Homework 2

Question 1:

Decoded Cipher:

**eachofthesemessageswillleadyoutoaplaceoncampuswhereyouwillfindashortnotefrommeifyouretrievethatnotebringittomeandyouwillgettendollarsforthisfirstquestionyouwillfindthecorrespondingnoteveryclosetomyofficethereisastackofbooksfrommydadanddrduttonthatarebeinggivenawayfindtheonecalledinternationalsimulationtechnologyconferenceopenituptopagetwohundredtofindthenoteremembertobringittometoclaimyourmoney**

For this problem, I went through the string that was provided and obtained the frequency that each letter appeared. From this, I copied a frequency chart online and used that to get a bassline for what I should replace. I went through a map of all the characters and their percentages and sorted them based on percentage, then using the English letter frequency, I replaced them correspondingly (e.g. if k is the most prevalent letter in the encoded text, it will be replaced with e). From this point on, I used paper and pencil to keep track of the letters, and started “swapping” letters in the English frequency list to eventually come up with more characters I knew were correct.

**a**, **q**, and **u** are never used. In the final substitution, these 3 can either map to **j**, **x**, and **z**, as these do not appear in the final decoded message.

For the rest of the letters, this is the changes:

**b c d e f g h i j k l m n o p r s t v w x y z**

**g m s u q n k i h e b a f d c t v p l y r o w**

Question 2:

Decoded Cipher:

**thistimeiwillleadyoutoadifferentspotstillinheciamlazysoidontwanttohidethenotetoofarawayfrommyofficebutthistimeiwillatleastputitonadifferentfloorgotothethirdfloorspecificallyfindroomthreetwotwonearitisafireexteinguisheropenthedoorwhereitisandliftitupunderneathityouwillfindthenotefrommebringittomeandgettendollars**

For this question, all my work done is in the attached C++ file. First, I determine the most likely group, from 2 to , where is some arbitrary limit I impose in my code. Then, for each in the range of , I split the string into groups. I run the Index of Coincidence for each of these groups. For each of these, I add to a total deviation from the standard English value of . If the average deviation of these groups is smaller than the best average deviation I have found so far, I keep it and set that as the best average deviation. I repeat this until groups to determine the most likely number of groups, therefore the keyword length. This is a semi-naive approach as it may not actually be the correct number of groups, but it gives me a good starting point to check the next most likely and so forth.

For the next section I found each of the shifts, assuming is the length of the keyword used. First, I calculate the frequencies that the letters appear in each group. Then, for each of these groups I shift through all possible letters , with each shift calculating a variance the true English frequency. If it is the best possible (minimized) variance from standard English, I remember this and use it to compare to future values. Eventually this gets me the most likely shift that each group has.

The keyword used in the Vigenère Cipher is:

**d r o w y e k**

Question 3:

Decoded Cipher (My answer):

**thisisthelastquestionandthelastchancetoclaimsomemoneybutiwillmakeyouworkforityouhavetoclimballthewaytothefourthfloorwheretheadministrativeofficeisforcomputersciencerightacrossfromthatofficethereisabulletinboardadvertisingmanyclubsactivitiesandjobslookbehindthehackucfpostertogetthelastnotefrommetoclaimthelastprizeforhomeworktwogoodluck**

This question I do the same process as Question 2, the big difference is my algorithm doesn’t get the string perfectly decrypted.

My algorithm gave this result:

**thisisthetastquestiwnandthelaatchancetoklaimsomemwneybutiwitlmakeyouwwrkforityochavetocliuballthewagtothefourbhfloorwhezetheadminqstrativeonficeisforkomputerscqencerighticrossfrombhatofficebhereisabutletinboarladvertisivgmanyclubaactivitieaandjobslowkbehindthmhackucfpoatertogettpelastnotenrommetocliimthelastxrizeforhoueworktwogwodluck**

After going through the few errors left, my result is what is right under Decoded Cipher.

The keyword used in the Vigenère Cipher is:

**w a t e r m e l o n**