Отчёт по лабораторной работе №6
Разложение чисел на множители

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Агеева Анастасия Сергеевна, 1032212304
Группа: НФИмд-02-21
Преподаватель: д-р.ф.-м.н., проф. Кулябов Дмитрий Сергеевич

18 декабря, 2021, Москва

Прагматика

Прагматика данной лабораторной работы

- В рамках дисциплины “Математические основы защиты информации и информационной безопасности” нам необходимо изучить ее разделы.
- Данная работа необходима для более глубоко и детального понимания работы алгоритмов шифрования.

Цель

Цель выполнения данной лабораторной работы

- Цель данной лабораторной работы изучение разложения чисел на множители.

Задачи

Задачи выполнения данной лабораторной работы

1. Реализовать программно алгоритм, реализующий p-метод Полларда.

Результаты выполнения данной лабораторной работы

Реализация p-метод Полларда

In [5]:
```
def f(x, n):
    return (x**2 + 5)%n
```

Figure 1: Сжимающая функция f

In [24]:
```
def pollard(n, c):
    a = c
    b = c
    while True:
        a = f(a,n)%n
        b = f(f(b,n),n)%n
        d = euclid(abs(a-b), n)
        print(a, b, d)
        if 1 < d < n:
            p = d
            return p
        elif d == n:
            return "Делитель не найден"
```

Figure 2: Реализация p-метода Полларда

Результаты p-метод Полларда

```
In [25]:  p = pollard(1359331, 1)
          p

          6 41 1
          41 123939 1
          1686 391594 1
          123939 438157 1
          435426 582738 1
          391594 1144026 1
          1090062 885749 1181

Out[25]:  1181
```

Figure 3: Результаты p-метода Полларда

Выводы

- Исходя из теоретических сведений, программа выполнена без ошибок, чему свидетельствуют полученные результаты.
- В ходе данной лабораторной работы я реализовала программно p-метода Полларда нахождения нетривиального делителя.