

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

**Шифрование гаммированием**

Юдин Герман Станиславович 1132236901

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
2.1	р-метод Полларда . . . . .	6
<b>3</b>	<b>Выводы</b>	<b>9</b>
<b>4</b>	<b>Список литературы</b>	<b>10</b>

# List of Figures

2.1	main_func . . . . .	7
2.2	output . . . . .	8

## List of Tables

# 1 Цель работы

Освоить на практике разложение чисел на множители.

## 2 Выполнение лабораторной работы

Требуется реализовать:

1. Алгоритм, реализующий р-метод Полларда

### 2.1 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 fig. 2.1.

```

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.

```
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)
```

PROBLEMS 10 OUTPUT DEBUG CONSOLE TERMINAL

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

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