ENCRYPTION & CRYPTOGRAPHY (THURSDAY AM)

Lesson Description: This lesson is designed to provide insight into the frequency with which encryption is used and the 2 main types of encryption techniques (symmetric and asymmetric). After explaining these types of encryption the students will be asked to come up with circumstances in which one would be preferable to the other. Additionally, students will learn about historical encryption/cryptographic techniques, modern techniques, and future techniques.

Prerequisite Knowledge: A basic understanding of mathematical terms and familiarity with some basic cryptography terms.

Length of Completion: 50 minutes

Level of Instruction: This lesson is intended for middle and high school students of all levels and expertise.

Applicable First Principles &/or Concepts: Confidentiality, Integrity, Defense in Depth

GenCyber First Principles

Domain Separation	Abstraction
Process Isolation	Data Hiding
Resource Encapsulation	Layering
Modularity	Simplicity
Least Privilege	Minimization

CYBERSECURITY EDUCATION AND RESEARCH CENTER
@ The University of Wyoming
www.uwyo.edu/CEDAR
www.cowpokes.camp
www.uwcedar.io/community/cowpokes/wikis

GenCyber Cybersecurity Concepts

Defense in Depth	Availability
Confidentiality	Think Like an Adversary
Integrity	Keep it Simple

Resources that are Needed:

- Whiteboard
- Participants
- Access to a web browser (for the instructor(s))

Accommodations Needed: N/A

LEARNING OUTCOMES

- Students will be able to identify real world situations where encryption is useful or necessary
- Students will be able to describe the difference between symmetric and asymmetric key encryption
- Students will be able to list common types of symmetric and asymmetric encryption algorithms

LESSON DETAILS (Century Gothic, 14 pt. White, Italic)

Interconnection: This lesson is a capstone to the Microbot Wars activity, it discusses formal encryption methods as an extension of the ways students defended their robots.

Assessment: Formative assessment - Instructors ask students to explain what they have learned about encryption during this lesson. In addition,

students make a 2 minute video at the end of the day summarizing what they have learned during the day.

Extension Activities: Students will create a "Bob & Alice" style chart of how both asymmetric and symmetric key encryption is used to send and receive secure messages as a review of the lesson.

Differentiated Learning Opportunities: Advanced students will be asked to individually explore the math and logic behind asymmetric key encryption and explore the consequences of quantum computing on current encryption methods.

LESSON

Warm Up: Students will have the opportunity to come up with passwords they think may be often used, and are therefore broken, and then as a group check the results of whether or not those passwords have been cracked by checking the haveibeenpwned.com website.

Lesson:

Begin with instruction on the definition of cryptography and encryption, and list several names of common encryption algorithms, briefly explaining several.

Present an overview of historical cryptography and describe the following famous ciphers:

Caesar Cipher

Vigenere Cipher

Playfair Cipher (with advanced students)

Students will then be asked to create a key for their own Caesar Cipher. After coming up with a key, they will encode a short message with it, find a partner, swap messages, and attempt to decipher their partner's message and reproduce their partner's key.