Course: Advanced Cybersecurity | Module: Advanced Cryptography

Lesson 1.1: Encryption Algorithms

https://codehs.com/course/7606/lesson/1.1

Description

In this lesson, students will learn about the basics of symmetric encryption. Students will explore the advantages and disadvantages of various ciphers and consider how using multiple ciphers impacts the decryption process. Students will also learn about the DES (Data Encryption Standard) and the AES (Advanced Encryption Standard).

Objective

Students will be able to:

- Explain the characteristics of symmetric algorithms and use them to encode and decode text. Specific ciphers include block, substitution, and transposition ciphers.
- Compare and contrast the strengths and weaknesses of symmetric ciphers.
- Compare and contrast the DES (Data Encryption Standard) and the AES (Advanced Encryption Standard).

Activities

1.1.1 Video: Encryption Algorithms
1.1.2 Quiz: Encryption Algorithms Quiz
1.1.3 Free Response: Enhanced Caesar Cipher
1.1.4 Free Response: Mixed Alphabet Cipher
1.1.5 Example: Pigpen Encoder
1.1.6 Free Response: Pigpen Cipher
1.1.7 Free Response: Rail Fence Cipher

Prior Knowledge

- This is an introductory lesson, so there is no prior knowledge necessary. However, students will be better equipped to discuss the advantages and disadvantages of ciphers if they are familiar with brute force attacks and letter frequency analysis.

Planning Notes

- Students will be introduced to many new vocabulary words over the course of this lesson and throughout the unit. To help students keep track of and use new words, write new vocabulary on the board or on an anchor chart that hangs in your class.
- Due to the number of activities in this lesson, it is a longer lesson that can be spread across multiple days. If this is not a possibility, focus on two-three ciphers instead of completing all four cipher explorations.
- There is a handout that accompanies this lesson. It can be used as an in-class activity or a homework assignment. Determine how and if this handout will be used.

Standards Addressed

Teaching and Learning Strategies

Lesson Opener:

- Have students brainstorm and write down answers to the discussion questions listed below. Students can work individually or in groups/pairs. Have them share their responses. [5 mins]
  - Note: The last question is designed to engage students in thinking about the process of decoding rather than actually getting to the correct answer. If students are familiar with the Caesar Cipher, you can tell them that is the cipher used to encrypt the message.

Activities:

- Watch the lesson video and complete the corresponding quiz. This quiz is a quick check for understanding [7-10 mins]
- Complete the *Enhanced Caesar Cipher* exercise. [10-15 mins]
  - Give students 5-7 minutes to decrypt the message and answer #2.
    - Note: Students can decrypt the message in multiple ways. If a student is stuck, encourage them to list the three encryption methods and then start with whichever seems easiest to them.
  - Debrief student approaches to decrypting the message as a class.

    - Give students 7-10 minutes to create their own cipher and answer #3 and #4.
    - Extension: have students switch their encrypted messages and hints with a partner!
- Complete the *Mixed Alphabet Cipher* exercise. [7-10 mins]
    - Give students 5 minutes to complete the activity and answer the questions.
    - Review student answers as a class.
- Complete the *Pigpen Encoder* and *Pigpen Cipher* activities. [15-24 mins]
    - Pigpen Encoder: [5-7 mins]
        - Give students 2-4 minutes to explore the pigpen cipher encoder.
        - Discussion question: Based on your exploration, how do you think the pigpen cipher works?
    - Pigpen Cipher:
        - #1: Give students 3-5 minutes to decrypt the message with a partner.
        - #2: Give students 5 minutes to encrypt their own message. Due to the symbolic nature of this cipher, students will need a separate sheet of paper to write out their encrypted message.
        - Give students 2 minutes to trade with a partner and decrypt each other's messages.
        - #3 and #4: Give students 5 minutes to answer the questions either independently or with a partner.
        - Debrief answers as a class.
- Complete the *Rail Fence Cipher* activity. [10-20 mins]
    - This is a slightly more complex cipher and students may need guidance in getting started. Use this website as a reference for how to decode a rail fence cipher.
    - #1: Give students 5-10 minutes to decrypt the message. Then share strategies as a class.
    - #2: Give students 5-10 minutes to create their own real fence cipher. Then, direct students to trade with a partner.
    - #3: Give students 2-3 minutes to answer the question independently or with a partner.
    - If time, discuss student responses as a class.

Lesson Closer:

- If students were unable to solve the ciphertext in the opening questions, return to it to see if they can decode the message!
- Have students reflect and discuss their responses to the end of class discussion questions. [5 mins]

Discussion Questions

Beginning of Class:

- Describe a time when you tried to keep a message secret or hidden. What did you do to keep it a secret? Were you successful?
    - *Responses will vary.*
- When might it be important to keep information protected and secure?
    - *It is important to keep personal information secure, such as bank account information or identification numbers.*
- How might you go about deciphering this secret message:
  Kocikpcvkqp ku oqtg korqtvcpv vjcp mpqyngfig. Hqt mpqyngfig ku nkokvgf, yjgtgcu kocikpcvkqp godtcegu vjg gpvktg yqtnf, uvkowncvkpi rtqitguu, ikxkpi dktvj vq gxqnwvkqp.
    - *"Imagination is more important than knowledge. For knowledge is limited, whereas imagination embraces the entire world, stimulating progress, giving birth to evolution." This is a quote by Albert Einstein. Students can decode the message by shifting all of the letters back 2 in the alphabet.*

End of Class:

- What is a similarity between a transposition cipher and a block cipher? What is a difference?
    - *Transposition and block ciphers are similar because they both involve manipulating the plaintext before it is encrypted. They are different because a transposition cipher scrambles words before applying the keys and a block cipher groups the plaintext into chunks.*
- How does mixing ciphers impact the level of difficulty of decrypting the ciphertext?
    - *Using a mix of ciphers makes it much harder to decrypt a ciphertext because if there is just one cipher, if you find the key to one letter, you can apply it to the entire message. Having multiple ciphers makes the decryption process longer and more complex.*
- What makes the AES more effective than the DES?
    - *The AES is significantly more effective than the DES because there are exponentially more keys, making it almost impossible to crack using brute force.*

Resources/Handouts

Confusion and Diffusion in AES Encryption (Student)

	Confusion and Diffusion in AES Encryption (Teacher)

Vocabulary

Term	Definition

Modification: Advanced	Modification: Special Education	Modification: English Language Learners
• Encourage students to use a mix of ciphers to encrypt their messages.	• Allow students to work with a partner when decoding ciphertext. • Decoding ciphertext can involve multiple steps. Break down the encryption process and check in with students at the end of each step before allowing them to move on. This will ensure they are on the right track. • Make the ciphers as visual as possible by having an alphabet available for the caesar cipher and a table prepared for the rail fence cipher.	• Provide a handout with key vocabulary and definitions: ciphertext, plaintext, substitution cipher, block cipher, transposition cipher. • Make the ciphers as visual as possible by having an alphabet available for the caesar cipher and a table prepared for the rail fence cipher.