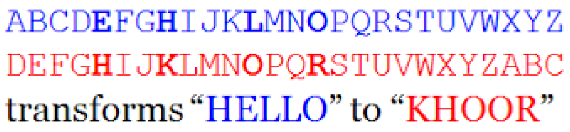
Model 1 Caesar Cipher

Julius Caesar famously used a "Cipher Wheel" to encrypt his messages to Cicero. This website provides an electronic version of the cipher wheel:

http://cryptoclub.org/tools/caesar_cipher.php

The Cipher Wheel uses a shift of the alphabet to determine which letters should be substituted. The outer ring is the original characters in **plaintext** (the first row of characters); the inner ring is the encrypted characters in **ciphertext** (the second row of characters).



ABCD**E**FG**H**IJK**L**MN**O**PQRSTUVWXYZ

DEFG**H**IJ**K**LMN**O**PQ**R**STUVWXYZABC

transforms "HELLO" to "KHOOR"

Questions (15 min) Start time: ________

1. In both the above model and in the electronic cypher wheel, blue (1st line) and red (2nd line) display the same set of characters. Which color/line represents the original characters, and which color/line represents the encrypted characters?

2. Rotate the electronic cypher wheel to match the blue and red characters above, by clicking on the white arrows. What is the key (the shift)?

3. Assume we do not know the key, but we know a Caesar encryption was used to encrypt this following ciphertext. Using trial and error, decrypt the phrase:

PDA XAOP PDEJCO EJ HEBA WNA BNAA

a) What is the original text?

b) What is the key (the shift)?

4. Consider how we might decrypt the phrase without the key.

a) How many different keys are there?

b) Describe the process that YOU used to decrypt a phrase when the key was unknown.

c) In contrast, describe the process a COMPUTER could use to decrypt a phrase when the key is unknown.

5. Think about the examples you brainstormed at the beginning of the activity. What is one advantage and one disadvantage of using Caesar Cipher encryption for online security?

a) one advantage:

b) one disadvantage: