Nick Wu

Intro to OS

Lab 13

1. A Caesar Cipher can be cracked in a couple of ways. One method is to brute force and try all 25 possible shifts. For each shift, we can check whether one gives us a meaningful output. Another method is to analyze the frequency of letters in the encrypted message. Based on the frequency, we can match it to the frequently used characters in the English language to correctly guess the shift. For example, the letter *e* is used more often than letters like *x*, so we can try to deduce the shift based on the encrypted letter’s frequency.

One method we can use to increase the security of a Caesar Cipher is to vary the shift from character to character. At each characters’ position, we can use a different key to shift the characters position rather than only one key. This would take more effort to crack. We could also provide a secret passkey to determine the shift. The shift for each letter in the text could be determined by the corresponding letter in the passkey.