Introduction to Cryptography:
Secret Codes and Ciphers

STEELS Standards

- 3.5.6-8.H
- 3.5.6-8.I
- 3.5.6-8.U
- 3.5.6-8.BB
- 3.5.6-8.CC
- 3.5.6-8.EE

Objectives

- Students will understand the basic principles of cryptography
- Students will understand the importance of encrypting sensitive information
- Students will create and decipher messages using simple substitution ciphers

Materials

- Paper Caesar Cipher Wheel
  - Assemble as directed (recommended to use a brass fastener)
  - Make sure the wheels can spin around independently of each other
- Interactive Caesar Cipher Wheel

Basic Vocab

- **Cryptography**
  - The practice and study of techniques used for secure communication in the presence of third parties.
  - It involves encoding and decoding messages to keep them secure.
- **Plaintext**
  - The original message before encryption algorithms are applied.
- **Ciphertext**
  - The encrypted text.
- **Encryption**
  - Process of converting from plaintext to ciphertext using an encryption algorithm and a key, making it unreadable to outsiders.
- **Decryption**
  - The process of converting ciphertext back into plaintext using a decryption algorithm and a key.
- **Cybersecurity**
  - The practice of protecting computer systems, networks, and data from unauthorized access, cyberattacks, and security breaches.
  - Cryptography is one of many methods used to ensure cyber security.
- **Key**
  - Knowledge held by either the sender, recipient, or both that allows them to decipher the cipher text.
- **Performance Overhead**
  - The additional resources such as time and memory that are required to execute a task in a computer system or software application.

Introduction

Begin by asking students if they have heard of cryptography before. Discuss with them what they think it is, what it actually is, and why it is important.

A classroom example might be students secretly passing notes. Peers or teachers can intercept the note, it might be accidentally dropped or forgotten for anyone to pick up and read. An encrypted message will only read as gibberish if it falls into the wrong hands. Without the key possessed by the creator and recipient of the message, the cipher text holds no meaning.

Ceasar Cipher

Introduce the Caesar cipher as one of the oldest and simplest forms of encryption. Julius Caesar first used it to communicate with his generals on the battlefield so opposing generals couldn't decipher his plans.

To demo it, write the alphabet on the board. And right under it, write the alphabet again offset by a shift of 3 (Caesar used a shift of 3) such that the letters line up.

Example:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Below are some examples you can work through with the class.

If you would like to make your own: Plaintext to Ciphertext

Plaintext	Ciphertext
Hello	?????
Lehigh	??????

Plaintext	Ciphertext
Hello	?????
Lehigh	??????
I love CS	? ???? ??
Learning is fun	???????? ?? ???
Caesar Cipher	?????? ??????

Using the wheels, encourage the students to try going from plaintext to ciphertext and vice versa. Once they are familiar, you can try shifting by different amounts as well. Spin the wheel so the right letters of the inner and outer rings line up to match according to the shift and start deciphering!

But what happens if you don't know the key? Intuitively, we might begin to try all possible keys until we come upon the right one. Doing so, we employ a brute force approach. Allow students to attempt deciphering a few words without telling them the key! You may discuss the strategies stated below as well.

Below are some examples, you can create your own as well!

Plaintext	Ciphertext	Key
I love eating ice cream	P svcl lhapun pjl jylht	?
Chocolate milk tastes bad	Hmthtqfyj rnqp yfxyjx gfi	?
Soccer is the best sport	Hdrrtg xh iwt qthi hedgi	?
What's your favorite season	Sdwp'o ukqn bwrknepa oawokj	?
My computer is white	Vh lxvydcna rb fqrcn	?

Hint:

When deciphering WITHOUT a key, a good idea is to look for common letters and match them with the most common letters in English words. Statistically this would be E, T, A. This method of analyzing the frequency of letters to aid in deciphering is called frequency analysis.

Another good idea is to look at stand alone letters or short words. A single letter is likely to be A or I, while two letter words may be is, am, etc.

Class Activity

Option 1:

Divide the class up into small groups and have them work on solving a longer cipher. The first team to finish wins!

You can make your own! Or here are some samples below:

Plaintext	Ciphertext	Key
?	llsplcl pu fvbyzlsm huk hss aoha fvb hyl. Ruvd aoha aolyl pz zvtlaopun puzpkl fvb aoha pz nylhaly aohu huf vizahjsl	7
?	Dgoxdi iokbc pbyw xyg iye gsvv lo wybo nsckzzysxdon li dro drsxqc drkd iye nsnx'd ny drkx li dro yxoc iye nsn ny. Cy drbyg ypp dro lygvsxoc. Cksv kgki pbyw dro ckpo rkblyb. Mkdmr dro dbkno gsxnc sx iyeb cksvc. Ohzvybo. Nbokw. Nscmyfob	10

Option 2:

Have the class write their own ciphertext, randomly distribute them across the room and let them decipher each other's ciphers!

Summary

Bring the class back together and have them share their decrypted messages (as applicable based on classroom activity). Discuss the strategies they employed and the challenges they faced during the activity.

Discuss real-world applications of cryptography and its role in cybersecurity. Encourage students to reflect on the role of cryptography in their own lives and why it is important. Where have they noticed it? Why do we need it? Do they see any problems (ethically/technologically), limitations, or alternatives? What is the impact it has had on technology and future implications?

In summary, cryptography is just one of the many tools used in cybersecurity and adds an extra layer of privacy and confidentiality that helps prevent data theft. Actual industry standards involve encryption algorithms far more complex than the Caesar cipher, notably AES and RSA. However, the underlying critical thinking and logical skills needed to use and create them are the same!

Discussion

(Try to guide student discussion to touch on these)

- Cryptography is all around us! It works behind the scenes in many applications we encounter on a daily basis. Pretty much anything that involves communications and data is encrypted.
  - Secure communication protocols such as HTTPS
  - Data storage
  - Emails
  - VPNs
  - Banking transactions
- Despite its widespread use, it is far from infallible
  - Over time, new vulnerabilities are discovered and exploited. They become increasingly susceptible to brute force attacks, cryptographic attacks, and implementation flaws.
    - Must be updated and maintained regularly which adds a level of complexity
  - Introduces performance overhead
    - The extra drain on computational resources can affect system performance and user experience especially in resource constrained environments such as mobile devices
  - Human factors
    - Attackers may choose to exploit human flaws to bypass encryption
    - Emphasize the importance of safe internet interactions
      - Don't give out your personal information to anyone
      - Avoid clicking unknown links and downloads

- Human factors
  - Attackers may choose to exploit human flaws to bypass encryption
  - Emphasize the importance of safe internet interactions
    - Don't give out your personal information to anyone
    - Avoid clicking unknown links and downloads
    - Secure wi-fi networks or use VPNs