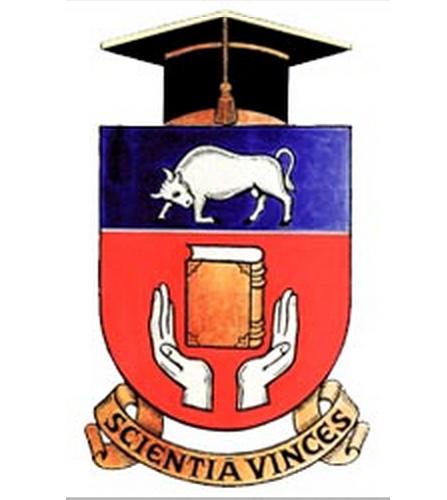
Universitatea de Stat din Tiraspol

Facultatea de Fizica Matematica si Informatica



Impartirea Secretelor

**Elaborat de**: Dordea Pavel, student gr.3i

**Verificat**: Globa Angela

**Chișinău, 2021**

**Împărțirea secretelor. Schema lui Shamir**

Fie că trebuie expediat un pin cod: YURII

Y –24

U –20

R –17

I –08

I –08

YURII - 2420170808

Schema lui Shamir se bazează pe interpolarea polinomială

1. Fie *S* – secretul; *S*=2420170808;
2. Alegem aleator *k* coieficienți: a1, a2, ..., ak;

*k=*6; a1=12; a2=3; a3=15; a4=7; a5=20; a6=27;

1. Construim polinomul: *f*(*x*)= ak·*xk* +ak-1·*xk*-1 + ... + a1·*x*+a0

a0=S;

*f*(*x*)= 26∙x6+20·*x*5+7·*x*4 + 15·*x*3+ 3·*x 2*+12·*x+*2420170808

1. Se alege un număr *n*=18; n - numărul de umbre (curieri)

Definesc umbrele, adică formez perechile (*i*, *f*(*i*))

|  |  |
| --- | --- |
| X | F(X) |
| 1 | 2420170891 |
| 2 | 2420173380 |
| 3 | 2420195657 |
| 4 | 2420300632 |
| 5 | 2420645943 |
| 6 | 2421551876 |
| 7 | 2423588005 |
| 8 | 2427678552 |
| 9 | 2435226467 |
| 10 | 2448256228 |
| 11 | 2469575361 |
| 12 | 2502954680 |
| 13 | 2553327247 |
| 14 | 2627006052 |
| 15 | 2731920413 |
| 16 | 2877871096 |
| 17 | 3076804155 |
| 18 | 3343103492 |

Ubrele se repartizează ca perechi:

**(1,** 2420170891**), (2,** 2420173380**),…, (18,** 3343103492**)**

Pentru restabilirea secretului avem nevoie de *k*+1 umbre

Deoarece *k*=6, atunci avem nevoie de 7 umbre pentru restabilirea secretului.

Pentru restabilirea polinomului vom aplica polinomul de interpolare Lagrange:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | X0 | X1 | X2 | X3 | X4 | X5 | X6 |
| i,x | 2 | 5 | 8 | 10 | 12 | 15 | 18 |
| f(i),y | 2420173380 | 2420645943 | 2427678552 | 2448256228 | 2502954680 | 2731920413 | 3343103492 |
|  | y0 | y1 | y2 | y3 | Y4 | Y5 | Y6 |

=...+...+ 2420170808

Secretul restabilit este: 2420170808

Pentru a obține secretul inițial se împarte numărul în secvențe de 2 cifre de la dreapta spre stânga: 24 20 17 08 08. Dacă prima secvență ete formată dintr-o cifră, atunci se adaugă 0 în fața sa: 24 20 17 08 08– YURII.

Sarcină.

1. Secretul lui Shamir, pentru k=5
2. Program
3. De verificat rezultatele de la pl1 și de afișat screenshot.

2.cod:

# -\*- coding: utf-8 -\*-

"""

Created on Wed Nov 10 13:21:17 2021

@author: Pavel

"""

import tkinter as tk

import random

root= tk.Tk()

root.resizable(0,0)

root.title('Impartirea secretelor')

root.configure(bg='#164A41')

L1=tk.Label(root,text="Introdu cheia secreta s :",bg='#164A41',fg='#FFFFFF',font='Helvetica 14 bold').grid(row=0,column=0,sticky='w')

sec = tk.Entry(root,bg='#F1B24A',fg='#FFFFFF',font='Helvetica 12 bold')

sec.grid(row=0,columnspan=3,sticky='ne')

