Report for Information Security Project 1

Jose Pedro Saraiva Vaz

Problem:

You are given parts of the plaintext and the ciphertext. • Ciphertext was generated by applying 13 rounds of autokey cipher. • Length of the primer key is 20, and the length of plaintext/ciphertext is 100.

✓ Plaintext: DECRYPTINGACIPHERGEN????????????????????????????????????????????ISSOLVABLEWITHOU????????????????????

✓ Ciphertext: ????????????????????RRAYLLEEDUIREFGHRSEPRRTXRYUOWEVRRTUVSPROOLRZVSFOLINBLEJVGUOHTXNOJVAGTHEFECERGXRY

(? are unknown alphabet characters)

Goals:

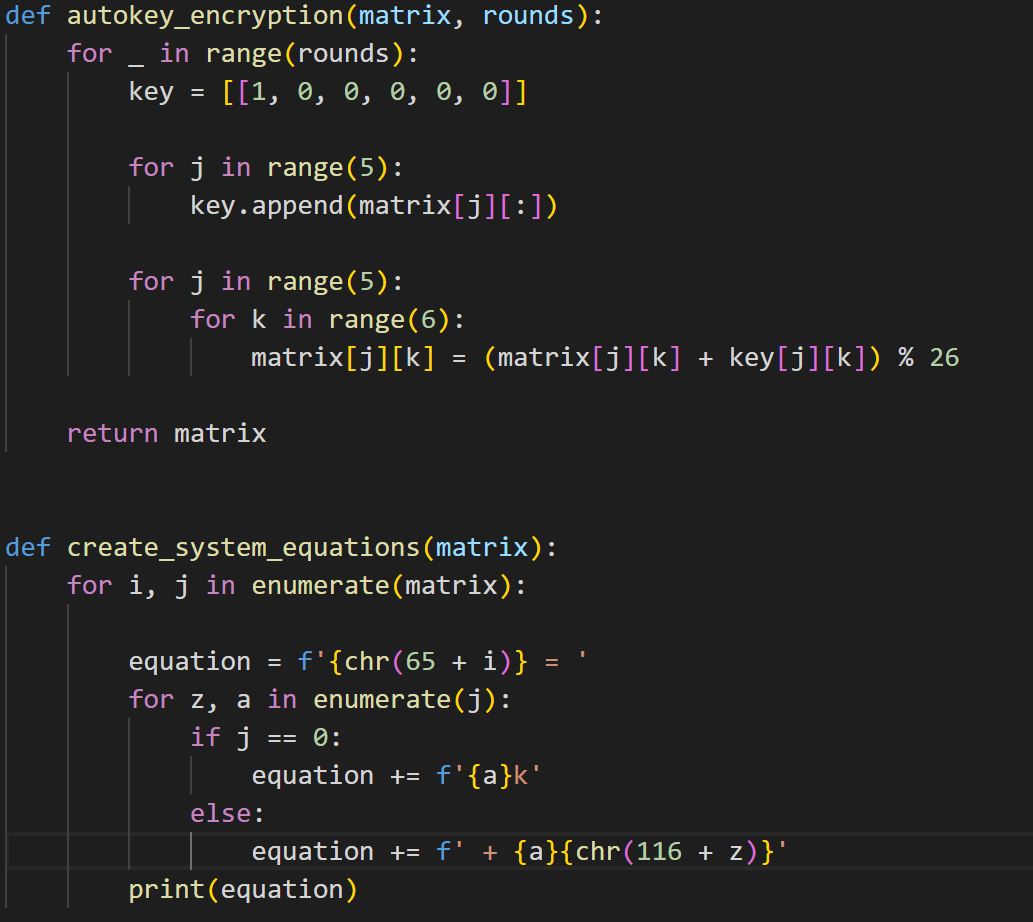
1. Find out the original plaintext

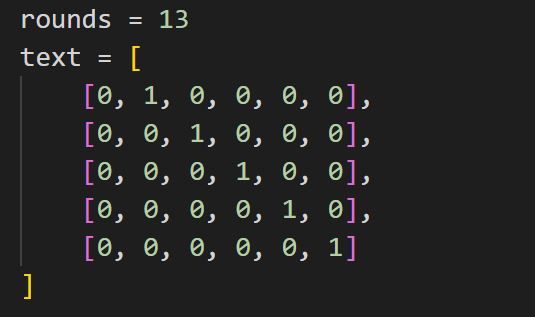
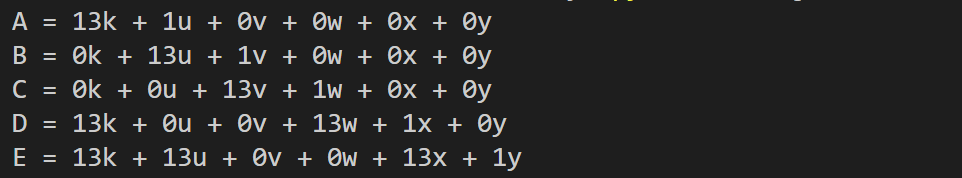
2. Describe in detail your strategy of decryption step by step (Reports with insufficient explanation can be degraded)

