

Лабораторная работа 6

Серенко Данил Сергеевич, НФИмд-01-23

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

ПРЕЗЕНТАЦИЯ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

дисциплина: Математические основы защиты информации и информационной безопасности

Преподаватель: Кулябов Дмитрий Сергеевич

Студент: Серенко Данил Сергеевич

Группа: НФИмд-01-23

МОСКВА

2023 г.

Прагматика выполнения лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий r -метод Полларда

Цель работы

Освоить на практике разложение чисел на множители.

Выполнение лабораторной работы

1. Для реализации r -метода Полларда:

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

```

def pollards_rho(N, c, f):
    a = b = c

    def rho(x):
        return f(x) % N

    while True:
        a = rho(a)
        b = rho(rho(b))
        d = gcd(abs(a - b), N)

        if 1 < d < N:
            return d
        elif d == N:
            return "Делитель не найден"

# Функция для нахождения наибольшего общего делителя (НОД)
def gcd(a, b):
    while b:
        a, b = b, a % b
    return a

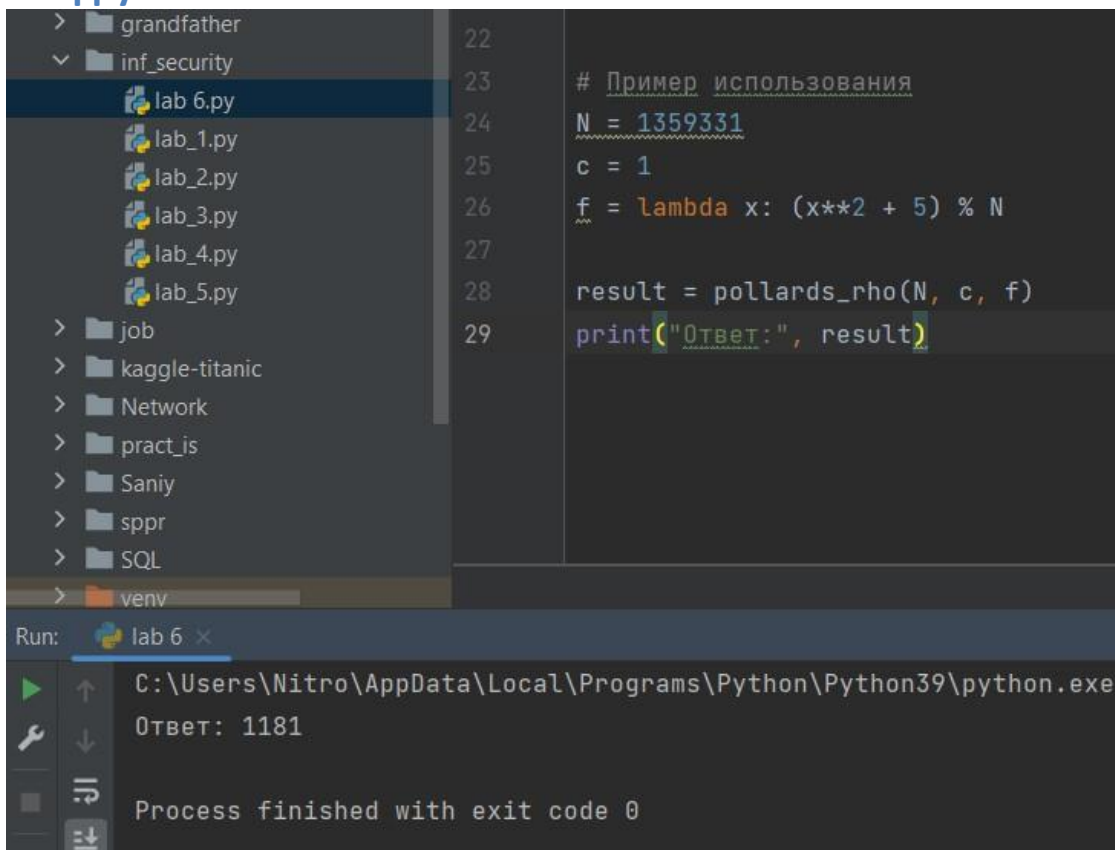
# Пример использования
N = 1359331
c = 1
f = lambda x: (x**2 + 5) % N

result = pollards_rho(N, c, f)
print("Ответ:", result)

```

main_func

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



```
> grandfather
  > inf_security
    > lab 6.py
    > lab_1.py
    > lab_2.py
    > lab_3.py
    > lab_4.py
    > lab_5.py
  > job
  > kaggle-titanic
  > Network
  > pract_is
  > Saniy
  > sppr
  > SQL
  > venv

Run: lab 6 x
C:\Users\Nitro\AppData\Local\Programs\Python\Python39\python.exe
Ответ: 1181
Process finished with exit code 0
```

```
22
23 # Пример использования
24 N = 1359331
25 c = 1
26 f = lambda x: (x**2 + 5) % N
27
28 result = pollards_rho(N, c, f)
29 print("Ответ:", result)
```

output

Выводы

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