CRYPTOGRAPHY

Lesson Description: This lesson introduces students to cryptography and a variety of symmetric encryption techniques.

There is a large amount of sensitive information being stored on computers and transmitted between computers today, including account passwords, trade secrets, and personal financial information. To keep this information hidden from third parties who may want access to it, cryptographic techniques must be used to encrypt it, making it difficult or impossible to actually recover the original data for anyone but the intended recipient. Because most modern cryptographic algorithms involve high-level mathematical concepts,this activity will investigate the general ideas behind cryptography and introduce the idea of analyzing the strength of different kinds of encryption.

Prerequisite Knowledge: Students should have an understanding of how the internet works, how information is stored digitally and the need for protecting information on an open network.

Length of Completion: One 90 minute block. This lesson could be split into 2 45 min classes. If lesson is taught over 2 days Introduction, Caesar Cipher & Random Substitution Cipher on Day 1 and Vigenere Cipher & Asymmetric Encryption on Day 2

Level of Instruction: Beginning HS Learners

Applicable Concepts:

GenCyber Cybersecurity Concepts

- Confidentiality - Reinforce to students why it is important tosecure their information or phone.
- Think Like an Adversary - Students explore ways they can protect information (encrypting data)

- Defense in Depth - Students ways in which there personal information can be protected on the internet

NYS COMPUTER SCIENCE AND DIGITAL FLUENCY STANDARD

9-12.CY.4: Evaluate applications of cryptographic methods.

Resources that are Needed: Specify

- Powerpoint Presentation
- caesar wheel
- Casear online decoder
- Cryptography Worksheet
- Mary Queen of Scot's Cipher
- Random Substitution Cipher Decoder
- Vigenère Cipher
- Vigenere Online Decoder
- Enigmator RSA Encryption Key Generator
- Enigmator RSA Encryption Tool

Accommodations Needed:

Students with visual impairments may need a screen magnifier or to manipulate browser and display settings on their device.

Accommodations for English Language Learners and Students with Disability include:

Vocabulary embedded in the lesson. Each vocabulary word is highlighted, provides a hyperlink to dictionary definition and is accompanied by visual when appropriate.

Accommodations in accordance with IEP and 504 plans will be in place.

LEARNING OUTCOMES

LESSON LEARNING OUTCOMES

- Explain the meaning of terms cryptography and cipher
- Recall some basic facts about the historic background of different ciphers
- Encrypt/Decrypt a message using Caesar Cipher
- Crack a message encrypted with a Caesar cipher
- Encrypt/Decrypt a message using Random Substitution Cipher
- Crack a message encrypted with random substitution using Frequency Analysis
- Encrypt/Decrypt a message using Vigenere Cipher
- Explain the weaknesses and security flaws of symmetric substitution ciphers
- Explain why encryption is an important need for everyday life on the internet
- Explain how public key encryption works

LESSON DETAILS

Interconnection: This would be taught as part of a series of lessons on cryptology and its role in cybersecurity . Students should have a basic understanding of how the internet works and how information is stored digitally

Assessment:
The assessment activities used in the this lessons include:
Formative - oral questions, pair-share and encryption exercises
Summative - Written reflection

Extension Activities:
Discuss and explore the ACSii table and how to replace the alphabet string to use the ASCii table and expand our encryption to include non-alpha characters.

Further exploration of both symmetric and asymmetric encryption methods.

Differentiated Learning Opportunities:

LESSON

Warm Up: (5 minutes) Students will play a round of HANGMAN allowing students to take turns guessing letters. Letter choices will be written in order to be used for later discussion about frequency analysis, etc..

Activity

Introduction (5 minutes)

Presentation on Cryptography & how it relates to Computer Science.

Caesar Cipher (15 minutes)

Brief presentation on Caesar Cipher as one of the earliest encryption methods

Distribute/have students make/use an online caesar cipher circle

ONLINE DECODERS:

https://cryptii.com/pipes/caesar-cipher

https://studio.code.org/s/hoc-encryption/lessons/1/levels/1

Printable Caesar Wheel
http://www.ece.uah.edu/~gaede/toyota_teacher_camp/STEM%20Activities%20for%20Students/printable-cipher-wheel_with%20alphabet.pdf

Students will complete exercises encrypting & decrypting messages using caesar wheel and then decrypt a message using an online tool with an unknown key thereby exposing the weakness of Caesar cipher.

Random Substitution Cipher (20 minutes)

Brief presentation on Random substitution cipher

Discussion on how what we know about solving hangman puzzles can help us decrypt random substitution cipher

Students will complete a encryption/decryption activity using a given key by hand and then be directed to:

Random Substitution Widget

Instruct students on how to use the widget

Have students work in pairs to decrypt a message provided using widget

Wrap Up Day 1 (Optional)

Think Pair Share: what is cryptography and how is it related to computer security.

Vigenere Cipher (15 minutes)

Brief presentation on Vigenere Cipher explaining that frequency analysis becomes more difficult since letters can map to different letters based on their position in the message

Students will complete a encryption/decryption activity based on a given key word using a vigenere grid

Vigenere Ciphers were thought to be unbreakable, however, using a variety of techniques they can be broken, given enough time.

Presentation on 10 and 256 bit encryption as a slight variation of a vigenere cipher

Introduce substitution cipher with 10 digit keys. Discuss 256 bit key encryption and the need to find increasing more difficult ways as processing speed increases exponentially

Asymmetric Encryption (15 minutes)

Presentation on what asymmetric encryption, High level overview of RSA encryption

Students will complete worksheet on RSA encryption where they will generate their own private and public key using the online tool and then exchange messages with a classmate thats encrypted using a public key and decrypted using a private key

Wrap Up (10 min)

Think-Pair-Share:

- What is symmetric vs asymmetric encryption
- How does asymmetric (public key) encryption keep data secure?