

## Лабораторная работа 6

Попов Дмитрий Павлович, НФИмд-01-23

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра математического моделирования и искусственного интеллекта

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Математические основы защиты информации и информационной безопасности

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Попов Дмитрий Павлович

Группа: НФИмд-01-23

МОСКВА

2023 г.

# **Прагматика выполнения лабораторной работы**

# Прагматика выполнения лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий р-метод Полларда

## Цель работы

# Цель работы

Освоение на практике разложение чисел на множители.

## **Выполнение лабораторной работы**

1. Для реализации р-метода Полларда:



# 1. Для реализации р-метода Полларда:

1. Функция, реализующая р-метод Полларда
2. Функция нахождения НОД

```
1  def rho(x):
2      return f(x) % N
3
4  def pollards_rho(N, c, f):
5      a = b = c
6      while True:
7          a = rho(a)
8          b = rho(rho(b))
9          d = gcd(abs(a - b), N)
10         if 1 < d < N:
11             return d
12         elif d == N:
13             return "Делитель не найден"
14
15     # Функция для нахождения наибольшего общего делителя (НОД)
16     def gcd(a, b):
17         while b:
18             a, b = b, a % b
19         return a
```

Figure 1: pollard

2. Основная функция запуска где получаем входные значения и шифруем слово

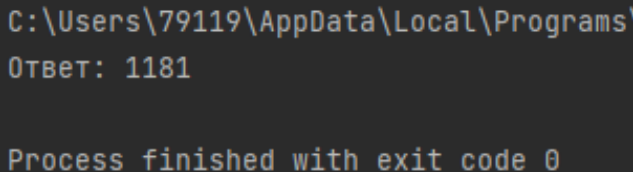
## 2. Основная функция запуска где получаем входные значения и шифруем слово

```
23  N = 1359331
24  c = 1
25  f = lambda x: (x**2 + 5) % N
26
27  result = pollards_rho(N, c, f)
28  print("Ответ:", result)
```

Figure 2: init

### 3. Выходные значения программы

### 3. Выходные значения программы



```
C:\Users\79119\AppData\Local\Programs\
Ответ: 1181

Process finished with exit code 0
```

Figure 3: output

## Выводы

## Выводы

В результате выполнения работы я освоил на практике алгоритм разложения чисел на множители.

