# CE708: Computer Security

# Lab Assignment 1 Report

# Name: Yaowei Lyu

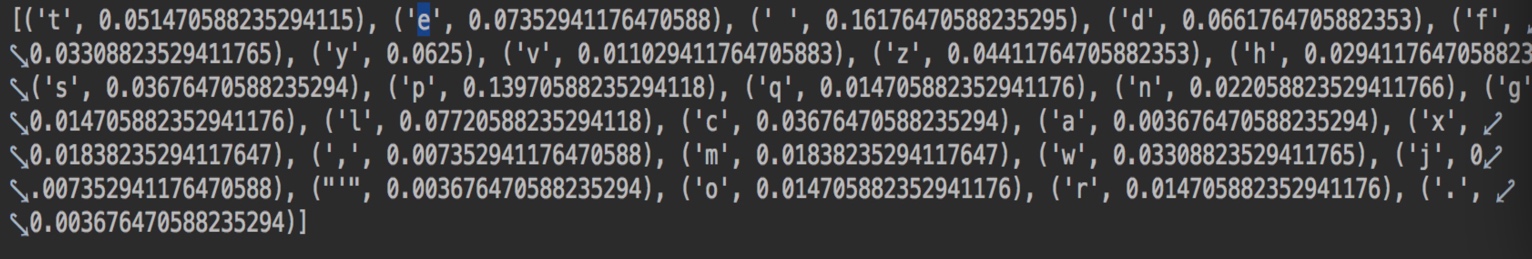
# Submit date:15th November 2018

**Introduction**

This case is going to test the Caesar Cipher and Playfair Cipher function and make a try to decrypt and encrypt some simple data. To implement the function, Python is used to generate a program and latest version is 3.7, in this assignment I chose version3.6 to finish the work and it works really efficient. I also use PyCharm as my operator which is an easy-operate software.

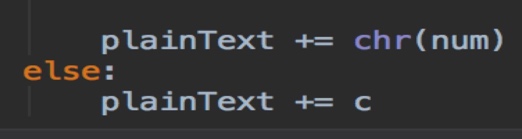
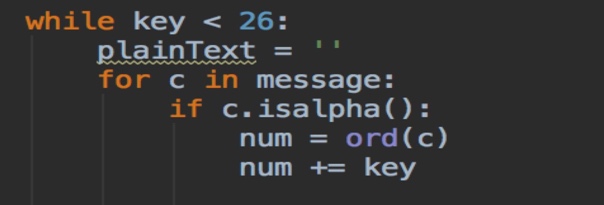
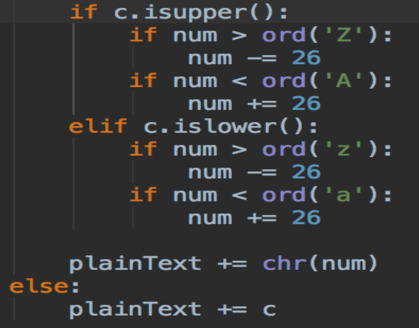
**Main body**

