1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —

**Институт кибербезопасности и защиты информации**

**ЛАБОРАТОРНАЯ РАБОТА №7**

1. «РАЗЛОЖЕНИЕ ЧИСЛА НА МНОЖИТЕЛИ НА ЭЛЛИПТИЧЕСКОЙ КРИВОЙ»
2. по дисциплине «Криптографические методы защиты информации»
3. Выполнил
4. студент гр. 4851003/70801 Гасанов Э.А.

<*подпись*>

1. Преподаватель
2. ассистент Ярмак А.В.

<*подпись*>

1. Санкт-Петербург
2. 2021

**Цель**

Реализация метода разложения числа на множители с использованием эллиптических кривых.

**Задание**

1. Вариант задания — 4
2. Разработать программу (**П-1**), реализующую разложение составного числа на эллиптической кривой.

**Ход работы**

Была написана программа на Python, реализующая алгоритм Ленстры поиска нетривиального делителя. Программа запускалась на различных примерах. Одно из самых больших чисел, проверенных в программе — 243308563933342444717. Число имеет размер 68 бит. За 1.27 секунды был найден 1 из 2 больших простых множителей числа — 15598351303 (34 бита). Для разложения использовалась кривая с коэффициентами a = 243153617065481326702 и b = 135832024027725137541. Начальная точка на кривой — (224144440102439826369 : 158292496274155451076 : 1).

|  |  |
| --- | --- |
| Число бит | Время, с |
| 20, n=1942114 | 0.000505208969116 |
| 40, n=1475933774372 | 0.00075500221252 |
| 45, n=34777999240230 | 0.000813961029053 |
| 47, n=140331115506726 | 0.00434303283691 |
| 50, n=984781815442598 | 0.00113892555237 |
| 68,n=243308563933342444717 | 1.27016084865187 |

# Вывод

Был изучен алгоритм Ленстры для поиска нетривиального делителя составного числа. Также были изучены особенности применения (псевдо)кривых над кольцом классов вычетов.

1. **Как зависит сложность разложения составного числа заданной длины методом эллиптических кривых от числа различных простых делителей числа n?**

Сложность зависит от размера минимального простого делителя, и, следовательно, чем больше простых делителей, тем меньше их размер, и там быстрее будет найден нетривиальный делитель.

1. **Сравните сложность разложения на эллиптической кривой составного числа вида , где − различные простые числа, и составного числа такой же длины, состоящего из двух различных простых делителей.**

Разложение в первом случае должно выполниться быстрее, так как длина простых множителей меньше.

# Приложение

Исходный код программы:

from random import randint

import time

def mul(n, P, k):

r = P-P

while k > 0:

if k % 2 == 1:

if r != P:

d = gcd(n,r[0]-P[0])

if d > 1:

print d

return d, P-P

else:

d = gcd(n,2\*P[1])

if d > 1:

print d

return d, P-P

r += P

d = gcd(n,2\*P[1])

if d > 1:

print d

return d

P += P

k //= 2

return 1, r

def fact(n):

B1 = int(sqrt(n))

print B1

while True:

while True:

x = randint(0,n)

y = randint(0,n)

a = randint(0,n)

b = (y^2 - x^3 - a\*x) % n

g = gcd(n, 4\*a^3+27\*b^2)

if 1 < g < n:

print g

return

elif g != n:

break

E = EllipticCurve(Integers(n),[a,b])

P0 = E(x,y)

print E

print P0

P = P0

for p in Primes():

if p > B1:

break

p0=p

p\*=p0

while p < B1:

p\*=p0

d, P = mul(n, P, p0)

if d > 1:

return

print "Here"

B=int(1.1\*B)

k = 2\*\*34

c = randint(int(sqrt(k)),k)

p = next\_prime(c)

q = next\_prime(p)

print p,q

start = time.time()

fact(p\*q)

end = time.time()

print "Time elapsed: ", end - start