Лабораторная работа №6

Математические основы защиты информации и информационной безопасности

Леонтьева Ксения Андреевна | НПМмд-02-23

Содержание

# 1 Цель работы

Реализовать на языке программирования p-метод Полларда.

# 2 Теоретическое введение

**Задача разложения составного числа на множители** формулируется следующим образом: для данного положительного целого числа найти его каноническое разложение , где - попарно различные простые числа, .

На практике необязательно находить каноническое разложение числа . Достаточно найти его разложение на два *нетривиальных сомножителя:* .

**p-метод Полларда.** Пусть - нечетное составное число, и - случайное отображение, обладающее сжимающими свойствами, например, . Основная идея метода состоит в следующем. Выбираем случайный элемент и строим последовательность определяемую рекуррентным соотношением

где , до тех пор, пока не найдем такие числа , что и . Поскольку множество конечно, такие индексы существуют. Последовательность будет состоять из “хвоста” длины и цикла той же длины.

Более подробно см. в [1].

# 3 Выполнение лабораторной работы

p-метод Полларда реализуем по следующей схеме:

На вход подается число , начальное значение , функция , обладающая сжимающими свойствами.

1. Положить .
2. Создать функцию
3. Вычислить .
4. Найти НОД
5. Если , то положить и результат: . При результат: “Делитель не найден”; при вернуться на шаг 2.

Код программы (рис. 1).



Рис. 1: p-метод Полларда

# 4 Выводы

В ходе выполнения данной лабораторной работы был реализован p-метод Полларда.

# Список литературы

1. p-метод Полларда [Электронный ресурс]. URL: <https://en.wikipedia.org/wiki/Pollard%27s_rho_algorithm>.