Защита лабораторной работы №6

Разложение чисел на множители

Бармина Ольга

2024 September 7th

Российский университет дружбы народов, Москва, Россия

Цель выполнения лабораторной работы

- Освоение *p-метода Полларда*, который является одним из алгоритмом разложения составного числа на множители
- Программная реализация представленного алгоритма разложения заданного числа на множители

Теоретические сведения

Задача разложения на множители - одна из первых задач, использованных для построения криптосистем с открытым ключом.

Задача разложения составного числа на множители: для данного положительного целого числа n найти его разложение на два *нетривиальных сомножителя*:

$$n = pq, 1 \leqslant p \leqslant q < n$$

Алгоритм, реализующий p-метод Полларда

Вход. Число n, начальное значение c, функция f, обладающая сжимающими свойствами.

Выход. Нетривиальный делитель числа n.

- положить $a \leftarrow c, b \leftarrow c$
- вычислить $a \leftarrow f(a)(mod\, n), b \leftarrow f(b)(mod\, n)$
- найти $d \leftarrow (a - b, n)$
- 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

Результат выполнения лабораторной работы

Постановка задачи:

- Реализовать алгоритм разложения числа на множители с помощью p-метода Полларда
- Разложить на множители заданное число

Результат выполнения лабораторной работы

Алгоритм, реализующий p-метод Полларда:

```
n = 1359331
c = 1
def f(x, n):
    return (x**2 + 5)%n
```

```
def pollard(n, a, b, f):
    a = f(a, n)
    b = f(f(b, n), n)

    c = a - b
    d = n
    if c < 0:
        d1 = 0
    else:
        while c!=0 and d!=0:
            if c>=d:
                c = c%d
            else:
                d = d%c
        d1 = c or d
    print(a, b, d1)

    if 1 < d1 < n:
        return d1
    elif d1 == n:
        return 'делитель не найден'
    else:
        pollard(n, a, b, f)
```

```
pollard(n, c, c, f)
```

```
6 41 0
41 123939 0
1686 391594 0
123939 438157 0
435426 582738 0
391594 1144026 0
1090062 885749 1181
```

Figure 1: p-метод Полларда

Выводы

Выводы

1. Изучили метод Полларда разложения чисел на множители
2. Программно реализовали представленный алгоритм разложения чисел на множители
3. Разложили на множители заданное число