Отчёт по лабораторной работе №6

Дисциплина: Математические основы защиты информации и информационной безопасности

Полиенко Анастасия Николаевна, НПМмд-02-23

Содержание

Список иллюстраций

1 Цель работы

Изучить алгоритмы разложения числа на множители.

2 Задание

Реализовать алгоритм p-метода Полларда.

3 Теоретическое введение

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

Задача разложения составного числа на множители формулируется следующим образом: для данного положительного целого числа n найти его каноническое разложение $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, где p_i - попарно различные простые числа, $\alpha_i \geq 1$

На практике не обязательно находить каноническое разложение числа n. Достаточно найти его разложение на два *нетривиальных сомножителя:* $n = pq, 1 \leq p \leq q < n$. Далее будем понимать задачу разложения именно в этом смысле.

p-Метод Полларда. Пусть n - нечетное составное число, $S = \{0, 1, \dots, n-1\}$ и $f : S \to S$ - случайное отображение, обладающее сжимающими свойствами, например $f(x) = x^2 + 1 \, (mod\, n)$. Основная идея метода состоит в следующем. Выбираем случайный элемент $x_0 \in S$ и строим последовательность $x_0, x_1, x_2, ...$, определяемую рекуррентным соотношением

$$x_{i+1} = f(x_i),$$

где $geq 0$, до тех пор, пока не найдем такие числа , j, что $< j$ и $x_i = x_j$. Поскольку множество S конечно, такие индексы , j существуют (последовательность «зацикливается»). Последовательность x_i будет состоять из «хвоста» $x_0, x_1, \dots, x_{i-1}$ длины $o\left(\sqrt{\frac{nm}{8}}\right)$ той же длины.

Более подробно см. в [1–6].

4 Выполнение лабораторной работы

Реализуем алгоритм алгоритм p-метода Полларда. (рис. 4.1)

```python
import numpy as np


def f(x, n):
    return (x**2 + 5) % n
n = 1359331
a = 1; b = 1
d = 1
while d == 1:
    a = f(a, n)
    b = f(f(b, n), n)
    d = np.gcd(a - b, n)
if d == n:
    print("Делитель не найден")
else:
    print("Нетривиальный делитель числа:", d)
```

```
Нетривиальный делитель числа: 1181
```

Рис. 4.1: p-метод Полларда.

5 Выводы

Изучила алгоритмы разложения числа на множители.

Список литературы

1. GNU Bash Manual [Электронный ресурс]. Free Software Foundation, 2016. URL: https://www.gnu.org/software/bash/manual/.
2. Newham C. Learning the bash Shell: Unix Shell Programming. O'Reilly Media, 2005. 354 с.
3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.
4. Robbins A. Bash Pocket Reference. O'Reilly Media, 2016. 156 с.
5. Таненбаум Э. Архитектура компьютера. 6-е изд. СПб.: Питер, 2013. 874 с.
6. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.