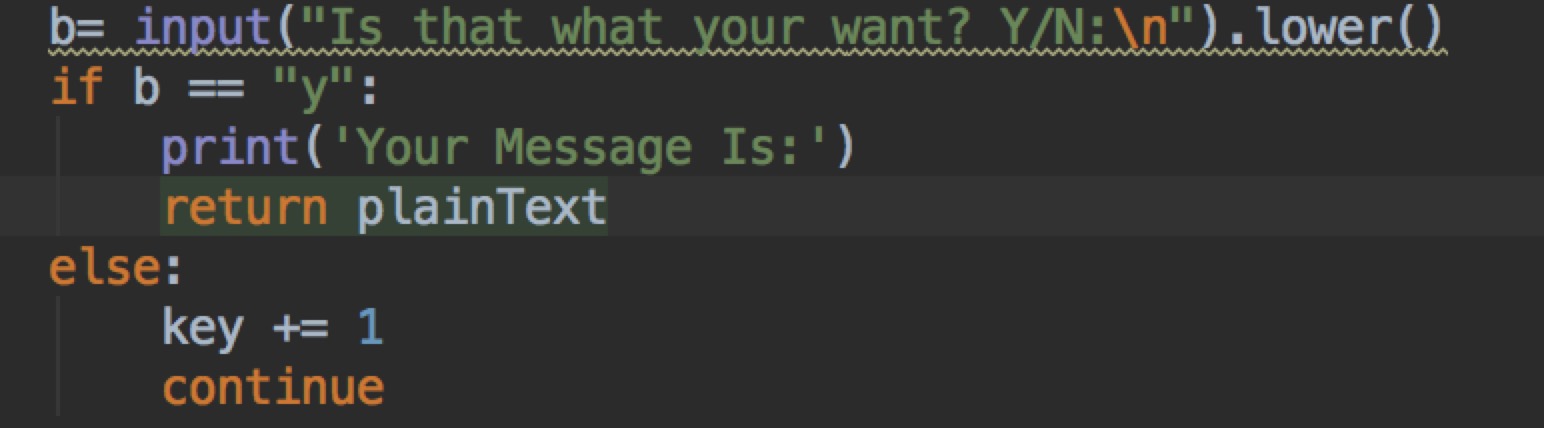
**Part I: Decrypt the ciphertext**

From the demand we know that there is no key for decrypt so we need to consider using Caesar Cipher and Simple Substitution Cipher. So we using Simple Substitution Cipher first, first of all we need to compute frequency of all letter and find out that the four most frequent letter, in ciphertext, we got P, E, D and Y, which we expect E, T, A and O.

By using Simple Substitution Cipher, we need to exchange letters by using ‘replace’ function in NLTK re module and analyze the possible combine. After finish this contempt, I found it is too difficult to do this unless we use dictionary function in python. So this ciphertext should decrypt by using Caesar Cipher.

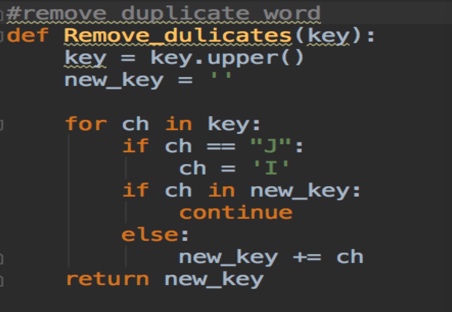
If we using Caesar Cipher, we need to know the shifting key to decrypt, but we can not find from the question, so we use brute force attack to obtain the plaintext. We have to try each key and show the plaintext to users and let them make decision whether the text is understandable. If we decrypt the possible message, then break the loop.

First of all, the max key size is 25, because Caesar Cipher’s key is a circle and word itself can not be the key otherwise it will decrypt useless information. WeChat271cafd70d467850f0e719aa80cd7052.png.I obtain the key by a loop that put every shifting key to the ciphertext and get the decrypt message . In this loop, if key is less than 26, I set up a String called “plaintext” and its initial value is none. Then try each letter in message (as known as ciphertext), the type of key is integer so I transfer ciphertext to ASCII value by using ‘ord’ function. After transfer we add key and plaintext, if we want to get the plaintext, we need to use ‘chr’ function to transfer ASCII to String. If the ciphertext’s ASCII value is larger than ‘Z’’s ASCII value, we need to miner 26. In a similarly way if ciphertext’s ASCII value is lower than “A’’s ASCII value, we need to add 26. 

When I first doing this job, I encounter a problem that there is no condition reason to exit the loop unless we use dictionary function. But we do not want use that because it makes thing much more difficult. So I design another loop to let user decide when to leave the loop. 

If user input Y or y or yes, computer will think it is the right message so return the plaintext.

**Part II: Playfair Cipher Encrypt and Decrypt**

****From the question we know that we need to decrypt and encrypt message by using playfair cipher. We learned from lecture that if we want to use playfair cipher we need to create a cipher table. To create a cipher table, we need key and alphabet. First we need to remove duplicate word of the key

