Name: Grishma Vemireddy

Student ID: 2045611

Problem 1: Substitution Cipher

Given the task of decrypting the given ciphertext, I know that I am needed to compute the frequency of the letters in the ciphertext and compare them with the frequencies given in the problem description. So first, I created a function called 'ComputeFrequency()' that take in the ciphertext and output the frequency of the letters in the ciphertext. Frequency table found below,

A: 0.009 B: 0.001 C: 0.001 D: 0.037 E: 0.004 F: 0.035 G: 0.025 H: 0.075 I: 0.013	J: 0.069 K: 0.029 L: 0.013 M: 0.032 N: 0.056 O: 0.047 P: 0.001 Q: 0.106 R: 0.014	S: 0.002 T: 0.016 U: 0.016 V: 0.058 W: 0.052 X: 0.047 Y: 0.015 Z: 0.011

Using the computed frequencies, I match them, manually, with the frequency of letters given in the problem text. Except for the letters with the same frequency, I found the substitute characters for the rest. Also given that the spacing and punctuation are the same, I assume that Dr. On is FO. VW, and based on this assumption I match D to F, R to O, O to V and N to W (format: plaintext to ciphertext). And using the English language to make sense of the words, I match the letters in the ciphertext with same frequency to the letters I believe are their substitute. I also convert the upper case text to lower case, and using a python dictionary to store the ciphertext letter and their substitutes I found. I replaced the ciphertext with their substitutes and ended up with this decrypted text,

"urgent message: i believe that dr. on is a member of a secret crime organization called p.h.a.n.t.o.m., whose goal is total world domination. their plan is to acquire a superweapon and to hold the world ransom. i am afraid that we do not have much time before they succeed. i recently intercepted an encrypted message (attachment cipher2.txt) that was sent by dr. on to one of his conspirators, the infamous mr. blowfield. i managed to discover that the message was encrypted using the jackal cipher (see source code), but i was not able to discover the secret key, and the cipher seems to be unbreakable. i am afraid that decrypting this message is the only way to stop dr. on's organization. please send reinforcements immediately! i tried to act cautiously, but i have a feeling that dr. on's henchmen are onto me. i don't know how long i have before they discover my real identity and my secret hiding pla"

Problem 2: Brute Force

Given that the number of possible keys for Jackal cipher is between 0 and 127, I write a nested for-loop that iterates through the possible key combinations calling the JACKAL_Decrypt() function until an

English text is found using the isEnglishText() function. I loop through until a valid combination is found. Finally, I print the decrypted plain text, stated below,

“Mr. Blowfield, my associate will deliver the payment to you next Friday at noon. The location of the exchange is 20.893369, -156.438838. I expect you to deliver the plans for the super-weapon in exchange. Do not dare to fail me.

You should encrypt the plans with one-time-pad to prevent anyone from stealing them. Use the following 11 byte values as the key: {2, 3, 4, 5, 7, 11, 13, 17, 19, 23, 29, 31}. If the plaintext is longer, then just repeat the key as many times as necessary.”

Problem 3: “One-Time” Pad

Bases on the decrypted text from Problem 2, we are given the key values. I am using the XOR operator to loop through the key values to each byte in the cipher_text. The decrypted output is shown below,

““Dr. On, I will deliver the plans personally to your secret underwater base at 30.395871, -46.471452 on September 15 at midnight.”

After discovering the location of Dr. On’s underwater base, you are finally ready to defeat him. Soon, P.H.A.N.T.O.M. will fall. You hop into your supersonic submarine and set course for Dr. On’s secret liar. It is time for him to learn the name Vond. James Vond.”