Отчет по лабораторной работе №6

Дисциплина: Математические основы защиты информации и информационной безопасности

Живцова Анна

Содержание

# 1 Цель работы

Изучить алгоритм факторизации Полларда.

# 2 Задание

Реализовать алгоритм факторизации Полладра.

# 3 Теоретическое введение

Задача разложения на множители – одна из первых задач, использующихся для построения криптосистем с открытым ключем. Подробнее в источниках [1,2].

В данной работе будем использовать -метод Полларда, позволяющий найит нетривиальный делитель числа. Для реализации метода нужно задать сжимающую функцию на конечном множестве. В качестве примера такой функции используется где – число, у которого необходимо найти делитель.

# 4 Выполнение лабораторной работы

## 4.1 Программная реализация

Для реализации алгоритма факторизации Полладра на языке Python была написанна следующая функция.

def poladr(n, c, f, a, b):  
 d = nod(max(a-b, n), min(a-b, n))  
 print(a, b, d)  
 if d < n and d > 1:  
 return d  
 elif d == 1:  
 return None  
 a = f(a, n)%n  
 b = f(b, n)%n  
 b = f(b, n)%n  
 return poladr(n, c, f, a, b)

Тут – число, у которого необходимо найти делитель, – сжимающая функция, – начальное приближение, – текущие параметры алгоритма, использующиеся в рекурсии.

Дополнительно были реализованы функции нахождения наибольшего общего делителя и сжимающая функция на конечном множестве

def nod(a, b):  
 if b == 0:  
 return 0  
 while b != 0:  
 a = a%b  
 a, b = b, a  
 return a   
  
def func(x, n):  
 return (x\*\*2 + 5)%n

## 4.2 Проверка функциональности программы

Функциональность данной функции была протестирована в среде jupyter notebook (см. рис. 1). Функция действительно помогла найти нетривиальный делитель числа.

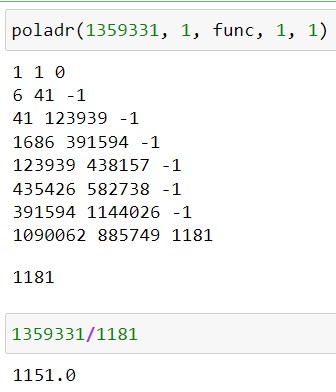


Рис. 1: Тестирование алгоритма факторизации Полладра

# 5 Выводы

В данной работе я изучила алгоритм факторизации Полладра, реализовала его программно и протестировала.

# Список литературы

1. Kulyabov D., Korolkova A., Gevorkyan M. Информационная безопасность компьютерных сетей: лабораторные работы. 2015.

2. Самуйлов К.Е. и др. Сети и телекоммуникации : Учебник и практикум. Издательство Юрайт, 2019. С. 1–363.