In this function, we need to input a key

and then transfer the key’s letter into

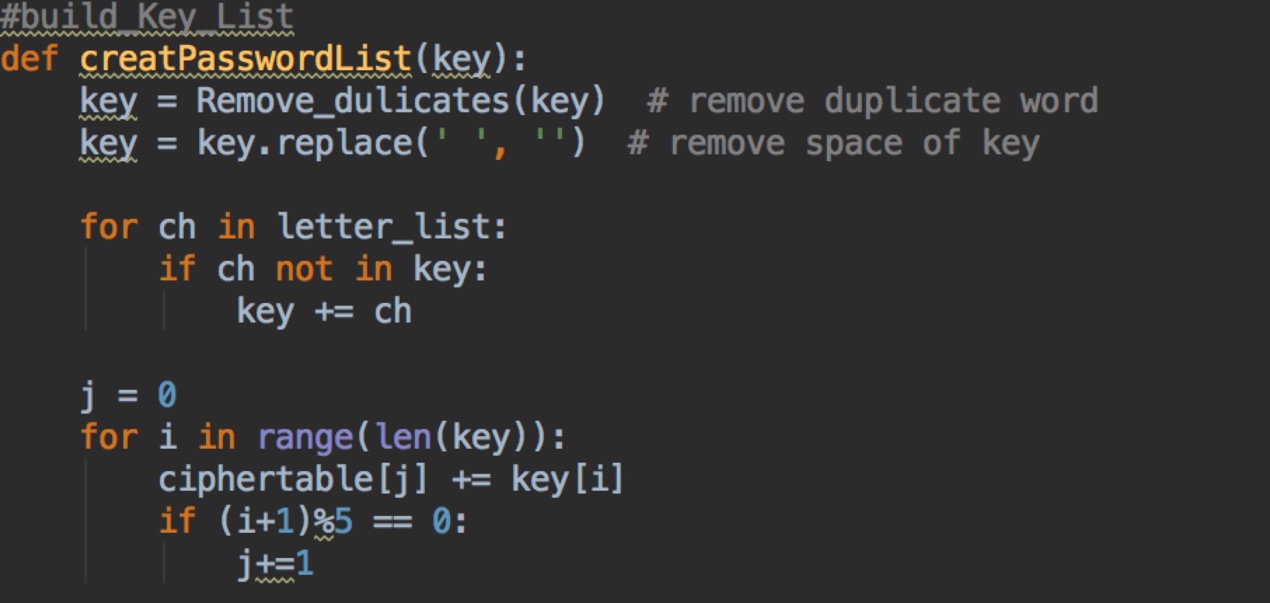
capital letter because the letter in alphabet

is capital letter. After doing this, I use a

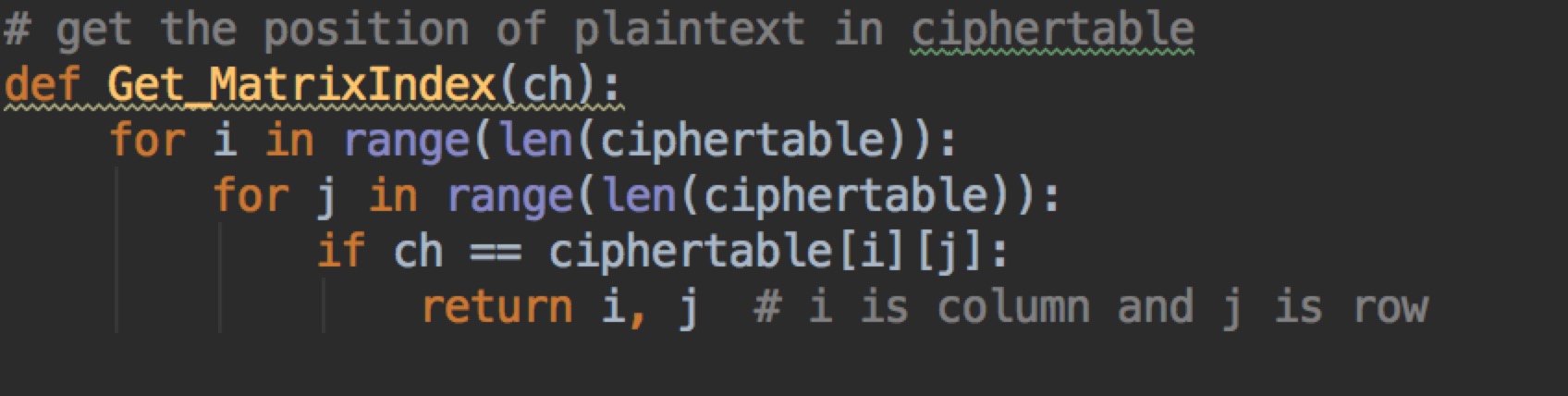
loop to generate a cipher key without

duplicate letter.

