**Ministerul Educaţiei Tineretului şi Sportului al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**RAPORT**

**LA CRIPTOGRAFIE**

Tema: Criptogragia cu chei publice

Lucrarea de Laborator nr. 5

A efectuat Studentul grupei \_SI-212\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_Vozian Vladimir\_\_\_\_

*semnătura nume, prenume*

A verificat Andronatiev Victor

*nume, prenume profesor*

**Chisinău 2022**

***Sarcin*a 2**. **De elaborat un program în unul din limbajele de programare preferate pentru implementarea unui element al algoritmului DES. Sarcina se va alege în conformitate cu numărul** *n* **de ordine al studentului din lista grupei, în conformitate cu formula: nr\_sarcina = *n* mod 11. Pentru fiecare sarcină să fie afișate la ecran tabelele utilizate și toți pașii intermediari. Datele de intrare să fie posibil de introdus de utilizator sau de generat în mod aleatoriu.**

## Atenție! La susținerea lucrării vor fi puse întrebări despre lucrul întregului algoritm!!!

## Varianta

2.2. Fiind dat *K*+ în algoritmului DES, de determinat *Ci* și *Di* pentru un *i* dat.

## Mersul lucrării

Codul:

Key\_p = input("Introduceti Key+ =>")

Key\_p = Key\_p.replace(" ","")

while len(Key\_p) != 56:

    print("Cheia trebuie sa fie egala cu 56 de biti, introduceti cheia din nou")

    Key\_p = input("Introduceti Key+ =>")

#Key\_p = "11110000110011001010101011110101010101100110011110001111"

list = list(Key\_p)

length = len(list)

middle\_index = length // 2

C = list[:middle\_index]

D = list[middle\_index:]

print(C)

print(D)

i = int(input("Dati i (1<=i<=16) pentru Ci si Di dorit: (1<=i<=16)"))

for a in range (1,i):

    if (i==1 or i==2 or i==9 or i==16):

        C.append(C.pop(0))

        D.append(D.pop(0))

    else:

        C.append(C.pop(0))

        C.append(C.pop(0))

        D.append(D.pop(0))

        D.append(D.pop(0))

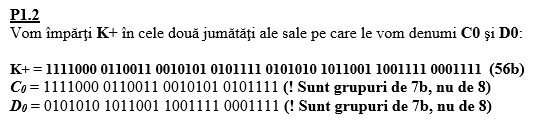
print(C)

print(D)

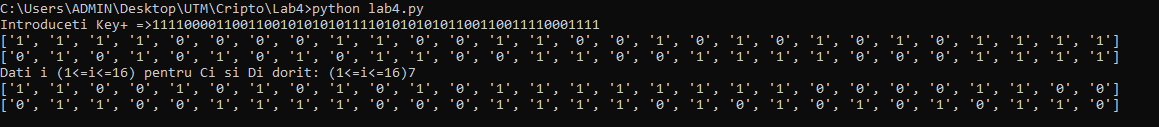
Deci cerem sa fie introdusa K+ si anume cu lungimea de 56 biți, altfel noi cerem cheia incontinuu. Se sterg spațiile ce pot fi introduse și începem cu împarțirea cheii in 2 liste diferite C0 si D0. Dupa ce prin for parcurgem iterația și anume etapa i pentru Ci Di și pentru i=1,2,9,16 mișcăm lista cu un bit in rest cu 2. Și afișăm rezultatul.

Rezultat:

Ca exemplu sa luat chiar modelul din file-ul prezentat de profesor DES ro:



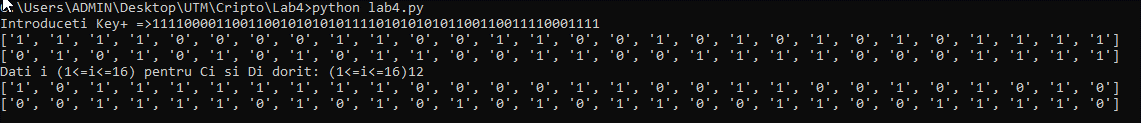
Și anume rezultatul pentru i=7





Din câte vedem rezultatele corespund.

Și pentru i=12





Concluzii:

Lucrarea dată era efectuată in python, lucrul efectuat cu părțile anumite ale cifrului DES era interesant, având mai multe alternative de execuție, la început venind ideea de a lucra deodata cu Bit operations in python, dar operatorii in python nu au putut satisface cerințele, pana la urma mam decis sa efectuez lucrarea utilizând lucrul cu string si schimbul caracterelor sau cu lista, ca rezultat am lucrat cu lista folosind functia pop.