**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

Факультет кібербезпеки, комп’ютерної та програмної інженерії

Кафедра комп’ютеризованих систем захисту інформації

**ЗВІТ З ЛАБОРАТОРНОЇ РОБОТИ №4**

**«КРИПТОГРАФІЧНІ СИСТЕМИ ЯКІ ЗАСНОВАНІ БАЗІ**

**ЕЛІПТИЧНИХ КРИВИХ»**

**КИЇВ – 2022**

**Тема:** криптографічні системи які засновані базі еліптичних кривих

**Мета:** отримати навички у створенні програмної реалізації криптографічної системи яка заснована базі еліптичних кривих.

**Основні завдання:**

1. Розробити об’єктно-орієнтованою мовою програмування консольний або віконний додаток, що реалізує шифрування та дешифрування вмісту текстового або виконуваного файлу з використанням апарату еліптичних кривих. Програма повинна запитувати ім'я вхідного і вихідного файлів, тип шифру та вхідні параметри для проведення криптографічних перетворень. В якості вхідних параметрів виступають: еліптична крива: *p*=751; *a*= -1; *b*=1; *E*751(-1,1); *y*2 = *x*3-*x*+1(mod751); генеруюча точка: G = (0, 1).
2. Представити блок структурну схему своєї програмної реалізації.
3. Зробити висновки на підставі проведених теоретичних та практичних досліджень. У висновках слід зазначити, які навички та знання отримано під час виконання завдань.

**Хід виконання та результати роботи.**

**Блок-схема**

****

Рисунок 1 – блок-схема

**Спочатку обраховуються лямбди.**

from random import random

###############################################PreMain block

def lyambda1(x1, y1, p, a):

l = ((3 \* pow(x1, 2) + a) / 2\*y1) % p

return l

def lyambda2(x1, y1, x2, y2, p):

l = ((y2 - y1) /(x2 - x1)) % p

return l

def odraz(x1, x2, y1, y2, p, a):

if x1 == x2 and y1 == y2:

l = lyambda1(x1, y1, p, a)

else:

l = lyambda2(x1, y1, x2, y2, p)

return l

def y(l, x1, x3, y1, p):

y3 = l \* (x1 - x3) - y1 % p

return y3

def x(l, x1, x2, p):

x3 = (pow(l, 2) - x1 - x2) % p

return x3

###############################################PreMain block

**Далі уже програма бере дані з інпут файлу і в моєму випадку це моя прізвище Bezpalyi,** яке в ASCII виглядає: 208 145 208 181 208 183 208 191 208 176 208 187 208 184 208 185 10. **За варіантом Ka = 15 Kb = 4.**

*def main():*

*file = input(Inputter1 .txt\n')*

*f = open(file, encoding="utf-8")*

*M = int(f.read())*

*print('M = ', M)*

*p = 751*

*a = -1*

*b = 1*

*E = (-1, 1)*

*G = (0, 1)*

*ka = random.randint(1, 100)*

*kb = random.randint(1, 100)*

*r = random.randint(1, 100)*

*print("Значення за варіантом:")*

*print("Повідомлення: ", M)*

*print("p = ", p)*

*print("a = ", a)*

*print("b = ", b)*

*print("E = ", E)*

*print("y^2=((x^3)-x+1)mod751")*

*print("G = ", G)*

*print("ka = ", ka)*

*print("kb = ", kb)*

**Далі обраховується Ya.**

*x1 = G[0] y1 = G[1]*

*x2 = G[0] y2 = G[1]*

*l = odraz(x1, x2, y1, y2, p, a)*

*x3 = x(l, x1, x2, p) y3 = y(l, x1, x3, y1, p)*

*Ya = (x3, y3)*

*print("Відкритий ключ користувача A: Ya = ", Ya)*

**Після цього обраховується Yb.**

*x1 = G[0] y1 = G[1]*

*x2 = G[0] y2 = G[1]*

*l = odraz(x1, x2, y1, y2, p, a)*

*x3 = x(l, x1, x2, p) y3 = y(l, x1, x3, y1, p)*

*Yb = (x3, y3)*

*print("Відкритий ключ користувача B: Yb = ", Yb)*

*print("Шифрування:")*

**Потім рахуємо rG(R):**

*x1 = G[0] y1 = G[1]*

*x2 = G[0] y2 = G[1]*

*l = odraz(x1, x2, y1, y2, p, a)*

*x3 = x(l, x1, x2, p) y3 = y(l, x1, x3, y1, p)*

*rG = (x3, y3)*

*print("rG = ", rG)*

**Також розрахуємо**

*x1 = Yb[0] y1 = Yb[1]*

*x2 = Yb[0] y2 = Yb[1]*

*l = odraz(x1, x2, y1, y2, p, a)*

*x3 = x(l, x1, x2, p) y3 = y(l, x1, x3, y1, p)*

*rYb = (x3, y3)*

*print("rYb = ", rYb)*

*x = rYb[0]*

*C = (M\*x) %p*

**Ну і далі виводяться дані**

*print("C = ", C)*

*print("Криптограма: ", C)*

*print("Дешифрування:")*

*# Q = kb\*rG*

*x1 = rG[0] y1 = rG[1]*

*x2 = rG[0] y2 = rG[1]*

*l = odraz(x1, x2, y1, y2, p, a)*

*x3 = x(l, x1, x2, p) y3 = y(l, x1, x3, y1, p)*

*Q = (x3, y3)*

*print("kb\*rG = ", Q)*

*x = Q[0]*

*M = (C \* x\*\*(p-1))%p*

*print("M-", M)*

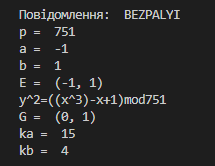
**

Рисунок 1 – повідомлення та інші параметри

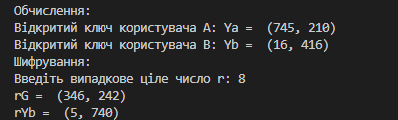
**

Рисунок 2 – Програма просить ввести випадкове число наприклад 8

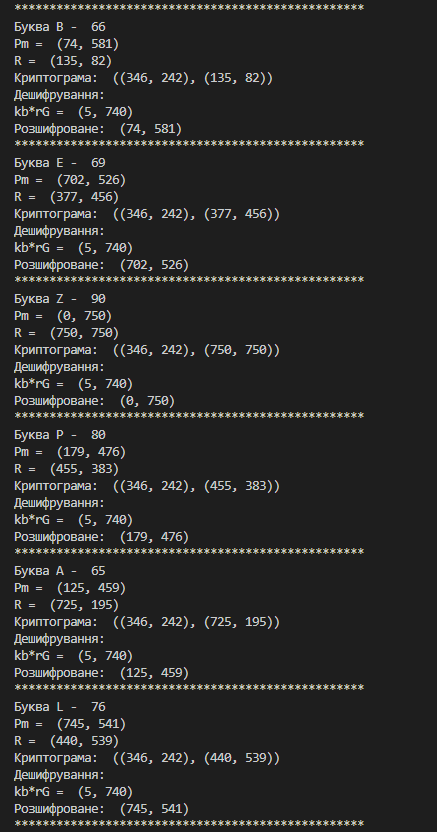
**

Рисунок 3 – Вивід букв

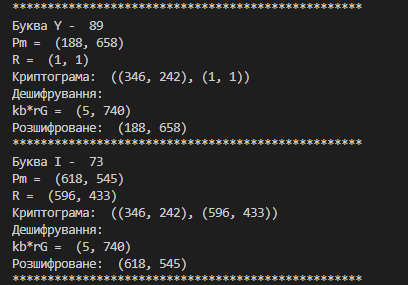
**

Рисунок 4 – Вивід букв

**Загальний код**

*from random import random*

*def lyambda1(x1, y1, p, a):*

*l = ((3 \* pow(x1, 2) + a) / 2\*y1) % p*

*return l*

*def lyambda2(x1, y1, x2, y2, p):*

*l = ((y2 - y1) /(x2 - x1)) % p*

*return l*

*def odraz(x1, x2, y1, y2, p, a):*

*if x1 == x2 and y1 == y2:*

*l = lyambda1(x1, y1, p, a)*

*else:*

*l = lyambda2(x1, y1, x2, y2, p)*

