Vigenere Cipher Password Cracking

Author: Manvir Kaur
Date: 09/20/2023

Introduction

The Vigenere Cipher is a classical method of encrypting text using a keyword. This report documents the results of my attempt to crack Vigenere Cipher-encrypted messages using a brute-force approach. The goal was to decrypt the messages and assess the performance and efficiency of the password cracking process.

Methodology

Brute-Force Decryption

I implemented a brute-force decryption method for the Vigenere Cipher. The process involved generating all possible key candidates of a specified length and decrypting the ciphertext with each candidate. My program checked if the first word of the decrypted text, based on a specified length, matched any word in a provided dictionary. If a match was found, the program considered it a potential decryption result.

Dictionary

I used a dictionary of English words loaded from the provided file (dict.txt) to verify if the first word of the decrypted text was a valid word. This dictionary contained thousands of words and was crucial in filtering out potential plaintext candidates.

Results

Key Length 2, First Word Length 6

- Plaintext: caesarswifemustbeabovesuspicion
- Quote: "Caesar's wife must be above suspicion."
- Key: KS
- Time Elapsed: 0.0205 seconds

Key Length 3, First Word Length 7

- Plaintext: fortunewhichhasagreatdealofpowerinothermattersbutespeciallyinwarcanbringaboutgreatchangesinasituationthroughveryslightforces
- Quote: "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: KEY
- Time Elapsed: 1.7922 seconds

Key Length 4, First Word Length 10

- Plaintext: experienceistheteacherofallthings
- Quote: "Experience is the teacher of all things."
- Key: IWKD
- Time Elapsed: 11.8378 seconds

Key Length 5, First Word Length 11

- Plaintext: imaginationismoreimportantthanknowledge
- Quote: “Imagination is more important than knowledge.”
- Key: KELCE
- Time Elapsed: 388.8650 seconds

Key Length 6, First Word Length 9

This message could not be successfully decrypted within a reasonable time frame.
(I considered anything over several minutes to be unreasonable, especially hours.)

Key Length 7, First Word Length 13

This message could not be successfully decrypted within a reasonable time frame

Discussion

The results show that my brute-force decryption method was successful in recovering the plaintexts for the first three messages with relatively short key lengths. However, as the key length increased, the time required for decryption grew exponentially. This is highlighted with the time difference between key lengths 4 and 5.

The efficiency of the password cracking process was highly dependent on the key length. For shorter keys, such as key length 2, 3, and 4, the process was efficient, taking only fractions of a second to a few seconds, increasingly. However, for longer keys like key length 5, the process became significantly slower, taking almost 7 minutes for the last message.

The exponential growth in decryption time as key length increased highlights the limitations of brute-force approaches for longer keys. To improve efficiency, other techniques, such as frequency analysis or precomputed substrings, could be explored. Additionally, parallelization could be employed to make better use of multiple CPU cores. I tried to implement some of these techniques in my program but I was unsuccessful and kept getting errors.

Conclusion

In conclusion, the brute-force decryption of Vigenere Cipher-encrypted messages can be effective for shorter keys but becomes increasingly inefficient for longer keys. The choice of decryption method and key length should consider the trade-off between security and computational resources. Further optimization and parallelization can significantly enhance the efficiency of the process for longer keys.