(http://csmatters.org) 3 - 11

0b11 - 0b1011

Cryptography: Symmetric Encryption

Unit 3. Information and the Internet

Revision Date: Jul 22, 2019
Duration: 1 50-minute session

Lesson Summary

Summary

Students are introduced to the topic of cryptography and learn to perform two encryption techniques. The students will identify the role of the algorithm and key in the encryption process. Students will use abstraction to see the general process used in symmetric encryption. The students will consider the strength of ciphers and the importance of keeping the key a secret.

Outcomes

- Students will understand how encryption is used to keep data secure.
- Students will learn how encrypting and decrypting data is accomplished using an algorithm and a key.
- Students will understand why the key must be kept a secret.

Overview

1. Getting Started (5 min) - Journal
2. Introduction to Content (15 min)
    1. Lesson Motivation [5 min]
    2. Presenting the Key Concepts [10 min]
3. Guided Activities (25 min)
    1. Practice [15 min]
    2. Follow Up: Analyzing the Strength of Ciphers [5 min]
    3. Follow Up: Defining Symmetric Encryption and Seeing the Abstraction in Symmetric Encryption Systems [5 min]
4. Wrap Up (5 min) - Journal

Learning Objectives

CSP Objectives

- *EU AAP-2 - The way statements are sequenced and combined in a program determines the computed result. Programs incorporate iteration and selection constructs to represent repetition and make decisions to handle varied input values.*
    - LO AAP-2.A - Express an algorithm that uses sequencing without using a programming language.
    - LO AAP-2.L - Compare multiple algorithms to determine if they yield the same side effect or result.
    - LO AAP-2.M - For algorithms: a. Create algorithms. b. Combine and modify existing algorithms.

    - LO AAP-2.O - For algorithms involving elements of a list: a. Write iteration statements to traverse a list. b. Determine the result of an algorithm that includes list traversals.
- *EU IOC-2 - The use of computing innovations may involve risks to your personal safety and identity.*
    - LO IOC-2.B - Explain how computing resources can be protected and can be misused.

Math Common Core Practice:

- MP1: Make sense of problems and persevere in solving them.
- MP2: Reason abstractly and quantitatively.
- MP8: Look for and express regularity in repeated reasoning.

Common Core ELA:

- RST 12.4 - Determine the meaning of symbols, key terms, and other domain-specific words and phrases

NGSS Practices:

- 5. Using mathematics and computational thinking

Key Concepts

- Encryption is used to keep data secure as it is transmitted through the Internet.
- Symmetric encryption involves encrypting and decrypting data using an algorithm and a key.
- Encryption algorithms themselves are standardized (well known), so the key must be kept secret.

Essential Questions

- How is cybersecurity impacting the ever increasing number of Internet users?

Teacher Resources

Student computer usage for this lesson is: **optional**

In the Lesson Resources folder:

- "Cryptography Partner Practice": A worksheet for the students
- "Cipher Python Project": A worksheet with instructions for a simple Python project
- "Cipher Python Project Rubric": The rubric for the Cipher project

Optional: Lesson slides with the key questions, encryption demos, and diagrams (the teacher could simply read the questions and present demos and diagrams by writing on a board).

For examples, consider reviewing *The Code Book* by Simon Singh.

Lesson Plan

Getting Started (5 min)

Journal:

- Name one website you use that requires you to log in with a username and password.
- Why does the website require you to provide a username and password?

Introduction to Content (15 min)

Lesson Motivation [5 min]

- Present the scenario: “Alice would like to send a message to her friend Li in China, but she wants to keep it secret from everybody else.”
- Ask the students: “If Alice sends the message to Li by email over the Internet, will her message remain secret?”
- Student responses should bring up the architecture and trust model of the Internet to show that Alice’s message could be intercepted along the way, since it will pass through many devices before it ends up at Li’s computer.

Present the Key Concepts [10 min]

Tell the students, “This problem is not a new one. Throughout history, people, including government and military officials and personnel, business owners, and others, have wanted to send secret messages to someone but worried that the message could be intercepted along the way.”

There are two ways to try to keep the message secret: Steganography and Cryptography.

Explain the basic difference between the two.

- *Steganography* is when a message is "hiding in plain sight". Examples: Writing something in invisible ink that can be revealed with a special type of light.
- *Cryptography* is when a message is modified in a way that hides the meaning of the message. For example, the letters are replaced with symbols that someone else would not understand.

Present two different encryption techniques, showing one example of each.

- Transposition:
  - Definition: Rearranging the letters in the message.
  - Example: Rail fence (or "box cipher") http://www.braingle.com/brainteasers/codes/railfence.php (http://www.braingle.com/brainteasers/codes/railfence.php) or http://practicalcryptography.com/ciphers/rail-fence-cipher/ (http://practicalcryptography.com/ciphers/rail-fence-cipher/)
- Substitution:
  - Definition: Each letter is replaced by a different letter or symbol (although, technically a letter could be replaced by itself).
  - Example: Caesar Cipher (Shift Cipher) http://www.braingle.com/brainteasers/codes/caesar.php (http://www.braingle.com/brainteasers/codes/caesar.php)
    or http://practicalcryptography.com/ciphers/classical-era/caesar/ (http://practicalcryptography.com/ciphers/classical-era/caesar/)
  - Online Tool for Demonstration: Cipher Disk - http://inventwithpython.com/cipherwheel/ (http://inventwithpython.com/cipherwheel/)

