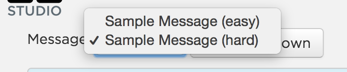
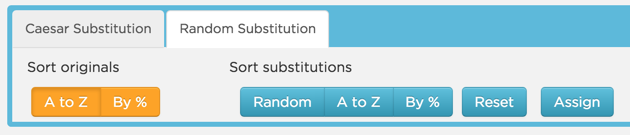
|  |  |  |
| --- | --- | --- |
|  | **Activity Guide - Cracking the Random Substitution Cipher** |  |

**Using the Frequency Analysis Tool**

## Getting Started

* Get together with a partner.
* Access the Frequency Analysis Tool through Code Studio [here](https://studio.code.org/s/cspunit2/stage/14/puzzle/2).
* In the upper left corner of the tool, select Sample Message (hard) from the dropdown.  
  *This loads a message that was encrypted with random substitutions.*

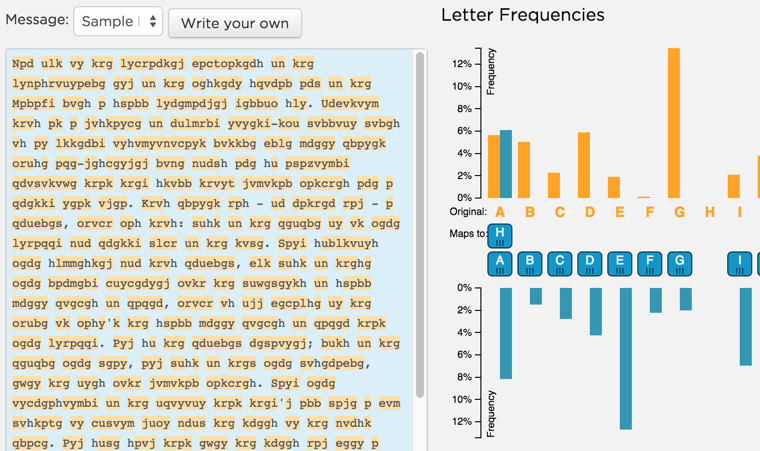
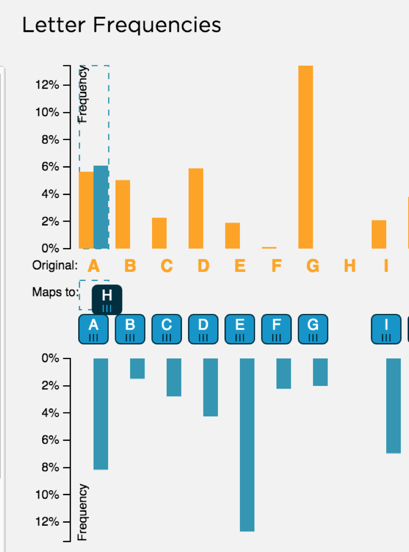


* Click the Random Substitutions tab below the frequency graphs.  
  *This makes available different options for viewing the frequencies of letters in the original input text (orange buttons) as well as different options to view the frequencies of letters in Standard English text (blue buttons)*

## Using the Tool

You will crack the message by guessing what each letter of the alphabet contained in the original ciphertext should be changed to. You can do so by dragging the blue letters of the alphabet directly underneath the orange letter you want changed in the original ciphertext. Letters that have been changed using your guesses will no longer be highlighted orange in the message window on the left.

For example, if you want all occurrences of the letter ‘A’ in the original ciphertext to change to ‘H’, then you would grab the blue letter ‘H’ and drag it underneath the orange letter ‘A’



## 

→

## 

## 

## Crack the Message!

Recall that the technique used to break a random substitution cipher is called frequency analysis. Letters appearing frequently in the ciphertext are likely to map to commonly occurring letters in standard English like “E”, “N”, “T”, etc. Above each orange letter you can see the frequency with which it appears in the ciphertext (orange graph). By comparing these frequencies to the frequencies of the letters in standard English (the blue graph), you can make reasonable guesses as to which letter is which.

Try using the two Sort...By % buttons in the Random Substitution tab to order the graphs by letter frequency. Does that give you any more clues or help you choose between two possible substitutions?



Check your progress and get ideas for more guesses by checking the progress of the output on the right. Do the letter combinations you see make sense? Are some words almost complete?

### Misconception Alert

|  |
| --- |
| You will likely have to change some of your guesses. Don’t worry if you struggle a bit at first. Once you’ve got 5 or 6 letters, you’ll see that the rest will come much more easily. Stick with it! |

## Review and Reflection

1. Once you believe you have successfully cracked the message, record the first ten words of the message in the space below.

Far out in the uncharted backwaters of the unfashionable end

1. Where is this quote - the cracked message - from?

Douglas Adams

1. Is the random substitution cipher a secure means of encrypting information? Is it more secure than the Caesar shift? Justify your response based upon your experience cracking both ciphers.

No, yes. Because the Caesar shift is easy to brute force simply, and with plugging in letters that occur often it is a lot easier to understand the text. It isn’t a super secure meaning you can solve it with easy substation.