Математические основы защиты информации и информационной безопасности

Отчет по лабораторной работе № 6

Меньшов Иван Сергеевич НПМмд-02-21

Содержание

# Цель работы

Изучить разложение чисел на множетели. Реалезовать р - метод Полларда.

# Теоретические сведения

## Разложение чисел на множетели

Задача разложения на множители — одна из первых задач, использованных для построения криптосистем с открытым ключом.

Задача разложения составного числа на множители формулируется следующим образом: для данного положительного целого числа n найти его каноническое разложение где рi — попарно различные простые числа, ai > 1.

На практике не обязательно находить каноническое разложение числа n. Достаточно найти его разложение на два нетривиальных сомножителя: n = pq , 1<=р<=q<n. Далее будем понимать задачу разложения именно в этом смысле.

## P - метод Полларда

P - метод Полларда - алгоритм разработанный Джоном Поллардом для разлажения числа n на множетели. Данный алгоритм выглядит следующим образом:

Вход. Число n, начальное значение c , функция f, обладающая сжимающим свойством

Выход. Нетривиальный делитель числа n.

1. Положить a = c , b = c
2. Вычислить a = f(a)(mod n) , b = f(f(b))(mod n)
3. Найти d = НОД(a - b, n)
4. Если 1 < d < n, то положить p = d и результат: p. При d = n результат:‘Делитель не найден’ .При d = 1 вернуться на шаг 2.

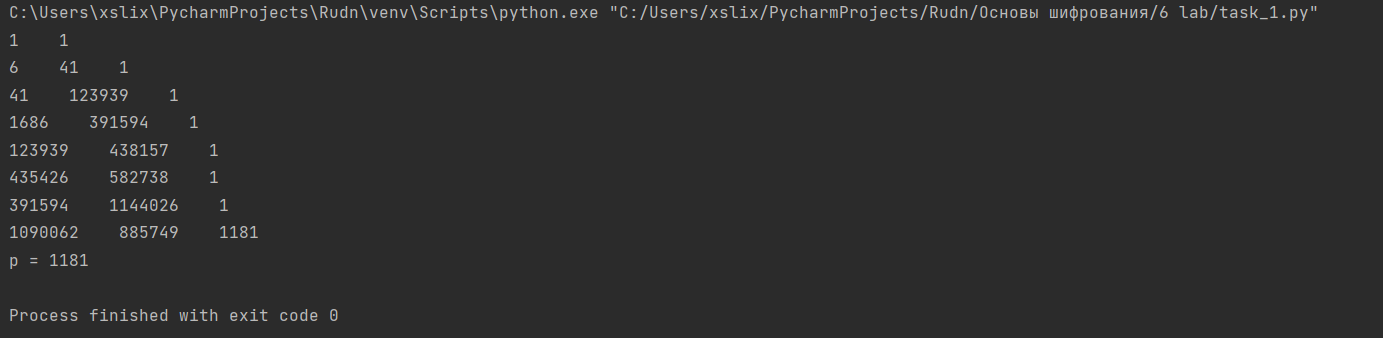
# Выполнение работы

## Реализация алгоритма на языке Python

*P - метод Полларда*

import math  
  
  
def func(x, y):  
 return (x \*\* 2 + 5) % y  
  
  
c = 1  
a = c  
b = c  
n = 1359331  
print(a, b, sep=' ')  
while True:  
 a = func(a, n) % n  
 b = func(func(b, n), n) % n  
 d = math.gcd(a - b, n)  
 print(a, b, d, sep=' ')  
 if 1 < d < n:  
 p = d  
 print(f'p = {p}')  
 break  
 elif d == n:  
 print('Делитель не найден')

## Контрольный пример



P - метод Полларда

# Выводы

Мной было изучено разложение чисел на множетели, а также реализован р - метод Полларда.

# Список литературы

1. [Инструкция к лабораторной работе №6](https://esystem.rudn.ru/pluginfile.php/1283459/mod_folder/content/0/lab06.pdf?forcedownload=1)