L2=tk.Label(root,text="Introdu n (in cite parti va fi divizat secretul):",bg='#164A41',fg='#FFFFFF',font='Helvetica 14 bold').grid(row=1,column=0,sticky='w')

nec = tk.Entry(root,bg='#F1B24A',fg='#FFFFFF',font='Helvetica 12 bold')

nec.grid(row=1,columnspan=3,sticky='ne')

L3=tk.Label(root,text="Introdu k (cite bucati sunt necesare pentru restabilirea cheii):",bg='#164A41',fg='#FFFFFF',font='Helvetica 14 bold').grid(row=2,column=0,sticky='w')

kec = tk.Entry(root,bg='#F1B24A',fg='#FFFFFF',font='Helvetica 12 bold')

kec.grid(row=2,column=1)

b=[]

L7=tk.Label(root,text="",bg='#164A41',fg='#FFFFFF',font='Helvetica 10 bold')

L7.grid(row=6,column=1,sticky='w')

def afla():

s=sec.get()

s = int(sec.get())

k = int(kec.get())

a = random.sample(range(1, 100), k)

n = int(nec.get())

def F(t):

w = s

for i in range(len(a)):

w += a[len(a)-i-1]\*pow(t,len(a)-i)

return w

#a=[12,3,15,7,20,26]

L5["text"]=str(a)

for i in range (1,n+1):

b.append(F(i))

for i in range (0,n):

L7["text"]+=("["+str(i+1)+"] "+str(b[i])+" \n")

L10['text']+="("+str(k)+' pozitii din lista de mai sus):'

x=[]

def calc():

y=[]

final=0

k = int(kec.get())

for i in range(k+1):

value = (nume.get())

value = value.split(' ')

x = [int(x) for x in value]

y.append(b[x[i]-1])

for g in range(k+1):

p2=p1=1

for r in range(k+1):

if (g != r):

p2 \*= (x[g]-x[r])

p1 \*= x[r]

final += ((p1\*y[g])/p2)

L12["text"]="CHEIA RESTABILITA ESTE:"

L13["text"]=round(final)

button\_afla = tk.Button(root,text="Calculeaza",command=afla,bg='#4D774E',fg='#FFFFFF',font='Helvetica 12 bold').grid(row=4,columnspan=3,sticky='we')

L4=tk.Label(root,text="Numerele aleatoare generate:",bg='#164A41',fg='#FFFFFF',font='Helvetica 12 bold').grid(row=5,column=0,sticky='w')

L5=tk.Label(root,text="",bg='#164A41',fg='#FFFFFF',font='Helvetica 10 bold')

L5.grid(row=5,column=1,sticky='w')

L6=tk.Label(root,text="Perechile de numere in care a fost impartita cheia:",bg='#164A41',fg='#FFFFFF',font='Helvetica 12 bold').grid(row=6,column=0,sticky='w')

L8=tk.Label(root,text="RESTABILIREA CHEII:",bg='#164A41',fg='#FFFFFF',font='Helvetica 12 bold underline').grid(row=7,column=0,columnspan=3,sticky='n')

L9=tk.Label(root,text="Introduceti perechile de numere care participa la restabilirea cheii:",bg='#164A41',fg='#FFFFFF',font='Helvetica 12 bold').grid(row=8,column=0,sticky='w')

L10=tk.Label(root,text="Numarul de ordine a perechii ",bg='#164A41',fg='#FFFFFF',font='Helvetica 12 bold')

L10.grid(row=9,column=0,sticky='w')

nume=tk.Entry(root,bg='#F1B24A',fg='#FFFFFF',font='Helvetica 12 bold')

nume.grid(row=9,column=1,sticky='w')

L12=tk.Label(root,text="",bg='#164A41',fg='red',font='Helvetica 12 bold')

L12.grid(row=11,column=0,columnspan=3,sticky='w')

L13=tk.Label(root,text="",bg='#164A41',fg='red',font='Helvetica 12 bold')

L13.grid(row=11,column=1,sticky='ne')

#button\_ceck = tk.Button(root,text="Adauga",command=check).grid(row=11,column=0)

button\_calc = tk.Button(root,text="Decrypteaza",command=calc,bg='#4D774E',fg='#FFFFFF',font='Helvetica 12 bold').grid(row=10,columnspan=3,sticky='we')

root.mainloop()

3.