Solution:

For this case I thought the best approach would I tried to find algebraically a way to represent how the ciphertext was obtained in consideration to plaintext and knowing that for the autokey ciper encryption the formula is Ci = (Pi + ki) mod 26 I made the a function to represent it. However I decided to split the plaintext and ciphertext into 5 chunks of 20 characters in order to make it possible to perform a description. This number was chosen because the first 20 characters for the plaintext are known, the unknown primer key is also 20 characters long and we only do not known the last 20 characters of the ciphertext.

I made a function that would create a system of equations with this and the result ended up being



And in this case each equation represents how the cypher key was produced

A,B,C,D,E = Represent the ciphertext in positions 1 to 20, 20 to 40, 40 to 60, 60 to 80 and 80 to 100 respectively.

K = primer key

u,v,w,x,y = Represent the ciphertext in positions 1 to 20, 20 to 40, 40 to 60, 60 to 80 and 80 to 100 respectively.

After rearranging the formulas in order to obtain the plaintext we get:

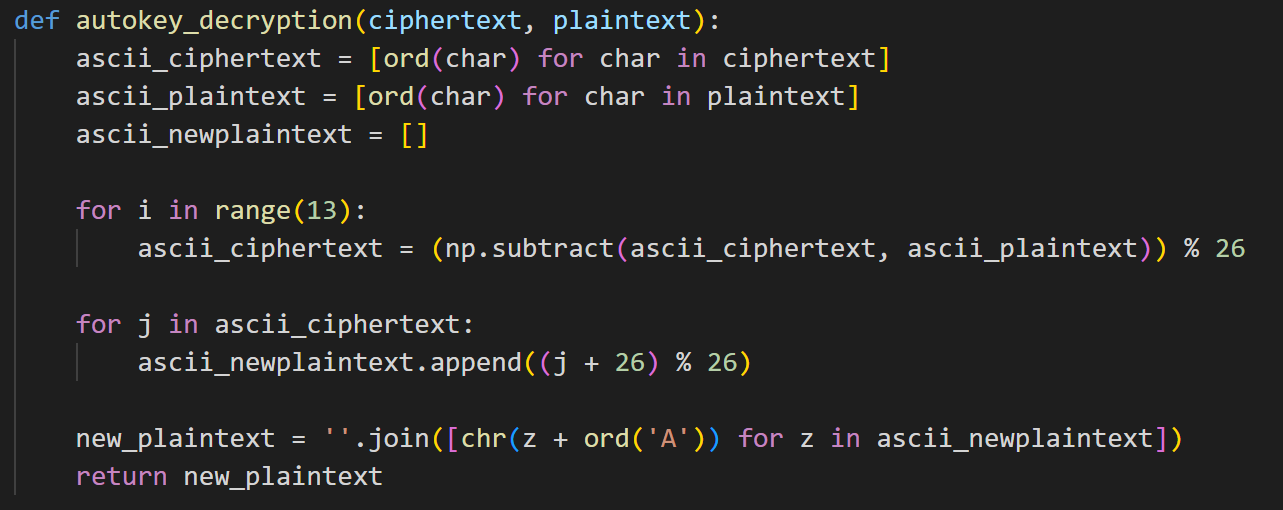
u = a -13k

v = B – 13u

w = C – 13v

x = D - 13k – 13w

y = E – 13k – 13u – 13x



This was not necessary to do anything to obtain u since we were given the first 20 characters of the plaintext in the problem

For v and w it is very straight forward it just applying autokey decryption formula Pi = (Ci - Ki) mod 26 for 13 iterations. But in this case K is the plaintext like we showed in the previous system of equations.

