Teacher Workshop: Capstone Project

Cyber-security First Principle: Information Hiding

Following is the beginning of a lesson in Cryptography. It is initially low-tech to allow students to brainstorm together and use their intellect and creativity.

A. As students enter class, put them in groups of 3 - 4 students. Teacher can be creative/methodical (or not) with method of group assignments.
B. Give each group the same encrypted message (encrypted with a Caesar Cipher) and with very little (if any) instruction, have groups try to decode the message. Instruct groups to work separately and discreetly.
C. After 3 - 5 minutes of collaboration, ask groups to pause and share some of their **problem-solving strategies** without divulging the message (if any group has already figured it out).
D. Now, hand each group the Cipher Wheel and tell them to try to decode the message with the assistance of this tool without any explicit directions on its use.
E. After 3-5 minutes, see if groups have figured out the message and have students share what they did.
F. At this point, we share the name “Caesar Cipher” and the history behind its use. We can also introduce the terms plaintext, ciphertext, and encryption key.
G. Next each group will decide on a short plaintext sentence to encrypt. Then pass their message to a different group and see if they can decrypt the message.

H. Show the class one or two Khan Academy videos to introduce cryptography. Then, the class could discuss the need/necessity for cryptography and more sophisticated cryptography.

I. As time permits, discuss/ask students where and when they encounter encryption in their daily life.

https://www.khanacademy.org/computing/computer-science/cryptography/crypt/v/intro-to-cryptography

https://www.khanacademy.org/computing/computer-science/cryptography/ciphers/a/ciphers-vs-codes

After this rudimentary lesson, the class could explore more sophisticated ciphers. Rather than telling the students the name of a particular cipher, assignment could be given based on a significant time in history or an organization or a country. A collaboration with the history/social studies teachers might be a possibility.

Examples: Find a cipher used during WWI or WWII.
Find a cipher used by the Freemasons.
Find a French cipher that was originally considered "the unbreakable cipher".
Find an encryption algorithm invented in the 1970's.

Introduce Technology: Raspberry Pi and Professor Adams' (graciously shared) programs could provide a nice follow-up to the initial lesson. Students could see how quickly a computer algorithm can encrypt and decrypt a message.

Other connection points in the high school math curriculum

Most of our math textbooks mention using matrices to code messages. This would be another great opportunity to interject some of the historical ciphers that utilized a matrix in their algorithm.

If one of the courses we teach covers combinations and permutations, we should make sure to link that concept to passwords and engage the students in a discussion of password security. The presentation Matt Wiseman gave us on "Safety II Best Practices" would be a great resource for this.