EECS 565
Project 1 Report
Tim Elvart
KUID: 2760606

For this project, I decided to use c++ since it is my most familiar language. After implementing the vigenere encrypt and de-crypt functions, I started thinking about how to make the cipher breaker efficient. I wanted a way to efficiently search through large numbers of strings to see if a certain one was present. Initially I thought a hash table would be the best implementation, but after doing some research on the web I discovered something called a prefix tree or trie. It just needed to traverse the trie M levels deep where M is the length of the string being searched for. It didn't search through a ton of unnecessary data. After that was figuring out how to generate all of the possible keys, recursion became my best friend while spending a ton of time figuring out how to do it iterative-ly. After having all of the tools, I implemented the actual password cracker. The algorithm for generating keys is recursive, but from analysing it is a safe assumption it has complexity O(26^n) where n is the number of characters in the strings being generated. After testing all 6 cases provided, the times, keys, and plain texts discovered are as follows:

1) "MSOKKJCOSXOEEKDTOSLGFWCMCHSUSGX"
key length = 2, first work length = 6

key used: KS, plain text: CAESARSWIFEMUSTBEABOVESUSPICION
time to find: 0.000078 seconds, time to test all 676 keys: 0.000206 seconds

2)
OOPCULNWFRCFQAQJGPNARMEYUODYOUNRGWORQEPVARCEPBBSCEQYEARAJUYGW
WYACYWBPRNEJBMDTEAEYCCFJNENSGWAQRTSJTGXNRQRMDGFEEPHSJRGFCFMACCB
key length = 3, first word length = 7

key used: JAY, plain text:
FORTUNEWHICHHASAGREATDEALOFPOWERINOTHERMATTERSBUTESPECIALLYINWAR
CANBRINGABOUTGREATCHANGESINASITUATIONTHROUGHVERYSLIGHTFORCES

time to find: 0.000784 seconds, time to test all 17,576 keys: 0.002251 seconds

3) MTZHZEOQKASVBDOWMWMKMNYIIHVWPEXJA
key length = 4, first word length = 10
key used: IWKD, plain text: EXPERIENCEISTHETEACHEROFALLTHINGS
time to find: 0.024564 seconds, time to test all 456,976 keys: 0.066654 seconds

4) HUETNMIXVTMQWZTQMMZUNZXNSSBLNSJVSJQDLKR
key length = 5, first word length = 11
key used: ZIENF, plain text: IMAGINATIONISMOREIMPORTANTTHANKNOWLEDGE
time to find: 1.52082 seconds, time to test all 11,881,376 keys: 1.56465 seconds

5)
LDWMEKPOPSWNOAVBIDHIPCEWAETYRVOAUPSINOVDIEDHCDSELHCCPVHRPOHZUSE
RSFS

key length = 6, first word length = 9

key used: HACKER, plain text: EDUCATIONISWHATREMAINSAFTERONEHASFORGOTTENWHATONEHASLEARNEDINSCHOOL

time to find: 9.68941 seconds, time to test all 308,915,776 keys: 36.01 seconds

6) VVVLZWWPBWHZDKBTXLDCGOTGTGRWAQWZSDHEMXLBELUMO
key length = 7, first word length = 13

key used: NICHOLS, plain text: INTELLECTUALSSOLVEPROBLEMSGENIUSESPREVENTTHEM

time to find: 607.4 seconds or 10.12 minutes
time to test all 8,031,810,176 keys: 1194.63 seconds or 19.9 minutes

The times were taken from my desktop machine at home. It runs on an Intel i7-6700k at 4GHz.