

# **Отчет по лабораторной работе № 6.**

## **Разложение чисел на множители**

**дисциплина: Математические основы защиты информации и  
информационной безопасности**

**Наливайко Сергей Максимович**

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>3</b>
<b>2</b>	<b>Задание</b>	<b>4</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>5</b>
3.1	Реализация алгоритма разложения чисел на множители . . . . .	5
<b>4</b>	<b>Выводы</b>	<b>7</b>

# 1 Цель работы

Научиться реализовывать алгоритмы разложения чисел на множители.

## 2 Задание

- Реализовать алгоритм, реализующий  $p$ -метод Полларда.

## 3 Выполнение лабораторной работы

### 3.1 Реализация алгоритма разложения чисел на множители

Реализуем алгоритм разложения чисел на множители на языке программирования C++.

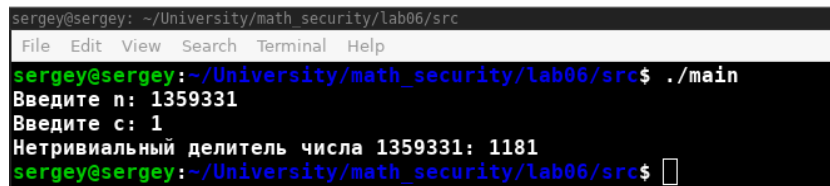
Код функции разложения чисел на множители:

```
uint64_t pollards_method(uint64_t n, uint64_t c, uint64_t (*f)(uint64_t))  
  
    uint64_t a = c, b = 1, p = -1;  
  
    while (true) {  
        uint64_t d;  
        b = f(b) % n;  
        a = f(f(a) % n) % n;  
        d = gcd(ABS(a, b), n);  
        if (d > 1 && d < n) {  
            p = d;  
        } else if (d == 1)  
            continue;  
        break;  
    }
```

```
    return p;  
}
```

Полный листинг программного кода представлен в файле main.cpp (архив lab06, директория src).

Скомпилируем и запустим программу fig. 3.1.



```
sergey@sergey: ~/University/math_security/lab06/src  
File Edit View Search Terminal Help  
sergey@sergey:~/University/math_security/lab06/src$ ./main  
Введите n: 1359331  
Введите c: 1  
Нетривиальный делитель числа 1359331: 1181  
sergey@sergey:~/University/math_security/lab06/src$
```

Figure 3.1: Разложение чисел на множители

## 4 Выводы

В ходе лабораторной работы мы реализовывали алгоритмы разложения чисел на множители.