 minutes)
- Career extnsions and exploration (15 minutes)

DAY 2

- Reframe the day (5 minutes)
- Suprpise Party game (45 minutes)

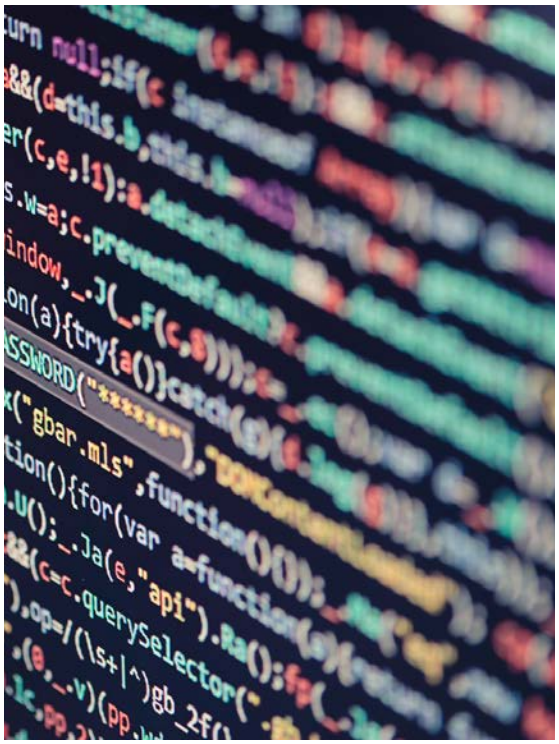
RECOMMENDED SUPPLIES

- Caesar Cipeher Worksheets, 1 per student
- The Secret Party worksheets, 1 pers student
- Scratch paper
- Pencils

CAREER CONNECTION AND LESSON OVERVIEW

Barry is an information assurance analyst for TriStar Engineering, a defense contractor in southern Indiana. Information security and cybersecurity professionals like Barry work to protect many different kinds of data, including banking information, health records, and people's personal information. This requires an in-depth knowledge of not only computer systems and programming but also encryption strategies.

Ciphers and shift codes are a simple way for students to practice and understand encryption and decryption strategies. While the encryption tools Barry uses for his job are much more complex, these types of codes and keys are the foundation of modern cryptography. In this activity, students will learn how ciphers and encryption are used to protect information from prying eyes.



IN THIS CHALLENGE, STUDENTS WILL:

- Learn about encryption techniques used to protect information.
- Create and use their own Caesar Cipher to send messages to their classmates.
- Learn about cybersecurity professionals and how they protect information.

Standards

Science & Engineering Process Standards

SEPS.1 Posing Questions (for science) and defining problems (for engineering)
SEPS.2 Developing and using models and tools
SEPS.4 Analyzing and interpreting data
SEPS.6 Constructing explanations (for science) and designing solutions (for engineering)
SEPS.8 Obtaining, evaluating, and communicating information

Preparing for College and Careers

PCC-2.1 Determine roles, functions, education, and training requirements of various career options within one or more career clusters and pathways
PCC-2.2 Analyze career trends, options and opportunities for employment and entrepreneurial endeavors for selected career clusters and pathways
PCC-2.3 Evaluate selected careers and pathways for education requirements, working conditions, benefits, and opportunities for growth and change
PCC-2.4 Use appropriate technology and resources to research and organize information about careers

Computer Science

6-8.DI.3 Represent data in a variety of ways (e.g., text, sounds, pictures, and numbers), and use different visual representations of problems, structures, and data (e.g., graphs, charts, network diagrams, flowcharts)
6-8.IC4 Describe ethical issues that relate to computers and networks (e.g., security, privacy, ownership, and information sharing), and discuss how unequal distribution of technological resources in a global economy raises issues of equity, access, and power

Grade 6-8 Employability Skills

6-8.WE.4 Understand failure as an opportunity for growth
6-8.WE.7 Understand and employ strategies for resisting pressures to engage in dishonest or unethical activities
6-8.LS.4 Identify possible career choices and high school course selection using self-assessment (including an appraisal of strengths, interests, and values)
6-8.LS.12 Use prediction and evaluation skills to develop potential solutions

Planning and Implementation

CRYPTOGRAPHY

Essential Vocabulary

- CIPHER: An algorithm for obscuring information so it can only be read by a specific person with a key to the code.
- CRYPTOGRAPHY: The art of writing or solving codes.
- ENCODE: To convert information into a coded form.
- DECODE: To convert a coded message into an easily understood format.
- ENCRYPTION: The process of converting information or data into a code, especially to protect it from unauthorized access.
- DECRYPTION: The process of taking encrypted data or information and converting it back into an understandable form.

In this challenge, students will:

- Learn about encryption techniques used to protect information.
- Create and use their own Caesar Cipher to send messages to their classmates.
- Learn about cybersecurity professionals and how they protect information.

Before Class:

- Read the activity outline sheet and leader notes to become familiar with the activity.
- Gather necessary materials. Be sure that you have printed enough student sheets for the class.

Guiding Questions

1. What does it mean for information to be “secure?” Why might someone want to make a message or data secure?
2. What are some ways that we can ensure that only the people a message is meant for can read it?
3. What role might this play in cybersecurity? What about history?

Day 1

Introduction

Show students Barry's job shadow video, available at https://www.regionalopportunityinc.orb/barry. Barry is an information assurance analyst, a person whose job it is to make sure that data is secure and can only be accessed by people with permission. One way to do this is through encryption, a process of encoding messages to keep them secret so that only an authorized person with the decryption key can access the information.

Cryptography is the study of encryption and decryption of messages. The goal of any encryption strategy is to ensure that only the intended receiver can understand the message. To be able to correctly (and efficiently) decode the message the recipient has to have access to the cipher. The cipher is the key that determines how the information is encrypted and decrypted.

The Caesar cipher is named for the roman emperor Julius Caesar, who used it to send messages to his military leaders. Cesar ciphers are shift ciphers, where each letter in the text is replaced by a letter some fixed number of positions down the alphabet. Caesar's original cipher was a "Shift 3" cipher, where each letter was encoded by replacing it with the one 3 letters after it. An A would be encoded as a D, a G as a J, etc.

Orignal →

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

Encoded →

So, the phrase "this is a cipher" would be: WKLV LV D FLSKHU

For our purposes, we'll be putting the original messages in lowercase letters and the shifted, encrypted messages in all capital letters. This cipher is relatively simple to break if you know it's a shift—there are only 25 possible keys—but it's a good way to learn about how to conceal information. Cryptography is widely used in computer science. Almost anything you send over the internet has some level of encryption to ensure privacy.

Brainstorm

To get students thinking:

1. Ask them to brainstorm a list of the kinds of information or things that people might want to be kept hidden.
2. Ask students to brainstorm how they might protect their own sensitive information.
    - For example: how do they keep their younger siblings out of their phone?
3. Introduce the Caesar Cipher activity. Provide a few example words and see if they can decrypt them using the Caesar shift 3 cipher.

Ceaesar Ciphers

Provide each student with the Caesar Cipher worksheet (page S1). This will give them an opportunity to practice using different ciphers and keys on their own. This should take about 20 minutes. If students complete the Caesar Cipher worksheet quickly, have them move on the Secret Party activity.

Day 2

The Secret Party

For this exercise, students will be planning a surprise party for a friend and will need to communicate the details without spoiling the surprise by creating their own cipher shift code. Group students into teams of 3 to 4 and have them work through the Secret Party activity. After the encoding is done, ask teams to swap their plans and see if they can decipher the details. This will be harder because the students will not know which cipher shift was used or what the answers should be.

If teams really struggle with cracking other students' ciphers, they can ask the encoding teams for a hint (what the shift was, what a word is, etc.) This portion of the activity could take 45 minutes or longer, depending on how complex the party instructions are.

