Simple Encryption

Unit 4 Lesson 7

Objectives

Students will be able to:

- Explain why encryption is an important need for everyday life on the Internet.
- Crack a message encrypted with a Caesar cipher using a Caesar Cipher Widget
- Crack a message encrypted with random substitution using Frequency Analysis
- Explain the weaknesses and security flaws of substitution ciphers

Aim: How does encryption play a role in how data is transferred on the internet?

Do Now: In your notes! Three minutes!

In your daily life what things do you or other people rely on keeping a secret? Who are these secrets being kept from? How are these things kept secret?

Do Now: In your notes!

In your daily life what things do you or other people rely on keeping a secret? Who are these secrets being kept from? How are these things kept secret?

Now, turn to a partner and discuss your response!

Secrecy is a critical part of our lives, in ways big and small.

Digital commerce, business, government operations, and even social networks all rely on our ability to keep information from falling into the wrong hands.

We need a way to send secret messages...

What is Encryption?

Encryption is the process of encoding a plain text message in some secret way

Encryption is not just for the military and spies anymore. We use encryption everyday on the Internet, primarily to conduct commercial transactions.

In Roman times, Julius Caesar is reported to have encrypted messages to his soldiers and generals by using a simple alphabetic shift - every character was encrypted by substituting it with a character that was some fixed number of letters away in the alphabet.

As a result an alphabetic shift is often referred to as **the Caesar Cipher**.

Task 1: Decode this Message!

Use the Alphabet here to count your shifts

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

serr cvmmn va gur pnsrgrevn

Tips:

- Find a small word and try alphabetic shifts until it's clear that it's an English word
- Remember the letters aren't randomly substituted - the alphabet is just shifted.
- Once you have found the amount of shift the rest comes easily.

ANSWER:

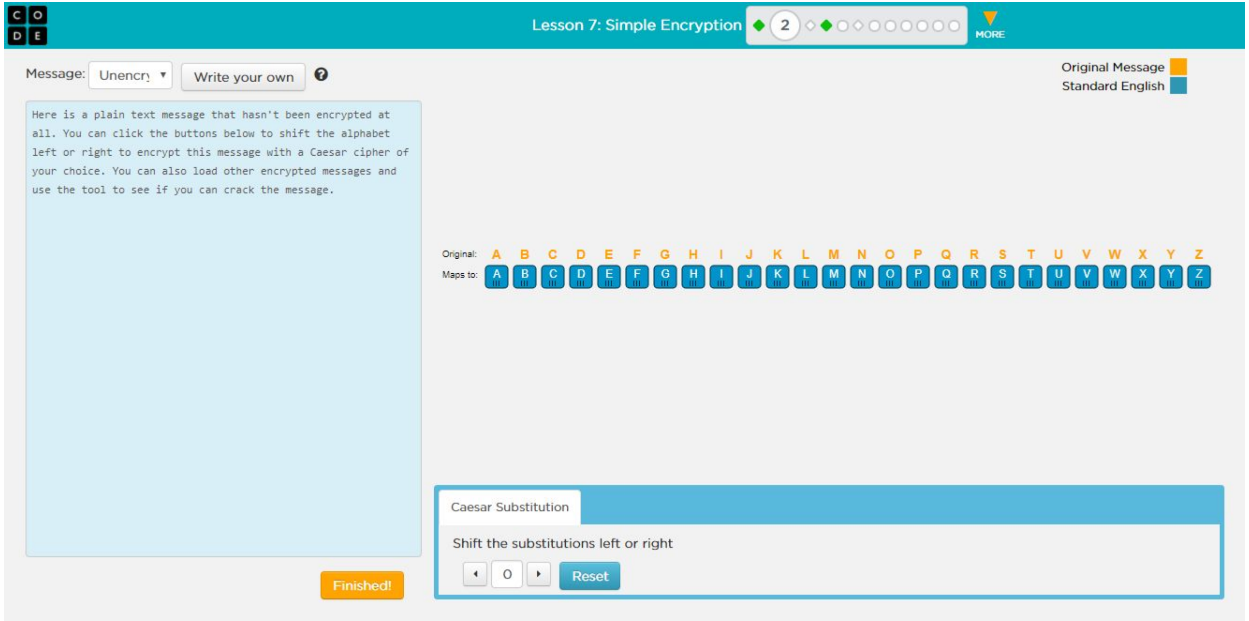
"free pizza in the cafeteria"

the A-Z alphabet is shifted 13 characters

- With this simple encryption technique it only took a few minutes to decode a small message.
- What if the message were longer BUT you had a computational tool to help you?!

Please log into Code.org! →Unit 4 Lesson 7.

We'll be starting with Bubble 2: Crack a Caesar Cipher



Here is a plain text message that hasn't been encrypted at all. You can click the buttons below to shift the alphabet left or right to encrypt this message with a Caesar cipher of your choice. You can also load other encrypted messages and use the tool to see if you can crack the message.

Original:	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
Maps to:	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

Shift the substitutions left or right

◂ 0 ▸

YOUR TASKS: WITH your partner!
Part 1 - Crack a Caesar Cipher

Challenge#2

Goal: Select a message encrypted with a caesar cipher and use the provided widget to “crack” it.

- Experiment with the tool - Click things, poke around, figure out what it’s doing.
- Choose one of the messages from the pull down menu and try to crack it using the tool.
- The goal is to complete **<u>at least two (2)</u>** messages!

Recap on Caesar Cipher Bubbles 3 & 4

Cracking a Caesar cipher is easy...trivial with a computational tool like the one we used.

The next step is to make the encryption slightly harder...

Bubble 5: Break a Random Substitution Cipher

What if instead of shifting the whole alphabet, we mapped every letter of the alphabet to a random different letter of the alphabet? This is called a random substitution cipher.

The new version of the widget you'll see is a more sophisticated version of the encryption tool that shows you lots of different stuff.

You will have 5 minutes to click around and explore this tool!

YOUR TASKS:
Part 2 - Crack a Random Substitution Cipher

Challenge#5

- Using this new tool, choose one of the encrypted messages to crack! Start with #1!
- As usual: you can’t break it. So click on things, poke around.

Recap

Encryption is essential for everyday life and activity

The “strength” of encryption is related to how easy it is to crack a message, assuming adversary knows the technique but not the exact “key”

A random substitution cipher is very crackable by hand though it might take some time, trial and error.

However, when aided with computational tools, a random substitution cipher can be cracked by a novice in a matter of minutes.

The Need For More Robust Encryption

Simple substitution ciphers give insight into encryption algorithms, but as we’ve seen fall way short when a potential adversary is aided with computational tools…our understanding must become more sophisticated.

If we are to create a secure Internet, we will need to develop tools and protocols which can resist the enormous computational power of modern computers.

Summary

Answer the following question in your notes:

Why encryption is an important need for everyday life on the Internet?

HW#4.6: Code.org lesson 5 questions 7,9,10,12