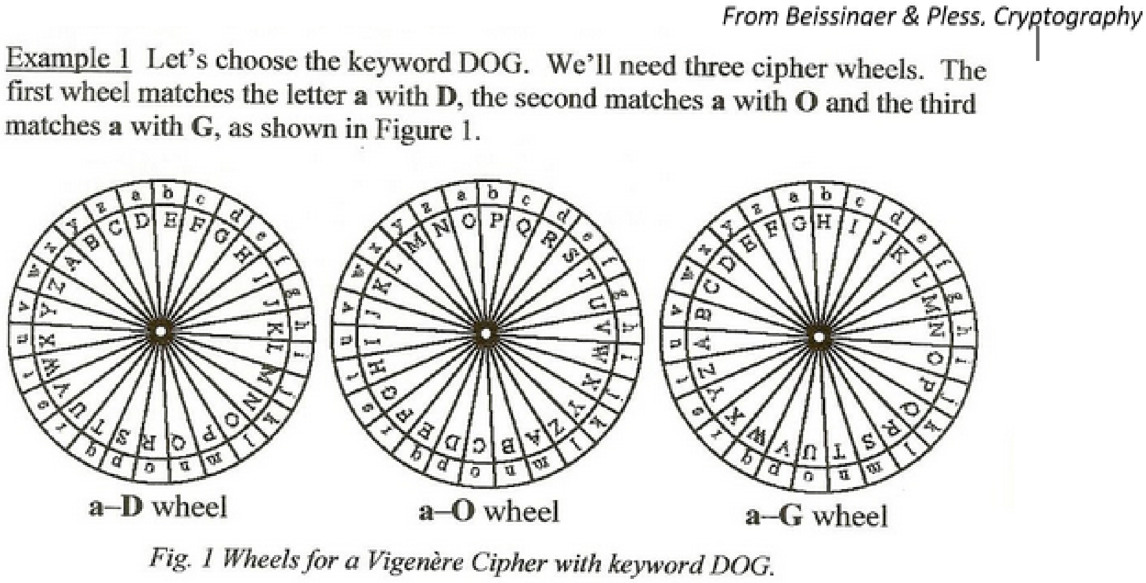
Model 1   Vigenère Cipher

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.

a–D wheel
a–O wheel
a–G wheel

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

Questions (15 min)

Start time: ________

1. Which letters in `UMBRELLA` use:

a) the a-D wheel for encryption? U, R, L

b) the a-O wheel for encryption? M, E, A

c) the a-G wheel for encryption? B, L

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

To make it easier to see the difference between plaintext and ciphertext.

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

C: P, N   A: E, U   T: A, T

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

`RETPUM` (the first key is 2, the second is 0, the third is 19)

5. 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.

26 * 26 = 676

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

26 * 26 * 26 = 17,576

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

The longer the keyword, the more secure it is. However, at some point it's not worth the extra computation. Plus there's only 26 unique letters. 12-15 is practically enough.

6. 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:

It's still relatively simple to compute, and more secure than Caesar ciphers.

b) one disadvantage:

The key is more complex, and it may be slower to perform the encryption.