Лабораторная работа 6

Терентьев Егор Дмитриевич, 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

Преподователь: Кулябов Дмитрий Сергеевич
Студент: Терентьев Егор Дмитриевич
Группа: НФИмд-01-23

МОСКВА
2023 г.

Прагматика выполнения лабораторной работы

Прагматика выполнения лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий p-метод Полларда

Цель работы

Цель работы

Освоить на практике разложение чисел на множители.

Выполнение лабораторной работы

1. Для реализации p-метода Полларда:

1. Для реализации p-метода Полларда:

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

```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:
```

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

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

```
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)
```

PROBLEMS 10 OUTPUT DEBUG CONSOLE TERMINAL

```
PS F:\учеба 5 курс\информационная безопасность> &
Ответ: 1181
PS F:\учеба 5 курс\информационная безопасность>
```

Figure 2: output

Выводы

Выводы

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