Discover: Try the Vigenère Cipher Widget!

Goals:
● Understand how the Vigenere Cipher Algorithm works
● Understand why simple frequency analysis doesn’t work against this cipher
● Figure out what makes for a good v. bad secret key

Instructions:
● You should have a partner for this exploration.
● Go to the interactive Vigenère Cipher Widget
● Click on buttons and try things out! Solve the mystery of what this tool is doing and how it’s doing it!

You should try each of the following - check off the DONE column once you’ve tried it

<table>
<thead>
<tr>
<th>Try This</th>
<th>Details</th>
<th>Done</th>
</tr>
</thead>
</table>
| Encrypt a few different messages using different secret keys | ● Enter a text message in the box and secret key  
● Step through the encoding of each character to see what’s happening  
● Try a different secret key | |
| Decrypt a message | ● Copy/paste the ciphertext of an encrypted message into the text message area.  
● Hit the button to “decrypt”  
● Now step through and see what happens | |
| Find a “bad” secret key | ● Hint: try “A” or “AAAAA” or “GGGG” or any single character, what about other patterns?  
● What makes a key bad? | |
| Find a “good” secret key | ● Use what you learned about bad keys and do the opposite  
● What are the characteristics of a good key? | |
| Try to decrypt without knowing the key (in other words: try to crack it!) | ● Have one partner look away, while the other copy/pastes the ciphertext of an encrypted message into the text area, and deletes the secret key from view  
● Have the partner who looked away come back and try to crack the message | |
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.

● Describe in your own words what the Vigenere Cipher Algorithm is doing.

● What makes for a good v. bad secret key using the Vigenere cipher? Give examples of a good key and a bad one and explain why.

● Compare and Contrast the difference between a substitution cipher (Caesar or Random) and Vigenere, using the message “I think I can I think I can I think I can” to explain why Vigenère is a stronger form of encryption than a substitution cipher.

● Will frequency analysis work to crack the Vigenere cipher? Why or why not? Keep your answer as simple as possible.

● If I promised you that the message at right was encrypted with the Vigenère cipher widget, 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.

● What if I told you that the message above was encrypted with the Vigenère cipher widget 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?