

Отчет по лабораторной работе 6

Дисциплина: Математические основы защиты информации и информационной безопасности

Дяченко З. К.

25 ноября 2022

Российский университет дружбы народов, Москва, Россия

Данная лабораторная работа выполнялась мной для приобретения практических навыков разложения чисел на множители.

Ознакомится и реализовать программно алгоритм, реализующий р-метод Полларда.

Задачи выполнения лабораторной работы

Реализовать программно алгоритм, реализующий р-метод Полларда (рис. - fig. 1).

```
In [4]: def f(x):  
        return x*x+5  
  
In [16]: import math  
  
In [22]: def polard (n, c):  
        a=c  
        b=c  
        d=1  
        while (d!=1):  
            a=f(a)%n  
            b=f(f(b))%n  
            d=math.gcd(a-b, n)  
            if (1<d and d<n):  
                p=d  
                return p  
            if (d==n):  
                return ("Делитель не найден")  
  
In [23]: polard(1359331, 1)  
Out[23]: 1181
```

Figure 1: Реализация алгоритма, реализующего р-метод Полларда

Разложить число на множители (рис. - fig. 2).

```
In [23]: polard(1359331, 1)
```

```
Out[23]: 1181
```

```
In [19]: 1359331/1181
```

```
Out[19]: 1151.0
```

```
In [21]: 1181*1151
```

```
Out[21]: 1359331
```

Figure 2: Разложение на множители

Результатом выполнения работы стала реализация алгоритма нахождения нетривиального делителя, что можно использовать для разложения числа на множители, что отражает проделанную мной работу и полученные новые знания.