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

Шифрование гаммированием

Терентьев Егор Дмитриевич 1132236902

Содержание

List of Figures

List of Tables

1 Цель работы

Освоить на практике разложение чисел на множители.

2 Выполнение лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий p-метод Полларда

2.1 p-метод Полларда

Метод Полларда применяется при факторизации натуральных чисел.

Основные шаги:

Вход: число N, начальное значение c, функция f, обладающая сжимающими свойствами Выход: нетривиальный делительно числа n 1) положить a <- c, b <- c 2) Вычислить a Б- f(a)(mod n), b <- f(b) (mod n) 3) Найти d <- НОД(a-b, n) 4) Если 1< d< n, То положить p <- dи результат: p. При d=n результат: “Делитель не найден”; при d=1 вернуться на шаг 2

Чтобы реализовать программу был написал след. код на python:

1. Функция, реализующая p-метод Полларда
2. Функция нахождения НОД fig. 2.1.

```python
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
```

Figure 2.1: main_func

Выходные значения программы (пример из методички) fig. 2.2.

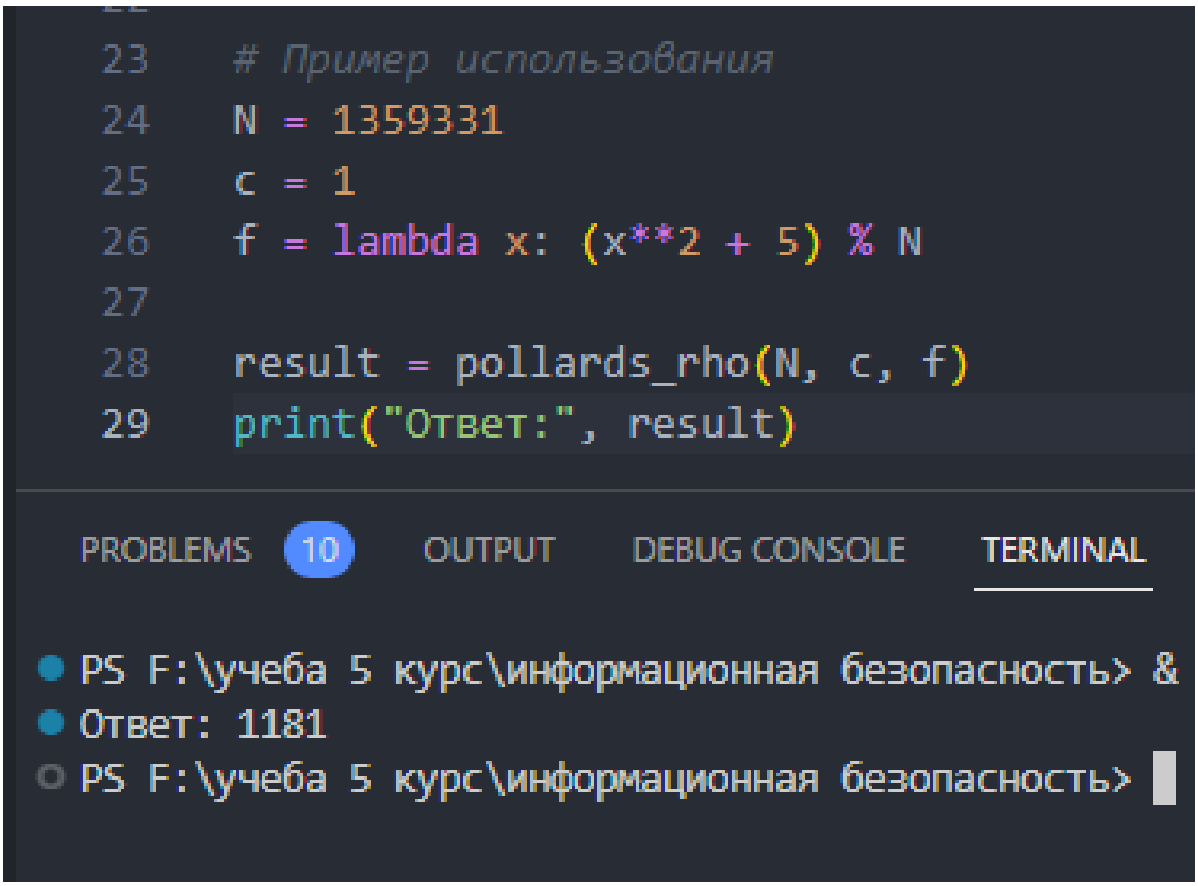

Figure 2.2: output

3 Выводы

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

4 Список литературы

1. Методические материалы курса