Discuss and Report

Every time you use the internet or your cell phone some or all of the information you're sending is encrypted. Prompt students to brainstorm information that may need to be kept secret. Responses may include:

- Banking or credit card info
- Emails and texts
- Software
- Medical records

The Caesar cipher is not strong enough on its own to protect this kind of info. In fact, modern computers can crack a Caesar cipher in seconds. New encryption algorithms are designed so that the password system only ever sees the encrypted version, never the actual password, making it nearly impossible to crack. Also: many systems change their decode key at regular intervals so that knowing how to crack the cipher today doesn't mean that you'll be able to decode the information tomorrow.

Prompt students to think about what makes an encryption system strong? Weak?

Career Exploration and Extension

Prompt students to think about and research what a career as an Information Assurance Analyst might entail.

- What does an information assurance analyst do all day? What does Barry do?
- What kind of training would a student need to become an information assurance analyst? What about a cybersecurity expert in general? What other jobs are like this?
- Are jobs like Barry's in demand? Will more people be hired for cybersecurity and information assurance jobs in the future? What kind of education is needed for these types of jobs? Where could a student be trained locally for a career in information assurance or cybersecurity?

Name: _____

The Caesar Cipher

Code Practice

Julius Caesar used this simple substitution cipher to send messages to his generals. In it, a letter is substituted with the letter 3 places down the alphabet so an A would be encoded as a D, a G as a J, etc.

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																						B	C

Using this Caesar cipher, how would you encode and write the name of your school? Check with your neighbor to see if you get the same answer.

_____

Computer scientists and cryptographers call this a “Shift 3” cipher, meaning the “key” to decrypt this code is 3. How many different keys are possible? Why?

_____

_____

_____

Test your skills! Decode the Caesar Ciphered message below.

F	U	B	S	W	R	J	U	D	S	K	B		L	V		D	Z	H	V	R	P	H

Name: _____

Practice

Below are three different version of shift, or Caesar, ciphers. What is the key (the number of letters shifted) for each one?

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
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

Shift key: _____ letters

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
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

Shift key: _____ letters

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
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

Shift key: _____ letters

Name: _____

The Secret Party

Encrypting Data

Your group is planning a surprise party for someone (could be a fellow student, a teacher, a family member, a famous person, etc!) To ensure that the guest of honor doesn't figure out the details you're going to encode them before you send out the invitations. As a group, figure out which team member will be responsible for each part of the party plan. Use one of the four versions of the cipher you've used so far.

When you're done encrypting your "invitations," give you paper to another team to "decrypt."

Who? Who is this party for?

Where? Where is this party going to happen?

Fun! What game or activities are you going to do?

Bring! What gift will you bring?

ACKNOWLEDGEMENTS

Activities developed and written for Regional Opportunity Initiatives by

Adrienne Evans Fernandez
Education Specialist

Emily Menkedick
Education Specialist

ROI would like to thank the following members of our Educator Advisory Group for their gracious support and review of this curriculum:

Amy Gordon
Elementary STEM Coordinator
Brown County Schools

Kelly Grimes
7th Grade Science Teacher
Richland-Bean Blossom
Community School Corporation

Alexis Harmon
Academy of Science &
Entrepreneurship Principal
Monroe County
Community School Corporation

Alison Kern
6th Grade Science Teacher
Mitchell Community Schools

Joann Novak
Business & Computer Science Teacher
Monroe County
Community School Corporation

Jean Schick
High School Science Dept Chair (Ret)
Monroe County
Community School Corporation

Katy Sparks
STEM & Computer Science Coach
Monroe County
Community School Corporation

Tara Weisheit
4th Grade Teacher
Washington Community Schools

IMAGE AND CONTENT CREDITS

Images

Stock photography courtesy of Canva.com
Still video images from "Barry - Information Assurance Analyst," available at http://www.regionalopportunityinc.org/barry

Content

Lesson adapted from "Cryptography," Colorado School of Mines, retrieved from http://csunplugged.mines.edu/Activities/Cryptography/Cryptography.pdf

Cryptography

Inspired by Barry, an Information Assurance Analyst in the Indiana Uplands.

Published by Regional Opportunity Initiatives