*return l*

*def y(l, x1, x3, y1, p):*

*y3 = l \* (x1 - x3) - y1 % p*

*return y3*

*def x(l, x1, x2, p):*

*x3 = (pow(l, 2) - x1 - x2) % p*

*return x3*

*def main():*

*file = input('Файл с cообщением .txt\n')*

*f = open(file, encoding="utf-8")*

*M = int(f.read())*

*print('M = ', M)*

*p = 751*

*a = -1*

*b = 1*

*E = (-1, 1)*

*G = (0, 1)*

*ka = random.randint(1, 100)*

*kb = random.randint(1, 100)*

*r = random.randint(1, 100)*

*print("Значення за варіантом:")*

*print("Повідомлення: ", M)*

*print("p = ", p) print("a = ", a) print("b = ", b) print("E = ", E)*

*print("y^2=((x^3)-x+1)mod751")*

*print("G = ", G) print("ka = ", ka) print("kb = ", kb)*

*# Ya:*

*x1 = G[0] y1 = G[1]*

*x2 = G[0] y2 = G[1]*

*l = odraz(x1, x2, y1, y2, p, a)*

*x3 = x(l, x1, x2, p)*

*y3 = y(l, x1, x3, y1, p)*

*Ya = (x3, y3)*

*print("Відкритий ключ користувача A: Ya = ", Ya)*

*# Yb:*

*x1 = G[0] y1 = G[1]*

*x2 = G[0] y2 = G[1]*

*l = odraz(x1, x2, y1, y2, p, a)*

*x3 = x(l, x1, x2, p) y3 = y(l, x1, x3, y1, p)*

*Yb = (x3, y3)*

*print("Відкритий ключ користувача B: Yb = ", Yb)*

*print("Шифрування:")*

*# rG(R):*

*x1 = G[0] y1 = G[1]*

*x2 = G[0] y2 = G[1]*

*l = odraz(x1, x2, y1, y2, p, a)*

*x3 = x(l, x1, x2, p) y3 = y(l, x1, x3, y1, p)*

*rG = (x3, y3)*

*print("rG = ", rG)*

*# rYb(P):*

*x1 = Yb[0] y1 = Yb[1]*

*x2 = Yb[0] y2 = Yb[1]*

*l = odraz(x1, x2, y1, y2, p, a)*

*x3 = x(l, x1, x2, p) y3 = y(l, x1, x3, y1, p)*

*rYb = (x3, y3)*

*print("rYb = ", rYb)*

*x = rYb[0]*

*C = (M\*x) %p*

*print("C = ", C)*

*print("Криптограма: ", C)*

*print("Дешифрування:")*

*# Q = kb\*rG*

*x1 = rG[0] y1 = rG[1]*

*x2 = rG[0] y2 = rG[1]*

*l = odraz(x1, x2, y1, y2, p, a)*

*x3 = x(l, x1, x2, p) y3 = y(l, x1, x3, y1, p)*

*Q = (x3, y3)*

*print("kb\*rG = ", Q)*

*x = Q[0]*

*M = (C \* x\*\*(p-1))%p*

*print("M-", M)*

**Висновок:** В результаті роботи було отримано програму в якій реалізовано програмне шифрування за алгоритмами криптографічних системи які засновані базі еліптичних кривих. Еліптична криптографія – розділ криптографії, який вивчає асиметричні криптосистеми, засновані на еліптичних кривих над кінцевими полями. Головна перевага еліптичної криптографії полягає в тому, що на сьогодні є невідомим існування субекспоненціальних алгоритмів вирішення завдань дискретного логарифмування. Використання еліптичних кривих для створення криптосистем було незалежно запропоновано Нілом Коблицем та Віктором Міллером у 1985 році.