Отчет по лабораторной работе 6

По предмету мат. основы защиты информации

Студент: Дидусь Кирилл Валерьевич, 1132223499
Группа: НПМмд-02-22
Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва, 2022

Содержание

1 Цель работы **5**

2 Задание **6**

3 Выполнение лабораторной работы **7**

4 Выводы **8**

5 Листинг программы **9**

Список иллюстраций

Список таблиц

1 Цель работы

Целью данной лабораторной работы является ознакомление с алгоритмом по разложению числа на множители.

2 Задание

Реализовать алгоритм для разложения заданного числа на 2 нетривиальных сомножителя.

3 Выполнение лабораторной работы

В ходе выполнения лабораторной работы было реализован алгоритм для разложения заданного числа на 2 нетривиальных сомножителя. Он реализует p-метод Полларда.

Программный код представлен в качестве листинга в конце отчета.

4 Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомился с алгоритмом для разложения заданного числа на 2 нетривиальных сомножителя, а так же мне удалось реализовать его на языке программирования Python.

5 Листинг программы

```
import math

def p_pollard(n,c,func):
    a = c
    b = func(c,n)
    count = 0
    while(True):
        a = func(a,n)
        b = func(b,n)
        d = math.gcd(a-b,n) #НОД
        count += 1
        if((d > 1) & (d < n)):
            return d
        elif(d == n):
            return "делитель не найден"
        if(count>100):
            return "ошибка вычисления"

def func(x,n):
    return (x**2 + 5)%n

print(p_pollard(133,1,func))
```