Access Your Potential®

Lesson 8 – Cybersecurity – Simple Encryption

Overview

In this lesson, students are introduced to the need for encryption and simple techniques for breaking (or cracking) secret messages. Students try their own hand at cracking a message encoded with the classic Caesar cipher and also a Random Substitution Cipher. Students should become well-acquainted with idea that in an age of powerful computational tools, techniques of encryption will need to be more sophisticated. The most important aspect of this lesson is to understand how and why encryption plays a role in all of our lives every day on the Internet, and that making good encryption is not trivial. Students will get their feet wet with understanding the considerations that must go into making strong encryption in the face of powerful computational tools that can be used to crack it. The need for secrecy when sending bits over the Internet is important for anyone using the Internet.

Purpose

"Encryption" is a process for transforming a message so that the original is "hidden" from anyone who is not the intended recipient. Encryption is not just for the military and spies anymore. We use encryption everyday on the Internet, primarily to conduct commercial transactions, and without it our economy might grind to a halt. This lesson gives students a first taste of the kind of thinking that goes into encrypting messages in the face of computational tools. Computational tools dramatically increase the strength and complexity of the algorithms we use to encrypt information, but these same tools also increase our ability to crack an encryption. Developing strong encryption relies on knowledge of problems that are "hard" for computers to solve, and using that knowledge to encrypt messages. As a resource, you may wish to read all of Chapter 5 of Blown to Bits. It provides social context which you may want to bring to your classroom.

Agenda

Warm Up (10 min)

- Classic Encryption - The Caesar Cipher

Activity (35 min)

- Part 1 - Crack a Caesar Cipher
- Part 2 - Crack a Random Substitution Cipher

Wrap Up (15 min)

- Video: Encryption and Public Keys
- Discussion
- Career Discussion

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

Preparation

- Examine both versions of the widget

Links

Heads Up! Please make a copy of any documents you plan to share with students.

For the Teacher

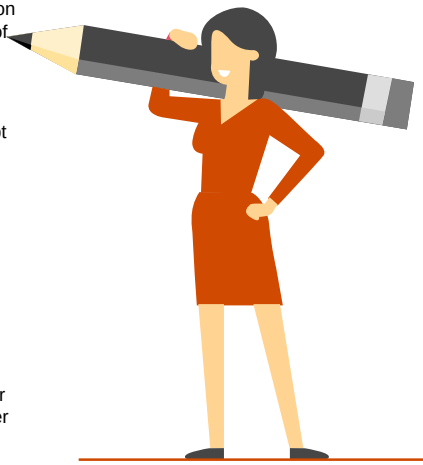
- **Student access to online course –** www.code.org/pwc

For the Students

- **Encryption and Public Keys** – Video

Vocabulary

- **Caesar Cipher –** a technique for encryption that shifts the alphabet by some number of characters
- **Cipher –** the generic term for a technique (or algorithm) that performs encryption
- **Cracking encryption –** When you attempt to decode a secret message without knowing all the specifics of the cipher, you are trying to "crack" the encryption.
- **Decryption –** a process that reverses encryption, taking a secret message and reproducing the original plain text
- **Encryption –** a process of encoding messages to keep them secret, so only "authorized" parties can read it.
- **Random Substitution Cipher –** an encryption technique that maps each letter of the alphabet to a randomly chosen other letters of the alphabet.



pwc

Teaching guide

Warm Up (10 min)

Remarks

Secrecy is a critical part of our lives, in ways big and small. As our lives increasingly are conducted on the Internet, we want to be sure we can maintain the privacy of our information and control who has access to privileged information. 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…

Classic Encryption - The Caesar Cipher

Background

Many of the ideas we use to keep secrets in the digital age are far older than the Internet. The process of encoding a plain text message in some secret way is called **Encryption**

For example 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.**

Prompt

- This message was encrypted using a Caesar Cipher (an "alphabetic shift").
- Let's see how long it takes you to decode this message

(remember it's just a shifting of the alphabet):

Display or write this on the board

seer common vat Gur pnsrgrevn

- Give students about 3-5 minutes to work on cracking the message.

– ANSWER: "free pizza in the cafeteria" – the A-Z alphabet is shifted 13 characters.

Recap

- 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?!

Content corner

If necessary provide context of some facts about the Internet:

- The Internet is not inherently secure.
- Packets traveling across the Internet move through many routers, each of which could be owned by different people or organizations.
- So we should assume all information traveling across the Internet to be public, as if written on a postcard and sent through the mail.

Activity (35 min)

Cracking Substitution Ciphers

In this set of activities students will use two different versions of a simple widget in Code Studio to "crack" a messages encoded with substitution ciphers, including an alphabetic shift and random substitution.

Transition to Code Studio: Encryption Widgets on Code.org (You can either share the URL directly with students, or tell students to navigate to www.code.org/pwc and select Lesson #8 - Simple Encryption)

Teaching tip

Resist the urge to give students a tool or device to aid in cracking this message -- that's coming in the next part of the lesson! Part of the point here is that it's possible without tools. With tools it becomes trivial, as we'll see next. If students are struggling to start here are a few strategy suggestions:

- 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.

Part 1 – Crack a Caesar Cipher

The instructions for this activity are simple - there is no handout:

- Put students in pairs/partners

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.
- If you want to, enter you own message, encrypt it, and have a friend decrypt it.

Give students about 5 minutes to get into the tool and crack a few messages

- Aided with the tool, cracking an alphabetic shift is trivial.
- Once you've done one, it only takes a matter of seconds to do others.

Optional - Pause and Recap

There is a page in Code studio which recaps terminology (encryption, decryption, crack, cipher, Caesar ciper) and poses the next problem.

