

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 Beissinaer & 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.

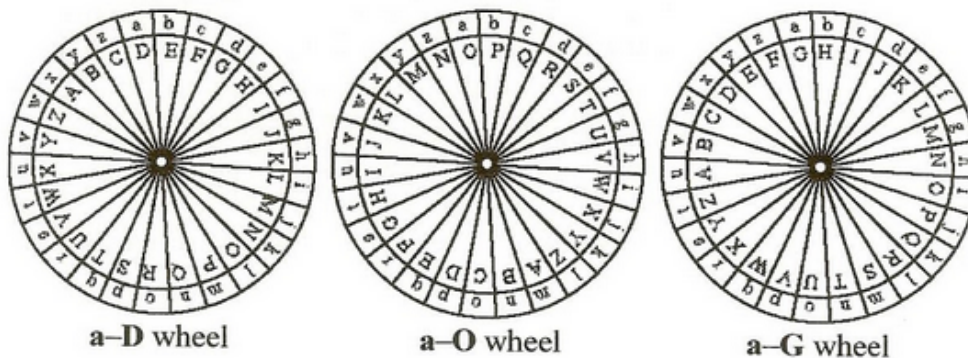


Fig. 1 Wheels for a Vigenère Cipher with keyword DOG.

Questions (15 min)

Start time: _____

1. 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?
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?

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

4. Encrypt PEANUT using the keyword CAT.

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.

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.

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:

b) one disadvantage: