Assignment 1- Part 4 - Report

Eugenio Ribón

Code description

The code accepts a ciphertext input and attempts to break the Vigenère Cipher by iterating through every possible key combination of lengths 1 to 4. For each candidate key, it decrypts the text and calculates a score based on standard English letter frequencies and a "bonus" for common English words (like "THE" or "IS"). The program then outputs the top-ranking candidates, allowing the user to identify the correct plaintext from the list. To run it, execute make to generate the v_cipher executable, then run ./v_cipher and input your ciphertext.

Attack method

I used a Brute Force Dictionary Attack combined with Heuristic Scoring.

- **Assumptions:** The key length is a maximum of 4 letters , the language is English , and punctuation is not encrypted.
- **Method:** The code generates all keys from 'a' to 'zzzz'. It decrypts the message with each key and assigns a fitness score. Because the text is short (~40 chars), simple letter frequency analysis was insufficient. I enhanced the scoring algorithm to reward decryptions containing common English words, ensuring the correct human-readable sentence appeared at the top of the results.

Alternative method

If the key length were unknown, I would use the **Kasiski Examination**.

- **Modifications:** I would modify the code to scan the ciphertext for repeated sequences of 3 or more characters. The distance between these repeats is likely a multiple of the key length. By calculating the factors of these distances, I can determine the probable key length. Once the length (L) is known, I would split the ciphertext into L columns and solve each one as a simple shift cipher using frequency analysis.

Results

Key: wzaa

Plaintext: TIME IS AN ILLUSION. LUNCHTIME DOUBLY SO