

Математические основы защиты информации и информационной безопасности. Отчет по лабораторной работе №6

Шифрование гаммированием

Серенко Данил Сергеевич 1132236895

Содержание

Цель работы

Освоить на практике разложение чисел на множители.

Выполнение лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий р-метод Полларда

р-метод Полларда

Метод Полларда применяется при факторизации натуральных чисел.

Основные шаги:

Вход: число N , начальное значение s , функция f , обладающая сжимающими свойствами
Выход: нетривиальный делитель n
1) положить $a \leftarrow s$, $b \leftarrow s$
2) Вычислить $a \leftarrow f(a) \pmod{n}$, $b \leftarrow f(b) \pmod{n}$
3) Найти $d \leftarrow \text{НОД}(a-b, n)$
4) Если $1 < d < n$, То положить $p \leftarrow d$
и результат: p . При $d=n$ результат: "Делитель не найден"; при $d=1$ вернуться на шаг 2

Чтобы реализовать программу был написан след. код на python:

1. Функция, реализующая р-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

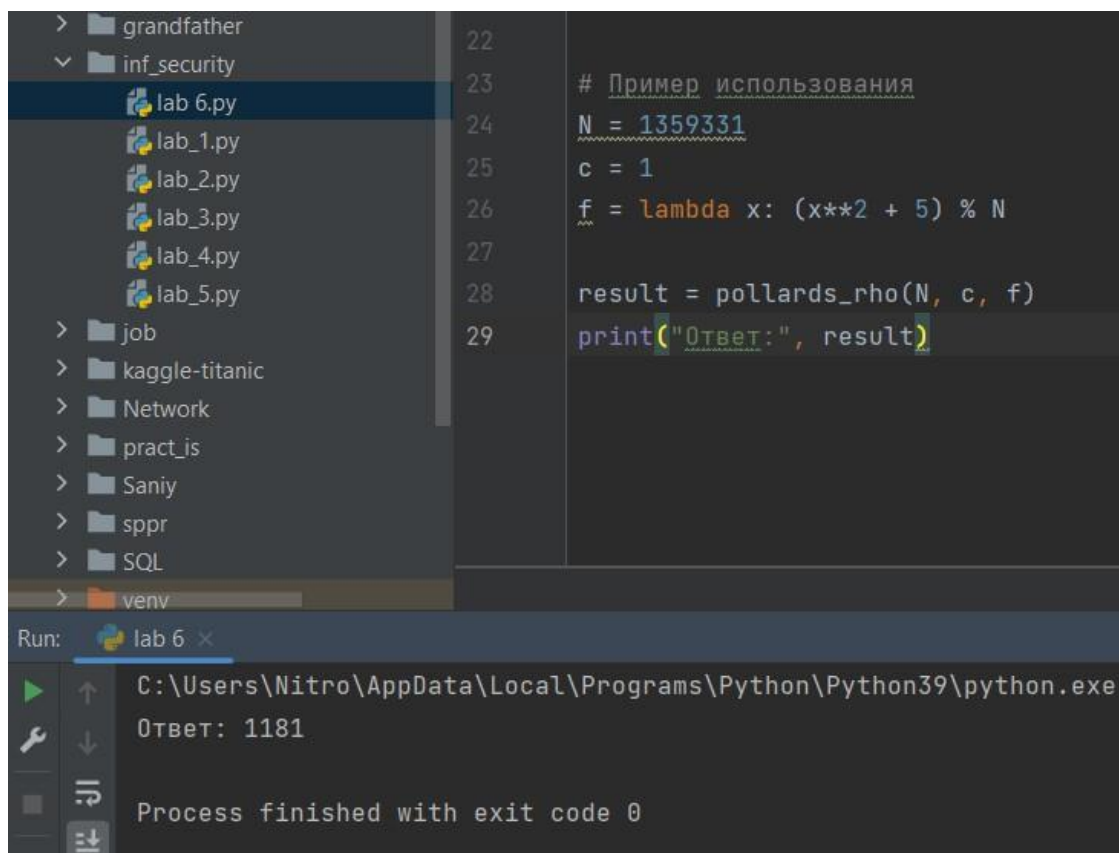
# Пример использования
N = 1359331
c = 1
f = lambda x: (x**2 + 5) % N

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

```

main_func

Выходные значения программы (пример из методички).



The screenshot shows a code editor with a file explorer on the left. The file explorer lists folders like 'grandfather', 'inf_security', 'job', 'kaggle-titanic', 'Network', 'pract_is', 'Saniy', 'sppr', 'SQL', and 'venv'. Under 'inf_security', there are files 'lab 6.py', 'lab_1.py', 'lab_2.py', 'lab_3.py', 'lab_4.py', and 'lab_5.py'. The 'lab 6.py' file is selected, and its code is visible in the editor. The code is a Python script that uses a function 'pollards_rho' to find a factor of a number 'N'. The script sets 'N = 1359331' and 'c = 1', then defines a function 'f = lambda x: (x**2 + 5) % N'. It then calls 'pollards_rho(N, c, f)' and prints the result. The output of the script is 'Ответ: 1181'. The 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)
```

Run: lab 6 x

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

output

Выводы

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

Список литературы

1. Методические материалы курса