Лабораторная работа №6

Математические основы защиты информации и информационной безопасности

Полиенко Анастасия Николаевна

26 сентября 2023

Российский университет дружбы народов, Москва, Россия

НПМмд-02-23

Разложение чисел на множители

Цель лабораторной работы

Изучить алгоритмы разложения числа на множители.

Задачи лабораторной работы

Реализовать алгоритм p-метода Полларда.

Ход лабораторной работы

Код

Реализуем алгоритм алгоритм p-метода Полларда.

```
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)
```

Выводы

Изучила шифрование гаммированием.