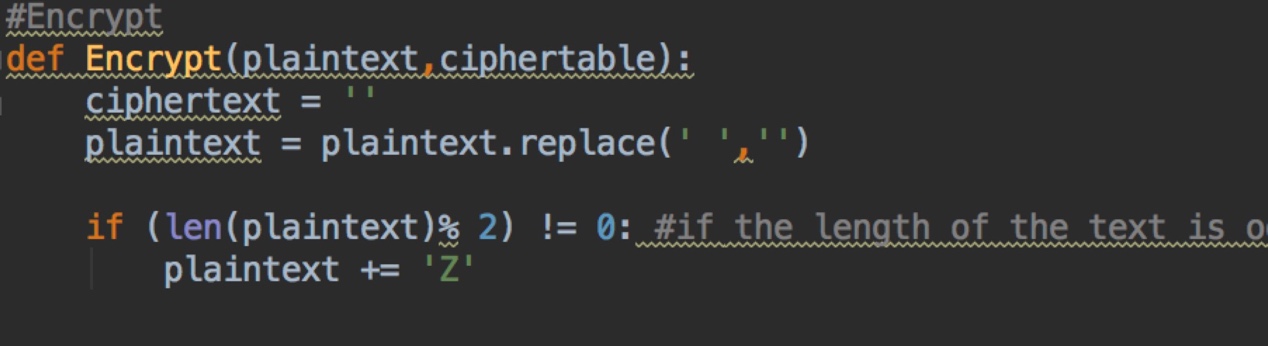
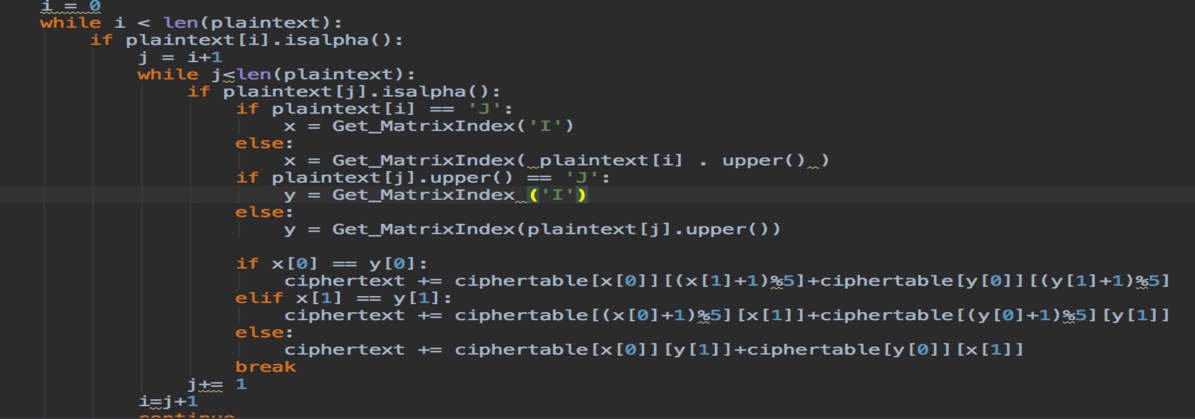




