Jerry Liu
404474229
Math 116

Question 1:
Decrypted Message: EVEISEAVESDROPPINGONUS

Since we know the key is “virgo”, we can reset the index of the key “virgo” after five iterations when we are looping through the ciphertext.

I wrote a function with a signature: decrypt(ciphertext, key);
The function can detect the key length.

Question 2:
Selected Most Frequent Letters: NEGO
Vigenere Key is: JACK
Decrypted Message:
WEUSEWORDSLIKEHONORCODELOYALTYWEUSETHESEWORDSASTHEBACKBONEOFALI
FESPENTDEFENDINGSOMETHINGYOUUSETHEMASAPUNCHLINEIHAVENEITHERTHETIME
NORTHEINCLINATIONTOEXPLAINMYSELFTOAMANWHORISESANDSLEEPSUNDERTHEBL
ANKETOFTHEVERYFREEDOMTHATIPROVIDEANDTHENQUESTIONSTHEMANNERINWHIC
HIPROVIDEIT

This question, we know the key length, but we have to do frequency analysis. I wrote a function with the signature: decryptVigenere(ciphertext, keyLength);
For this problem, I just pass 4 as the keyLength.

This function will do frequency analysis using a tool, “Counter”, from “collections” library. It will start from the most frequently appeared letter, say ‘ch’ and assume it is ‘E’. Then, it will shift back by $('ch' - 'E')$, and then store the dot product of the frequency analysis from the shift and the original English letter frequency, say $\overrightarrow{A_0}$. After 13 iterations, this function will stop and give back the letter ‘ch’ that has the largest dot product. I set it to 13 iterations since the frequency of letter ‘E’ is unlikely to be after those of 13 other letters.

Question 3:
Selected Most Frequent Letters: AEXWSR
Vigenere Key is: WATSON
Decrypted Message:
HOLMESHADBEENSEATEDFORSOMEHOURSINSILENCEWITHHISLONGTHINBACKCURVED
OVERACHEMICALVESSELINWHICHHEWASBREWINGAPARTICULARLYMALODOROUSPRO
DUCTHISHEADWASSUNKUPONHISBREASTANDHELOOKEDFROMMYPOINTOFVIEWLIKEA
STRANGELANKBIRDWITHDULLGREYPLUMAGEANDABLACKTOPKNOTSOWATSONSAIDH
ESUDDENLYYOUDONOTPROPOSETOINVESTINSOUTHAFRICANSECURITIES

This question involves one more step than question 2. I simply shift the ciphertext and see when it has the most coincidences, and then I will pass the result to the function I wrote in question 2. (Function signature: findKeyLength(ciphertext);)