**CE708 computer security**

**Assignment 2**

**Professor: Dr Hossein Anisi**

**Student: Lyu Yaowei**

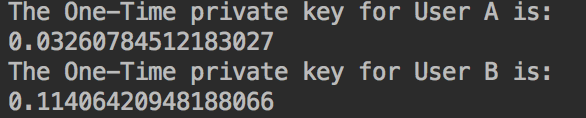
**Student Number: 1802697**

**Submit date:18th December**

In this program, we are going to use the re and random packages.

**Question 1**

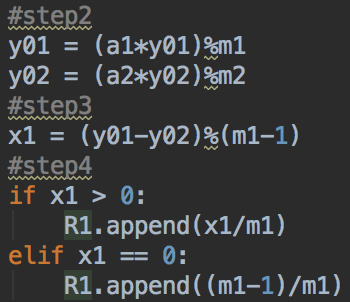
Result:



In this question,we are going to use the combined liner congruential generators. In the assignment ,we are asked to generate two random number from (1,2,147,483,641) and from (1,2,147,483,422).



Then we going to use the combined liner congruential generators to generate two one-time private key for user A and user B. Following the step of the combined liner that we learned from the lecture.



**Question 2**

Result:



In the question 2 we are going to use the Diffie-Hellman algorithm and the private key generated in the question 1. the user A private key in question 1is 

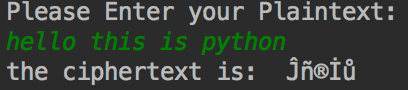
The user B private key is .

After we getting the private key, so we can use the Diffie-Hellman algorithm. First of all, we need to compute the public key of user B or the public key of user A. I am going to use user B to explain the excuse of the algorithm. We calculate the public key of user B by using the pow function in Python. in this question, a is 3 xb is the private key of user B and q is 353. Because the secret key for user A and user B is the same, so we only need to compute one secret key.

Key = (yb^xa)mod q.

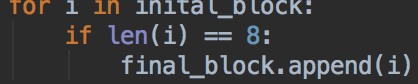
**Question 3**

Results:



In this question,we are going to use RC4 algorithm and the secret key generated in the question 2. First of all, we need to generate the block text of 64 bits which is 8 bytes.we use the re package to split the message into 8 bytes and add to the array.





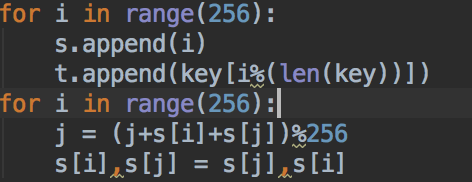
Then we output the last element which is the last 64-bits block text.



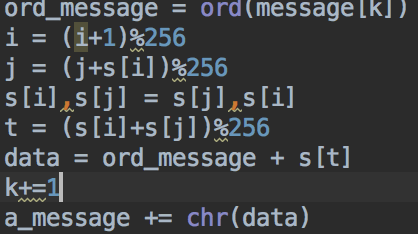
If the user enter the message that length is less than 8 bytes ,we can ask them to re-enter the message.



After create the last 64bits block, we going to use the RC4 algorithm to encrypt the message. First we need to create the S-box

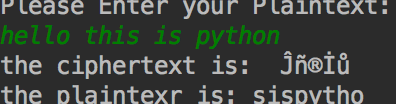


i is the index of s-box and j is in order to disorganize the s-box. Then we need to XOR the each element in the message with the s-box.



**Question 4**

Results:



In this question we are going to use the RC4 algorithm and the ciphertext generated in the question 3. The question 4 is actually reverse of question 3. we also need to create the s-box and XOR the ciphertext with the s-box.

But the difference between the 3 and 4 is decryption. So we need to minus the ciphertext with the s-box.