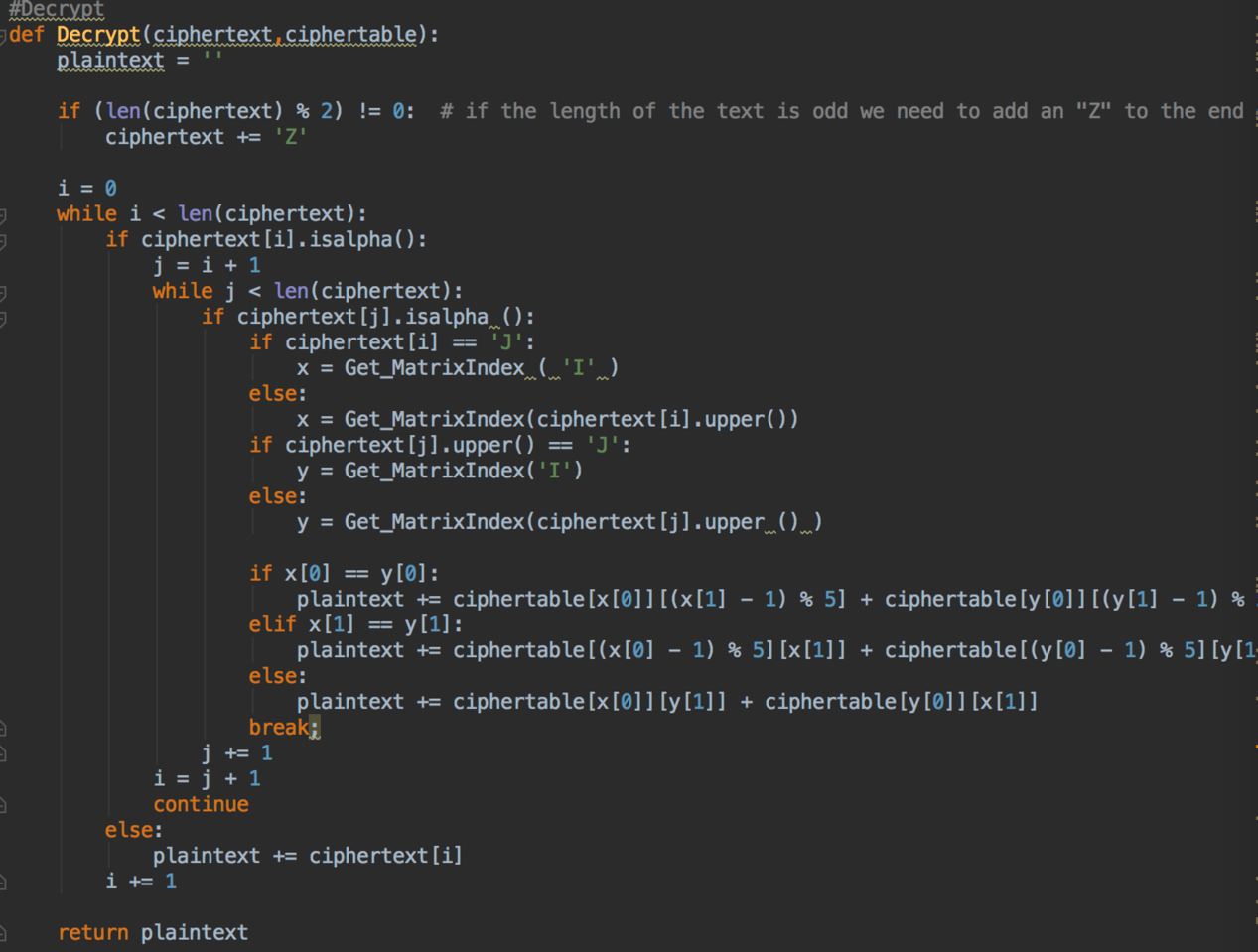
When we obtain the key, we have to build the cipher table. First of all ,remove the dulicate word of key and replace the blank in the key.Secondly,obtain each letter in letter\_list(as know as alphabet),if the letter is not in the key, then add to key.By now we got 25 key letters, then we need to build a 5\*5 cipher table.Create another variable j,obtain each letter in key,then add to array[j].Because each column of cipher table has 5 characters ,so if (i+1)%5==0,j=j+1.i is the column and j is the row.



After we build the Cipher table,we need to get the position of plaintext or ciphertext in cipher table.From above we can see input of this function is ‘ch’. “ch” is each letter in the plaintext or ciphertext.So we search from cipher table and it will return i and j.i is column and j is row



After we build the cipher table, we can start to encrypt messages. I encrypt message by using my own function. It need input plaintext and cipher table. Frist of all, create a String called ‘plaintext’ and its initial value is none. We also need to replace the blank due to we have to count the number of text and add ‘Z’ if the length is odd. After doing this, we need to create two variable i and j in order to obtain the character of plaintext. The first loop is going to obtain column and inside this loop there is another loop to get the row. Abstract the letter when it begin with English letter. If the letter is “J”, we need to get the position of “I” because the rule of playfair cipher says that we need to exchange “J” to “I”. When we got the position of letter, if two letters are in the same column, we take letter below them to replace. If both letters are in the same row, take the letter to the right of each one If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle After doing this, we can output the plaintext



We can also decrypt messages. It likes the reverse version of encrypt. It is same as the encrypt function in some way but it take the opposite position to output the ciphertext of encryption

**Reference**