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 decrypt functions, I started thinking about how to make the cipher breaker efficient. I wanted a way to efficently 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 unneccary 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 iteratively. After having all of the tools, I implemented the actual password cracker. After testing all 6 cases provided, the times, keys, and plaintexts discovered are as follows:

1)  **"**MSOKKJCOSXOEEKDTOSLGFWCMCHSUSGX**"**

key length = 2, first work length = 6

key used: KS, plain text: CAESARSWIFEMUSTBEABOVESUSPICION

time to decrypt: 9.8 \* 10^(-5) seconds, time to test all 676 keys: 0.000248 seconds

2) OOPCULNWFRCFQAQJGPNARMEYUODYOUNRGWORQEPVARCEPBBSCEQYEARAJUYGWWYACYWBPRNEJBMDTEAEYCCFJNENSGWAQRTSJTGXNRQRMDGFEEPHSJRGFCFMACCB

key length = 3, first word length = 7

key used: JAY, plain text: FORTUNEWHICHHASAGREATDEALOFPOWERINOTHERMATTERSBUTESPECIALLYINWARCANBRINGABOUTGREATCHANGESINASITUATIONTHROUGHVERYSLIGHTFORCES

time to decrypt: 0.001204 seconds, time to test all 17576 keys: 0.003253 seconds

3) MTZHZEOQKASVBDOWMWMKMNYIIHVWPEXJA

key length = 4, first word length = 10

key used: IWKD, plain text: EXPERIENCEISTHETEACHEROFALLTHINGS

time to decrypt: 0.024418 seconds, time to test all 456976 keys: 0.071764 seconds

4) HUETNMIXVTMQWZTQMMZUNZXNSSBLNSJVSJQDLKR

key length = 5, first word length = 11

key used: ZIENF, plain text: IMAGINATIONISMOREIMPORTANTTHANKNOWLEDGE

time to decrypt: 1.86535 seconds, time to test all 11881376 keys: 1.91568

5) LDWMEKPOPSWNOAVBIDHIPCEWAETYRVOAUPSINOVDIEDHCDSELHCCPVHRPOHZUSERSFS

key length = 6, first word length = 9

key used: HACKER, plain text: EDUCATIONISWHATREMAINSAFTERONEHASFORGOTTENWHATONEHASLEARNEDINSCHOOL

time to decrypt: 11.9298 seconds, time to test all 308915776 keys: 44.4411

6) VVVLZWWPBWHZDKBTXLDCGOTGTGRWAQWZSDHEMXLBELUMO

key length = 7, first word length = 13