Project 1 Report

For this project, I wrote two functions in C++ to encrypt and decrypt text using a Vigenere cipher and a third to use brute force to crack a Vigenere cipher given the cipher text, key length, and the length of the first word of the plain text. Using my brute force cracker, I decrypted these messages in the following time:

1. CAESARS WIFE MUST BE ABOVE SUSPICION (00:00:24)
2. FORTUNE WHICH HAS A GREAT DEAL OF POWER IN OTHER MATTERS BUT ESPECIALLY IN WAR CAN BRING ABOUT GREAT CHANGES IN A SITUATION THROUGH VERY SLIGHT FORCES (00:07:33)
3. EXPERIENCE IS THE TEACHER OF ALL THINGS (01:46:40)
4. IMAGINATION IS MORE IMPORTANT THAN KNOWLEDGE (08:34:55)
5. EDUCATION IS WHAT REMAINS AFTER ONE HAS FORGOTTEN WHAT ONE HAS LEARNED IN SCHOOL (20:31:44)

The main thing this project has taught me is that code breaking can be incredibly inefficient. My algorithm came up with every possible key given the length and attempted decryption with each one. This proved to be very inefficient and took an extraordinary amount of time. My algorithm was so slow, that I could not decrypt the last message in a reasonable amount of time.

One possible way to improve the speed of decrypting a Vigenere cipher is to perform a frequency analysis of the message given the length of the key. This would greatly speed up decryption, as you would not have to create and test each possible key. Using this algorithm would have made this project much easier for me and would have allowed me to decrypt the final message.