Goals for the lesson:

- Learn the history of cryptography - from its purpose through early usage
- Learn the different keywords that deal with cryptography
- Learn several different ciphers, including historic and modern
- Encrypt and decrypt your own messages

Important Links:


Activity #1: Cryptography Definitions

What is purpose of encryption? Why use it? Do you use encryption? Examples: cell phone, gaming, banking, https

Definitions:

- Cryptography - secret or hidden writing
- Cryptology - study of secrets
- Encryption/Decryption - the act of turning normal text ("plain text") into garbled mess ("ciphertext")
- Cipher - the algorithm for conversion

Activity #2: History of Cryptography

Early years (before modern era)

- Concerned solely with keeping messages secret
- Between governments, military leaders, spies, etc
- Very earliest cryptography - none… because not many people could read, including couriers
- First ciphers went into three main categories: transposition, substitution, and physical

Transposition ciphers - kinda like word scrambles, but with a specific, regular way for scrambling

- Rail Fence
- Route
- Columnar

Substitution ciphers - replacing a letter with another letter

- Caesar
- ROT13
Physical ciphers - scytale

Your turn: Encode a message using one of these ciphers. See if your neighbor can decrypt it!

**Activity #3: Computers and Encryption**

Late 1400’s a problem was found with substitution and transposition ciphers
The problem was popularized in 1843 when Edgar Allan Poe wrote "The Gold Bug"
  - [http://etext.virginia.edu/toc/modeng/public/PoeGold.html](http://etext.virginia.edu/toc/modeng/public/PoeGold.html) - 131
  - Did you know Poe went to Virginia?

The problem Poe identified is called “frequency analysis.”

How do we counteract frequency analysis? The Vigenère Cipher.
[http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher](http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher)

Modern Cryptography
  - Started in WWII
  - The German Enigma Machine - multiple polyalphabetic cipher
  - Rotor based - lights lit up when key was pressed - rotors changed for different keys
  - Could still be cracked - thanks to Alan Turing

RSA
  - Cryptography and math!
  - The NSA and keeping algorithms secret - you can't export encryption schemes!
  - RSA - the reason it works are numbers are really hard to divide/find common factors

Modern uses of cryptography
  - Encryption/Decryption
  - Signing

**Activity #4: Encryption for fun!**

Garbled letters are too easy to spot - so are keys - use common items!

---

**Things to consider later:**
What things would you want encrypted? Are there things that need to be kept secret or private? Do you trust your computer to keep things secret?
Route Cipher
--------------------
"Form a square. Start at midnight and go to 3:00"

PIEHAHALBARNAYRIICYCKSEDN

Caesar Cipher
--------------------
PDUN LV JRLQJ WR GLVQHB

Viginere Cipher
--------------------
City in VA where Poe lived
Twowghruj itl mkrvfug