EECS 565 Project 2  
Report

The following is an output of my generated plaintext and matching keys.

Enter string of ciphertext: MSOKKJCOSXOEEKDTOSLGFWCMCHSUSGX  
Enter key length: 2  
Enter first word length: 6

Plaintext: CAESARS WIFE MUST BE ABOVE SUSPICION  
Key: JR  
Execution time 2150 miliseconds.

Enter string of ciphertext: OOPCULNWFRCFQAQJGPNARMEYUODYOUNRGWORQEPVARCEPBBSCEQYEARAJUYGWWYACYWBPRNEJBMDTEAEYCCFJNENSGWAQRTSJTGXNRQRMDGFEEPHSJRGFCFMACCB  
Enter key length: 3  
Enter first word length: 7

Plaintext: 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  
Key: IZX  
Execution time 82716 miliseconds.

Enter string of ciphertext: MTZHZEOQKASVBDOWMWMKMNYIIHVWPEXJA  
Enter key length: 4  
Enter first word length: 10

Plaintext: EXPERIENCE IS THE TEACHER OF ALL THINGS  
Key: HVJC  
Execution time 2088564 miliseconds.

Enter string of ciphertext: HUETNMIXVTMQWZTQMMZUNZXNSSBLNSJVSJQDLKR  
Enter key length: 5  
Enter first word length: 11

Plaintext: IMAGINATION IS MORE IMPORTANT THAN KNOWLEDGE  
Key: ZIENF  
Execution time 52748862.25272015 miliseconds.

Password cracking is extremely time and resource consuming. The time needed to crack a password is compounded by the number of possible keys (key length) and the size of the dictionary. Since each key must be checked with each dictionary entry, each increase in key length drastically increases the time needed to crack the password. Thus, small tweaks in code and computational methods can have an enormous impact on the efficiency of any password cracking program. In addition to efficient algorithms, the language chosen to compute the passwords can also have a massive impact. The data structure used to store the data being searched (in this case the dictionary entries) also has a huge impact on the speed of the program. If I were to re-design my program, I would reconsider the data structures and searching methods I implemented. Multithreading or cloud computing environments may speed up password cracking techniques as well.