# Activity 6: Encryption

## Context: Security and Privacy

We learned last week how easy it can be to examine network packets (e.g., using Wireshark) and how insecure the Internet can be. As a team, brainstorm for a few minutes what activities people do online that they would like to be kept secure and/or private. List several examples in the space below, and then have your presenter write the two most important on the whiteboard.

## Model 1 Random Substitution

You have likely decoded "secret messages" that simply used a different letter for each letter of the alphabet. These types of encryption schemes can be broken easily using frequency analysis. For example, we know that the letter E typically appears most frequently in English, followed by the letter T. Consider the following quotation, encrypted using a random substitution:

**PXL QLHP PXABCH AB OAGL KML GMLL**

### Questions (10 min) Start time: _____

1. Count the frequency of each letter in the above quotation.

   a) Which letter appears the most often?

   b) Which letter(s) appears the second most often?

   c) Which letter(s) appears the third most often?

2. Now consider commonly used English words.

   a) What are some commonly used three-letter words?

   b) What are some commonly used two-letter words?

c) Based on your answers to the above two questions, and using trial and error, decrypt the above quotation.

d) Discuss as a group the process you just used to decrypt the message, and describe it here.

## Model 2 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.math.uic.edu/shiftcipher/shiftcipher.htm

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).

ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
transforms "HELLO" to "KHOOR"

**Questions (15 min)** **Start time:** _____

3. 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?

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

5. 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)?

6. 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.

7. 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:

# Model 3 Vigenère Cipher

Vigenère Ciphers are a value-added Caesar Cipher that is very difficult to crack. Instead of using a single number, the key is a word. Each character in the key is encoded with its own Caesar Cipher. For example, here is how you encrypt the word `UMBRELLA` using the key `DOG` shown below.

1. Enter plaintext: `UMBRELLA`
2. Apply the key: `DOGDOGDO`
3. Get ciphertext: `XAHUSROO`

*From Beissinger & Pless, Cryptography*

Example 1 Let's choose the keyword DOG. We'll need three cipher wheels. The first wheel matches the letter **a** with **D**, the second matches **a** with **O** and the third matches **a** with **G**, as shown in Figure 1.

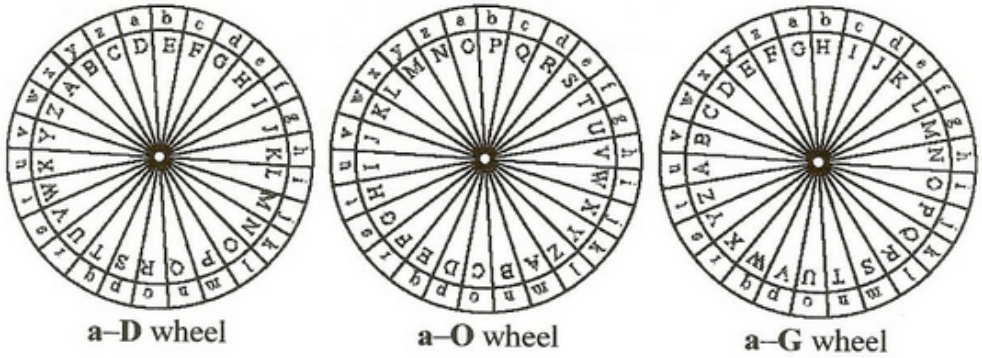


*Fig. 1 Wheels for a Vigenère Cipher with keyword DOG.*

## Questions (20 min) Start time: _____

8. Which letters in `UMBRELLA` use:

   a) the a-D wheel for encryption?

   b) the a-O wheel for encryption?

   c) the a-G wheel for encryption?

9. Why do you think the online cipher wheel uses lower-case letters for the outer wheel and upper-case letters for the inner wheel?

10. If you were encrypting the word `PEANUT` using the keyword `CAT`, list which letters would use which cipher wheel.

11. Encrypt `PEANUT` using the keyword `CAT`.

12. Consider the length of the keyword.

a) If we knew the keyword was two letters long, how many combinations of cipher wheels are there? Show your work.

b) If we knew the keyword was three letters long, how many combinations of cipher wheels are there? Show your work.

c) Ideally, if we needed to encrypt a 1000 character document, how long should the keyword be? Explain your answer.

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

a) one advantage:

b) one disadvantage:

## Conclusion

Modern encryption techniques (e.g., RSA and AES) are much more sophisticated than the shift ciphers we've looked at in this activity. But the idea is the same: you apply a "key" to some plaintext and transmit the resulting ciphertext.