You may optionally pause here to recap and go over terms if you like or just let students proceed (see activity part 2 below).

Content corner

If you'd like your students to read a little bit about **Historical Cryptography** and cracking ciphers, check out 'Substitution Ciphers and Frequency Analysis' in **Blown to Bits, Chapter 5 - Reading** pp. 165-169.

Part 2 – Crack a random substitution Cipher

After re-capping the first activity make sure **students understand the following before proceeding:**

- 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...

New Challenge

- 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.
- **But what it does is bit of a mystery!** Let's check it out...

Get Cracking

- Have students click to the next bubble to see the frequency analysis version of the widget. (It should look like the screen shown below)

Goal: let students explore for **5-10** minutes to see if they can discover what the tool is showing them and allowing them to do.

The tasks laid out for students in code studio are:

- Figure out what is going on in this new version of the tool
- What information is being presented to you?
- Figure out what the tool let's you do
- As usual: you can't break it. So click on things, poke around.
- If you figure it out you might be able to crack a message encoded with random substitution.

Teaching tip

Don't rush it, but don't linger on cracking Caesar ciphers. Presenting and cracking a caesar cipher should go **pretty fast.**

The widget is pretty self-explanatory. Let students figure out how to use it on their own. The goal here is make points about cracking encryption with computational tools, and start to use some common terms. You should move on to cracking random substitution relatively quickly.

- **After some exploration time regroup** to clarify what the tool is and how it works.
- **If necessary** point out to students that the next level in code studio (the one after the frequency analysis tool) explains a little bit about how frequency analysis works and suggests a few strategies for how to get started.

Give students about 15-20 minutes to crack one of the messages.

- If they finish there are more to try.
- Students can enter their own messages, do a random substitution to encrypt it, then copy/paste the encrypted version and see if a friend can crack it.
- It is possible to get pretty proficient at cracking these messages with the tool.

Wrap Up (15 min)

Video: Encryption and Public Keys

- Show the **Internet: Encryption & Public Keys** – Video

You should know about this video:

- **0:00 to 4:11** covers Caesar and Vigenere ciphers and explains why they are hard to crack
- After 4:11...it explains the difference between encryption that uses symmetric v. asymmetric keys which is **related to material on public key encryption** and is intended as a preview/teaser for more modern encryption techniques.

Use a Discovery-based approach Reminder: Discovery-based introduction of tools in a nutshell:

- Get students into to the tool without much or any introduction
- Give students working in partners a fixed amount of time (5 minutes or so) to poke around and see if they can figure out what it does and doesn't do – typically this might be presented as a mystery worth Investigating
- Ask the group to report what they found
- Teacher fill in any gaps or explanations of how the tool works afterwards

This widget, like all others, are meant as a learning tool. You cannot break it so you are encouraged to let students play and investigate to figure out how the tools work.

These discovery-based methods of introducing tools have been tested in professional development and have worked well for teachers who use this curriculum. This method is effective for a few reasons, but overall students find this approach more engaging and fun, and they tend to be more receptive to, and motivated to hear, explanations of how the tool works after trying to "solve the mystery" themselves.

Wrapping goals

The video re-iterates a number of points that came out in this lesson. In wrapping-up, make sure students:

Understand the relationship between cryptographic keys and passwords.

- A Key is an input to an encryption algorithm. A password is basically the same thing.

Understand why using longer passwords makes them harder to guess.

- Longer passwords increase the number of possible keys making it **Computationally hard** to guess what the key is.

Discussion

As part of wrap up **the major points we want to draw out are:**

- Encryption is essential for every day 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.
- 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.

Here are a couple of thought-provoking prompts you can use to bring closure to the lesson and as an avenue to draw out the points above. Choose one or more.

Prompts

How much easier is it to crack a Caesar cipher than a random substitution cipher? Can you put a number on it?

- For Caesar's Cipher there are only 25 possible ways to shift the alphabet. Worst case, you only need to try 25 different possibilities. A random substitution cipher has MANY more possibilities (26 factorial = 4 x 1026 possibilities). However, as we learned, with frequency analysis we can avoid having to try all of them blindly.

Was it difficult to crack a Random Substitution cipher? Did it take longer than you thought? shorter? Why?

- Computational tools aid humans in the implementation of encryption, decryption, and cracking algorithms. In other words, using a computer changes the speed and complexity of the types of encryption we can do, but it also increases our ability to break or circumvent encryption.

Any encryption cipher is an algorithm for transforming plaintext into ciphertext. What about the other way around? Can you write out an algorithm for cracking a Caesar cipher? What about a random substitution cipher?

- An algorithm for cracking a Caesar cipher is pretty easy - for each possible alphabetic shift, try it, see if the words come out as english.
- An algorithm for cracking random substitution is trickier and more nunanced. There might not be a single great answer but through thinking about it you realize how tricky it is to codify human intelligence and intuition for doing something like frequency analysis into a process that a machine can follow. It probably requires some human intervention which is an interesting point to make.

Review of Terminology -- you can use this opportunity to review new vocabulary introduced in the activity and respond to questions students may have encountered during the activity.

- Definitions of cryptography, encryption, decryption, cracking/breaking an encryption, cipher, etc.

Career Discussion

Introduce yourself and your career:

- What do you work, what do you do, and what do you love most about your job?
- What or who inspired you?
- How did you get interested in computer science?
- Did you have a mentor?
- Share a story about how tech affects everyone

Ask the students questions and leave time for Q&A.

- What jobs are they interested in, what are their favorite tech gadgets or apps, and how do they think they are built?
- Do the students have any questions for you?