CSI Rapport For Lab 3 Exo 3 and 7

Guebli Ayoub Abdessami Group 2

Exo 03 :

To do our calculations ,first we have this 2 method , to convert string to number and number to string:

```
def LtoN(a):
   return [ord(c) - ord('A') for c in a.upper()]

def NtoL(a):
   return "".join(chr(num + ord('A')) for num in a)
```

So after this we can calculate, we will need to calculate the diff between this 2 word we have (`"HQQYAJT"` and `"RJAJPWG"`) so we used this method to do that

```
def sub_mod_26(t1, t2):
   n1 = LtoN(t1)
   n2 = LtoN(t2)
   return [(num1 - num2) % 26 for num1, num2 in zip(n1, n2)]
```

So after calculating the diff between this words , we opened the dictionary and started adding the diff to all words of this dictionary by the next method :

```
def add_mod_26(t1, diff):
   n1 = LtoN(t1)
   return NtoL([(num1 + d) % 26 for num1, d in zip(n1, diff)])
```

and checking if the word is true by checking in the dictionary again , so the code will be like this

exo3.py

```python
def LtoN(a):
    return [ord(c) - ord('A') for c in a.upper()]

def NtoL(a):
    return "".join(chr(num + ord('A')) for num in a)

def sub_mod_26(t1, t2):
    n1 = LtoN(t1)
    n2 = LtoN(t2)
    return [(num1 - num2) % 26 for num1, num2 in zip(n1, n2)]

def add_mod_26(t1, diff):
    n1 = LtoN(t1)
    return NtoL([(num1 + d) % 26 for num1, d in zip(n1, diff)])

w1 = "HQQYAJT"
w2 = "RJAJPWG"
diff = sub_mod_26(w1, w2)
possible_pairs = []

with open('fr.txt', 'r') as file:
    words = [line.strip().upper() for line in file if len(line.strip()) == 7]
    words_set = set(words)

for word1 in words:
    expected_word2 = add_mod_26(word1, diff)
    if expected_word2 in words_set:
        possible_pairs.append((word1, expected_word2))

for pair in possible_pairs:
    print(pair)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

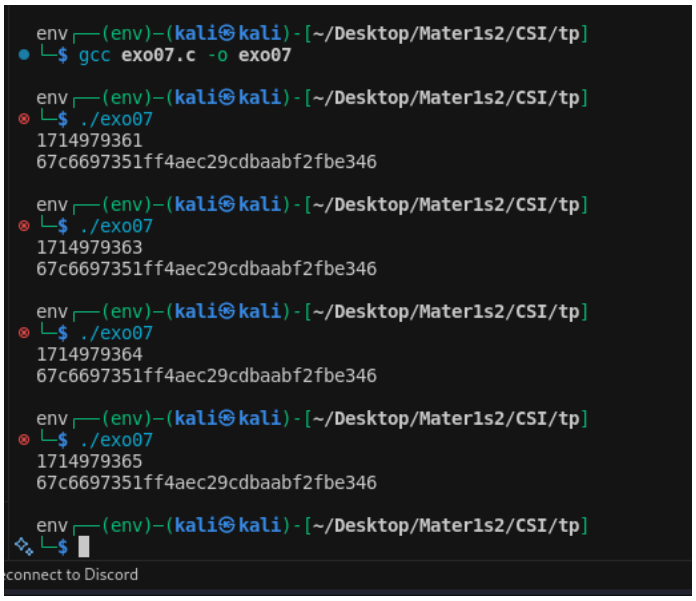
```
env ┌──(env)─(kali㉿kali)-[~/Desktop/Mater1s2/CSI/tp]
└─$ /home/kali/Desktop/Mater1s2/CSI/tp/env/bin/python /home/kali/Desktop/Mater1s2/CSI/tp/exo3.py
('MASQUER', 'CHIFFRE')

env ┌──(env)─(kali㉿kali)-[~/Desktop/Mater1s2/CSI/tp]
└─$
```

Exo 07 :

1- everytime a new key

2- same key everytime



So the srand is reponsable to create a key using the time , and every second the time changed so a new key

3- to ket the right key , we first generate all the keys are probably the ones, and searching the one by testing all that keys, so by that c , we created all the keys we can generate on that day by this c code (3 hours before , i didnt find the key in so i did all the day) and i saved the time on unix type , to make it easy to know what time the key generated:

```c
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#define KEYSIZE 16

int main() {
   int i;
   long long start_time, end_time;
   unsigned char key[KEYSIZE];

   struct tm timeinfo = {0};
   timeinfo.tm_year = 2018 - 1900; // Year since 1900
   timeinfo.tm_mon = 3;            // Month (0-11)
   timeinfo.tm_mday = 18;          // Day of the month
   timeinfo.tm_hour = 22;          // Hour
```

```
    timeinfo.tm_min = 1;            // Minute
    timeinfo.tm_sec = 49;           // Second
    end_time = mktime(&timeinfo);
    printf("Unix Timestamp: %lld\n", (long long)end_time);

    start_time = end_time - 24 * 3600;

    FILE *fp = fopen("keys.txt", "w");
    if (fp == NULL) {
        printf("Failed to open file for writing.\n");
        return 1;
    }

    for (long long t = start_time; t <= end_time; t++) {
        srand(t);
        for (i = 0; i < KEYSIZE; i++) {
            key[i] = rand() % 256;
        }

        fprintf(fp, "%lld,", t);
        for (i = 0; i < KEYSIZE; i++) {
            fprintf(fp, "%.2x", (unsigned char) key[i]);
        }
        fprintf(fp, "\n");
    }

    fclose(fp);
    printf("Done generating keys.\n");

    return 0;
}
```

So i got the keys on the file “keys.txt” , then i tried to use the Crypto library , to use the AES algorithm , then by that iv i have , and every key , i ty to generate cipher by AES.new , and try to decrypt the cipher text and i should have the plain text to know that key is right so i did this

```
from Crypto.Cipher import AES

plaintext = bytes.fromhex('255044462d312e350a25d0d4c5d80a34')
ciphertext = bytes.fromhex('d06bf9d0dab8e8ef880660d2af65aa82')
```

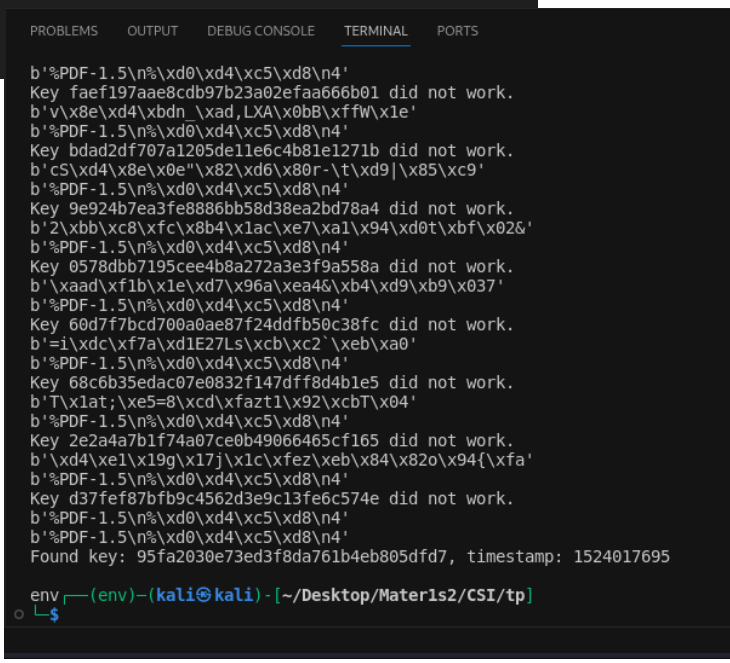
```python
iv = bytes.fromhex('09080706050403020100A2B2C2D2E2F2')

def try_decrypt(ciphertext, key, iv):
    cipher = AES.new(key, AES.MODE_CBC, iv)
    decrypted = cipher.decrypt(ciphertext)
    return decrypted

with open('keys.txt', 'r') as file:
    hex_keys = file.readlines()

for hex_key in hex_keys:
    date,key_hex = hex_key.split(',')
    key_hex = key_hex.strip()
    key = bytes.fromhex(key_hex)
    decrypted = try_decrypt(ciphertext, key, iv)
    print(decrypted)
    print ( plaintext )
    if decrypted == plaintext:
        print(f'Found key: {key.hex()}, timestamp: {date}')
        break
    else:

        print(f'Key {key.hex()} did not work.')
```



So by execute the next code i got this

Found key: 95fa2030e73ed3f8da761b4eb805dfd7
, timestamp: 1524017695

And by using a website to get the time from unix type I got this time :

GMT: Wednesday, April 18, 2018 2:14:55 AM

4- Use a cryptographically secure randomnumber generator and avoid using predictable seeds like timestamps for cryptographic key generation.