An alternative to this lecture portion above is to have students independently study the same concepts using a reading, video, or online learning tool. Here are some suggested resources:

- Khan Academy: Have students watch the videos on "What is cryptography?" and "The Caesar Cipher" and complete the "Caesar Cipher Exploration". https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/intro-to-cryptography (https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/intro-to-cryptography)
- Practical Cryptography: Have students use the tools and descriptions to learn how to perform the rail fence encryption and decryption: http://crypto.interactive-maths.com/rail-fence-cipher.html (http://crypto.interactive-maths.com/rail-fence-cipher.html)

Summarize with this overview: "Each encryption scheme involves an algorithm and a key. The algorithm is the set of steps that you follow to accomplish the encryption. The key is the secret piece of information that is needed to know exactly how to apply the algorithm in this case. This allows you to securely send encoded information across the Internet and decode it when it arrives. Some codes are more secure than others."

Guided Activities (25 min)

Practice [15 min]

Have the students pair up and practice sending each other encrypted messages, then decrypting them to make sure they end up with the correct message.

A worksheet called "Cryptography Partner Practice" is provided in the Lesson Resources folder.

1. Each student gets to write two short messages that they will encrypt and send to their partner.
2. First message: Transposition: Use the rail fence algorithm. You must agree on the number of rails to use (this will be the “key”).
3. Second message: Substitution: Use the shift substitution cipher algorithm. You must agree on the amount to shift (this will be the “key”).
4. For each message, pass it to your partner and have them decrypt it using the agreed upon algorithm and key. Have them read back the decrypted message to make sure they decrypted it correctly.

Follow Up: Analyzing the Strength of Ciphers [5 min]

Ask the students: “How difficult would it be to crack a message that was encrypted using the Caesar (shift) cipher if you didn’t know the key? How would you do it?” (Easy, try each of the 25 possible shifts.)

Present: There are two ways to increase the strength of encryption:

Option #1: Increase the number of possible keys.

A general substitution (not limiting to just a shift) dramatically increases the number of keys. The number of keys in this case is the number of permutations (different orderings) of the 26 letters in the alphabet. This can be computed by multiplying the 26 options for the first letter in the cipheralphabet, by the 25 remaining options for the 2nd letter, 24 remaining options for the 3rd letter, etc. (26! or 26 factorial).

The answer: 4.032914e x 10^{26} keys (Google will calculate it for you).

This analysis makes it seem as though a substitution cipher would be unbreakable, but clever people have invented tricks (e.g., frequency analysis) that can be used so you don't have to try all of the different keys.

Option #2: Use a better algorithm.

For example, use a polyalphabetic cipher that combines multiple cipher alphabets.

(If time allows, you can have students explore other ciphers. For further study, see Khan Academy or *The Code Book* by Simon Singh.)

Follow Up: Defining Symmetric Encryption and Seeing the Abstraction in Symmetric Encryption Systems [5 min]

Present a diagram that shows high-level view of the encryption and decryption process (see *The Code Book*, p. 11).

1. Identify this as an example of abstraction. (You can ask the students to try to explain why.) Example: This is abstraction because it shows the general process of encryption and decryption using any key or algorithm. It omits the details of the specific algorithm and the type of key.
2. Tell the students, “The types of encryption you learned today are called “symmetric”. Why do you think they are called “symmetric”? (The same key is used to encrypt and decrypt. You use the algorithm to encrypt, and then reverse it to decrypt.)
3. What do you think it would mean for encryption to be asymmetric (non-symmetric)? (foreshadowing the next lesson)

Wrap Up (5 min)

Journal:

- What is the role of the algorithm in the encryption process? What is the role of the key?
- Which one of these, the algorithm or the key, is more important to keep secret? Why?

Optional Project for additional Python Practice

Use the "Cipher Python Project" worksheet in the Lesson Resources folder. Students are tasked to create a simple Caesar cipher program that uses ASCII values to shift messages by a certain letter. The rubric for this project is also in the Lesson Resources folder.

Homework (Optional): *Choose one of the following or let each student choose which one to complete.*

1. Computer Encryption: Use bitwise XOR to do substitution cipher (see *The Code Book,* p. 247)
2. Students read a historical account that involves encryption (Mary, Queen of Scots) http://www.nationalarchives.gov.uk/spies/ciphers/mary/ (http://www.nationalarchives.gov.uk/spies/ciphers/mary/) (After reading the introduction, click on the links below the picture for “Mary’s ciphers” and “The Babington Plot”)
3. Students read about cryptanalysis and learn about the frequency analysis technique. Try using it on an encryption puzzle..
    1. An example of breaking a substitution cipher: http://www-math.ucdenver.edu/~wcherowi/courses/m5410/exsubcip.html (http://www-math.ucdenver.edu/~wcherowi/courses/m5410/exsubcip.html)
    2. Try deciphering an encrypted message using the techniques you read about: http://cryptogram.org/solve_cipher.html#contents (http://cryptogram.org/solve_cipher.html#contents)

Evidence of Learning

Formative Assessment

The teacher will evaluate student responses to the journal entries, class discussion questions, and the students performance during the encryption practice.

(http://www.umbc.edu/) (http://www.umd.edu/) (http://www.nsf.gov/)

Authored by: CS Matters in Maryland
Website: csmatters.org (http://csmatters.org)
Email: csmattersinmaryland@gmail.com (mailto:csmattersinmaryland@gmail.com)