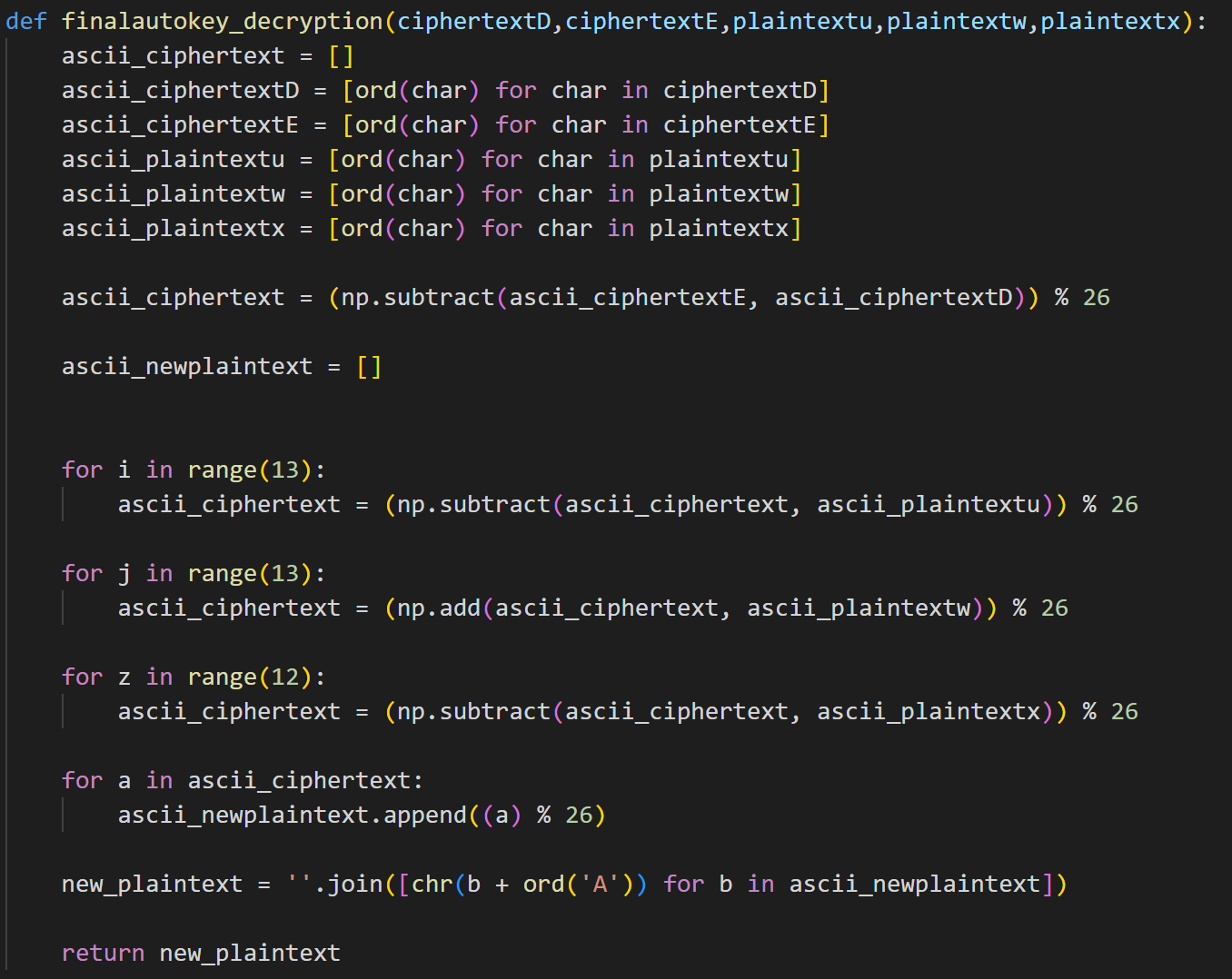
u= DECRYPTINGACIPHERGEN  
v=ERALLYREQUIRESTHESEC  
w=RETKEYHOWEVERTHISPRO

When we got x we encountered a problem because it has 13k and we do not know what the key is. However we were given previously 16 characters in problem. Therefore, we can make a guess taking into consideration all the plaintext characters known.

DECRYPTINGACIPHERGENERALLYREQUIRESTHESECRETKEYHOWEVERTHISPRO????ISSOLVABLEWITHOU

Since there 4 characters we had to discover and the previous word was not complete and the word after ???? was a new one I assumed it was a word with 7 characters starting in PRO. And taking into consideration this sentence I chose BLEM as the unknown characters. And this I knew the plaintext for all characters from 1 to 80. Only having the characters from 81 to 100 left with the final equation being y y = E – 13k – 13u – 13x. This equation initially is impossible to compute as we do not know the key. However using our system of equations we can rearrange our equations to get rid of 13k by using another variable that also contains 13k in this case being D. Ending up with y = E – D – 13u – 12x + y.

It was not possible to compute this equation in our previously created function as a lot more variables would be used and inputted. Therefore, a final decryption function was created.



This function allowed to get the plaintext for position 81 to 100 which is TKNOWINGTHESECRETKEY.

Having this way solved the problem and found the original plain text which is

DECRYPTINGACIPHERGENERALLYREQUIRESTHESECRETKEYHOWEVERTHISPROBLEMISSOLVABLEWITHOUTKNOWINGTHESECRETKEY

