Name:Kokil Dhakal
Collaborator:None
Extension:None
Source: https://inventwithpython.com/cracking/chapter5.html
https://stackoverflow.com/questions/613183/how-do-i-sort-a-dictionary-by-value

Estra credit work at the last of this file.....

lab 3 working process:
I will be explaining by method used in this process.

Design:
1.Caesar Cipher:
Caesar cipher encrypting decrypting process is easier one. As encryption take place by replacing each letter of the message with another letter with a fixed key number. So we will be provided message to be encrypted and key with which each letter of that message will be encrypted. For this we need a dictionary key as letter and number as value up to 26. now we go through each letter of the message and calculate its position in letter dictionary. then add position value by key number and find out the final position number in letter dictionary. and finally find the letter representing that final position number. and this letter represent encrypted letter. similarly, we go over each letter of the message and convert to encrypted message.
for decoding cipher, we do same process but in reverse direction i.e. we subtract key value instead addition.
Finally, we also have to handle wrap around.

2. breaking Caesar Cipher:
for this we use Brute Force technique and frequency analysis of the letters from cipher text. we have provided the frequency occurrence of letter in English language. based on that we will find key to decrypt the cipher text. first, we make a dictionary in which counter for each letter is 0. we well go over each letter of the cipher text and add number of occurrences of each letter and finally sorted descending order. We will check higher number of occurrences of letter and mapped with higher number with higher number of occurrence letter in English which is e followed by t etc. so combination of brute force which gives 26 possibilities and frequency analysis we can crack Caesar cipher.

3. Vigenère cipher: this is similar to encrypting and decrypting Caesar cipher except the key. instead of using single letter or a number this process uses a group of letters as key that will be repeated over. on this we have to handle two wrap around one on message and another on key. number of words in key will be repeated over until all letters in message is encrypted. decrypting Vigenère cipher is similar to encrypting but in reverse direction.

4.OTP:

for this we approach differently instead of using dictionary we use binary number. Each letter in message are converted to binary numeric and we will randomly produce the keys same length of that message binary number. after that we use bitwise XOR operation between binary key and binary message numeric. Product from this operation will be encrypted cipher text. similarly, we will decrypt the cipher text numeric by doing XOR with same key and then convert to message string.

Extra Credit:
2.one time pad is a way to make Vigenère cipher unbreakable. it uses one time randomly generated key which length is as same as the length of message. these three criteria make OTP impossible to hack. Number of possible keys will be 26 raised powers of the total number of letters in the message which is a very big number. Also, there is possibility of same ciphertext from multiple messages. so it is hard for cryptanalyst to figure out which is original message even if he/she able to crack key by using powerful computers. (Reference from https://inventwithpython.com/cracking/chapter21.html)

3.In Vigenère cipher we use same keys multiple times over the length of a message, reusing same key over a message is same as reusing key multiple times in Vigenère cipher, which is hackable. That is why reusing same key in OTP is vulnerable to be hacked.