Cryptography

By Kristy Barr

Intro: Share the video from the movie National Treasure: Playfair Cipher.m4v
Discuss the movie clip and share what they know about codes and ciphers.

Discussion:
Cryptography is the practice of encoding information so that people can read and understand it. Why do we need that? In what instances would we need to keep information secret? Who needs cryptography now?

Explain the Caesar Cipher:
Let's travel back to around 100 BC when Julius Caesar was a Roman general and politician. He realized that if he was going to take down the Roman Republic, he would need to communicate with only the people he trusted with messages that could not be read by everyone. He used a method of encryption to convey secret messages to his army generals on the war front. This was known as Caesar Cipher, where each character of the original text would be substituted by another character based on a rule, perhaps +3 characters. That way A would become D, B would become E and so on. While this worked well in the early days of encryption, there was an obvious flaw. Well, obvious to us, but perhaps not to those living over 2000 years ago. Can anyone guess what that flaw was?

A cipher is an algorithm used for encryption or decryption. In a substitution cipher, each character of the plaintext (plaintext is the message which has to be encrypted) is substituted by another character to form the ciphertext (ciphertext is the encrypted message). The variant used by Caesar was a shift by 3 cipher. Each character was shifted by 3 places, so the character 'A' was replaced by 'D', 'B' was replaced by 'E', and so on. The characters would wrap around at the end, so 'X' would be replaced by 'A'. It is easy to see that such ciphers depend on the secrecy of the system and not on the encryption key. Once the system is known, these encrypted messages can easily be decrypted. In fact, substitution ciphers can be broken by using the frequency of letters in the language.

Next, lead the students in creating their own Caesar cipher wheel using the following material:
cipher wheel.pdf
To practice using the wheel lead students in encoding the teacher's name: Mrs. Barr.

In partners, have the students complete the following tasks:

1. Encode the name of our school: Casper Classical Academy
2. Encode your full name-first, middle and last.
3. Encode the name of your favorite song and trade with your partner so they can decode it.
4. Encode a message of your own on a sticky note and hand it to the teacher. She will then give you a different student's sticky note to encode.
5. With your partner, discuss how good is a cipher at protecting messages? Brainstorm one or two ways to improve it.

Lesson based on and materials are from Cryptography: The Caesar Cipher by CodeHS.org