Cipher (si-fer)

noun

1. An algorithm for performing encryption or decryption – a series of well-defined steps that can be followed as a procedure.

Hail Caesar!

- Caesar Cipher
  - One of the earliest known examples of text encryption
  - Given a text message and an integer *key*
    - Substitute each letter in a message with the letter key positions down the alphabet
    - If you hit the end of the alphabet, wrap around
    - Do the reverse to *decrypt* the message
  - Decrypt this message, with the a key of 3:
    - L olnh fkhhvh

Encoding vs. Encryption

- Encoding (like we talked about last week)
  - Representing data (e.g. text) in another system (e.g. binary)
  - **Goal is to make it usable, simple, efficient, etc.**
- Encryption
  - Representing data (e.g. text) in another system (e.g. still text)
  - **Goal is to make it really, really hard to figure out!**

Secret-er

- Caesar is pretty limited, because it maps from the 26 characters to the same 26 characters
  - Better: map from characters to an infinite number of integers
    - (Kind of like the ASCII table)

- Activity: Roll your own encryption

Algorithms and keys

- A = 1, B = 2, etc
  - Encoding, not encryption
  - An algorithm, but no key (same every time)
- A = key, B = key + 1, etc
  - Encryption, only meant to be read by people who know **both** the algorithm **and** the key

- Lousy encryption, though.
- Partner discussion:
  - How would you decrypt a Caesar Cipher encrypted message if you didn't know the key?
  - How would you decrypt a message using that key + 1 cipher if you didn't know the key?

Cracking the code

- Here's my encryption algorithm:
  - Select two integer keys, `key1` and `key2`
  - For each character in the original message
    - Look up the ASCII value for that character
    - Multiply that value by `key1` and add `key2`
    - Add the resulting number to the encrypted message

- Activity: Dastardly criminals!

The Punchline

- Character-by-character encryption is all bad, actually
  - It gives the attacker a fixed set of numbers to figure out
  - Languages have well known *distributions* of letters
    - Imagine a program that just counts how many of each letter in all the English digital books in the world
  - Makes it pretty easy to figure out which number is which letter

- Secret key encryption is also generally bad
  - Have to communicate the key secretly, which is another potential point of attack
  - Asymmetric (public-key) encryption is much better