Nathan Fleet
CS 32301 Human Interface Computing
February 24, 2023

Homework 4

How can an attacker decrypt based on the cipher and algorithm used?

The cipher I used in my program was the caesar cipher. This cipher can be easily decrypted by an attacker with knowledge of this cipher. This is because the caesar cipher uses a key to shift each letter in the plaintext a certain number of spaces. There are only 26 possible keys, so a brute force attack using all 26 keys would reveal the unencrypted message. Also, this cipher is vulnerable to frequency analysis because an attacker can compare the frequency of characters in the encrypted text to the expected frequency of characters in the English language, and use this to determine which characters are ‘e’, ‘t’, ‘a’, etc.