Fall 2019 CIS 3362 Week One Assignment Solutions

1) It's easy enough to write a program which takes in the input and outputs the input shifted by the 26 possible shifts. When we run the attached program (hmk1-12.c), we see that adding 12 to the cipher text produces the following plain text (I've added spaces and punctuation):

This is just the first question. Don't be thrown off by the appearance of a q.

The corresponding encryption key was \( k = 14 \), since the decryption key, \( +12 \equiv -14 \) (mod 26).

2) Run the same program on the ciphertext given. When we add 19 to the ciphertext, we get the following plaintext:

It was the best of times. It was the worst of times.

The corresponding encryption key was \( k = 7 \), since the decryption key, \( +19 \equiv -7 \) (mod 26).

2) Now, run a program that tries all 312 possible affine cipher keys on the ciphertext to see which produces meaningful output. The attached program (hmk1-34.c) does this. After combing through the results, we find that applying \( a = 19, b = 10 \), the correct decryption keys, produces the following output

For this question you had to look through three hundred and twelve possible decipherments. Hope you didn't get cross-eyed.

We can do the following math to find the corresponding encryption keys:

\[
\begin{align*}
f(x) &= (19x + 10) \mod 26 \\
x &= (19f^{-1}(x) + 10) \mod 26 \\
(x - 10) &= 19f^{-1}(x) \mod 26 \\
11(x - 10) &= 11(19f^{-1}(x)) \mod 26 \\
f^{-1}(x) &= (11x - 110) \mod 26 \\
f^{-1}(x) &= (11x + 20) \mod 26
\end{align*}
\]

Thus, the encryption keys were \( a = 11, b = 20 \).

4) Edit the code used for #3 to remove both loops, set \( b = 19 \) and \( i = 6 \) (since ALIST[6] = 15) and then run the program which produces the following cipher text:

ktxnrpivaljsuqjwbmvebgcjzhvoyhfd