|  |  |  |
| --- | --- | --- |
|  | **Activity Guide - Exploring the Vigenère Cipher** |  |

# 

# Read about the Vigenère Cipher

## Your Task

* Read the first 3 paragraphs of the section called “Secret Keys and One-Time Pads” and consider the diagram in [*Blown to Bits,* Chapter 5](http://www.bitsbook.com/wp-content/uploads/2008/12/chapter5.pdf), pp. 169-170.
  + **Secret Keys and One-Time Pads** (starts on p. 169)
  + Don’t continue past the diagram of the Vigenère cipher box on p. 170.
* *With a partner,* answer the questions about the reading below.

## Questions

* The “key” to a Caesar cipher was knowing how much to shift the alphabet. The “key” to a random substitution cipher is simply the table linking letters in the plaintext to their corresponding letter in the ciphertext. What is the “key” for a Vigenère (“Vee-zhun-aire”) cipher?

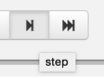
It is to find the length of the key and then brute force or trial and error all the different combinations of that length of key.

* As simply as possible, explain why/how simple frequency analysis doesn’t work on a Vigenère cipher. (There is a simple example in the reading.)

It doesn’t work because letters can be repeated for different letters.

# Try the Vigenère Cipher

## Getting Started -- Investigate the Widget

* You should have a partner for this exploration.
* Go to the interactive [Vigenère Cipher Widget](https://studio.code.org/s/cspunit2/stage/14/puzzle/3); this is an interactive version of the Vigenère cipher that animates the encryption as it’s happening. It works a *little* differently from the example in *Blown to Bits*, but it’s the same principle.
* **Encrypt a message**
  + Load the page with the widget.
  + Click (Step) several times, and trace what’s happening. Pay attention to:
    - How the ciphertext is being produced
    - What happens when you get to the last character of the key
  + After you’ve stepped through a few characters click (play) to watch the rest animate.
  + Hit (restart) and play the animation again with the text given. You can use the speed slider to speed it up or slow it down.
* **Decrypt a message**
  + Encrypt a message as above, then:
  + Highlight and copy the ciphertext.
  + Paste it into the plaintext area.
  + Don’t change the key.
  + Change the Encrypt/Decrypt toggle to Decrypt: 
  + Hit (play).
  + You should see the original text emerge.

### Misconception Alert

|  |
| --- |
| In decrypt mode, the widget flips whether it looks up the character of the key across the top or down the side. If a key was used to encrypt a message, then the same key can be used to decrypt it in decrypt mode. |

## 

## Investigate Different Messages and Keys

**Setup:** Make sure the widget is in “encrypt mode.” Enter whatever text you want in the plaintext area.

* Try encrypting with the key “A”. What happens? Why?

It is the exact same sentence as before because none of the original letters were going to change as A is equivalent to moving 0 places.

* Try the key “AAAA”. What happens? Why?

It is the exact same thing as the question above with the same explanation.

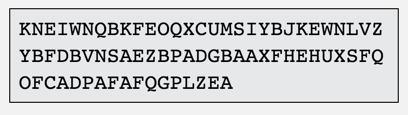
* In the “text message” area do this:
  + For the message enter a long string of the same character, for example: BBBBBBBBBBBBBB.
  + Then change the key to something you want (use your name, perhaps) and encrypt the message.

Compare and Contrast: What’s the difference between the Vigenère Cipher and the Caesar cipher in the way it encrypts long strings of repeated characters? Use the example of encrypting the word “Mississippi” to explain why Vigenère is a stronger form of encryption than Caesar.

The Vigenère cipher could change each amount of movements from the original letter determined by the key while the Caesar cipher just has a set amount of movements for all the letters.

## **Thought Questions**

You might want to play with the widget a little bit more in trying to answer these questions, but they can be answered based only on the properties of the Vigenère cipher.

* If I promised you that the message below was encrypted with the Vigenère cipher, would that make it easy to crack (yes or no)? Explain why. Your explanation should include a description of what you would need to know to decrypt this and how you might go about figuring that out.
  + ciphertext:  
    ****

Yes because I would be able to put it into a decrypter for Vigenère ciphers and it would be able to brute force the message.

* What if I told you that the message above was encrypted with the Vigenère cipher *and* the key I used was 10 characters long. Does that make it any easier to crack the message? Again, what would you need to figure out and how would you go about finding it?

Yes because then I could use the same program before and this time specify how long the key was allowing it to take less time to solve the message.