Assignment 1
SIL765

Gaurav Chauhan
2018CS50406

Question1.

In the first question, first I changed the value of the input cipher corresponding to the given substitution in the question. Now, after changing all the characters into the small case alphabets, I printed out the frequency of each alphabet.

In cipher1.txt

In this I first mapped the most occurring value with either A or I as these are the most occurring characters in a common sentence as studied by me through this webpage(https://www.dummies.com/games/cryptograms/cryptography-101-basic-solving-techniques-for-substitution-ciphers/).

Now I started looking for two-three words and started guessing them by already made assumptions of the single element. Through these iterations of hit and trial and also logic of frequency analysis I decoded the question.

SUBSTITUTIONS:

['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
to
['b', 'r', 'p', 'q', 'i', 'v', 'g', 'd', 'e', 'm', 'n', 'w', 'o', 'j', 's', 'y', 'k', 'a', 'l', 'c', 'u', 'x', 'h', 'f', 't', 'z']

DECODED MESSAGE:

“a disadvantage of the general monoalphabetic cipher is that both sender and receiver must commit the permuted cipher sequence to memory. a common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. for example, using the keyword cipher, write out the keyword followed by unused letters in normal order and match this against the plaintext letters. make reasonable assumptions about how to treat redundant letters and excess letters in the memory words and how to treat spaces and punctuation. indicate what your assumptions are. note, the message is from the sherlock holmes novel, the sign of four.”

In cipher2.txt

In this I saw that an element ‘zw’ was occurring a lot in the start of many sentences. Hence I narrowed down the options to he, we and so for the input file. I started solving the cipher with he in the same fashion as above for cipher1.txt and ended up getting the right output.

SUBSTITUTIONS:

['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
to
['a', 'g', 'c', 'n', 'w', 'q', 'x', 'z', 'v', 'p', 'f', 'd', 'u', 'o', 'm', 'h', 'y', 't', 'r', 'k', 'l', 'i', 'e', 's', 'b', 'j']

DECODED MESSAGE:

“defeated and leaving his dinner untouched, he went to bed. that night he did not sleep well, having feverish dreams, having no rest. he was unsure whether he was asleep or dreaming. conscious, unconscious, all was a blur. he remembered crying, wishing, hoping, begging, even laughing. he floated through the universe, seeing stars, planets, seeing earth, all but himself. when he looked down, trying to see his body, there was nothing. it was just that he was there, but he could not feel anything for just his presence.”

RUNNING COMMANDS:

python3 substitutioncrack.py <input_file_name>