Презентация по лабораторной работе №4

Дисциплина “Математические основы защиты информации и информационной безопасности”

Живцова А.А.

10 октября 2024

Кафедра теории вероятностей и кибербезопасности, Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Информация

Докладчик

- Живцова Анна Александровна
- студент кафедры теории вероятностей и кибербезопасности
- Российский университет дружбы народов имени Патриса Лумумбы
- zhivtsova_aa@pfur.ru
- https://github.com/AnnaZhiv

Вводная часть

Актуальность

Наибольший общий делитель чисел, позволяющий, например, определять взаимно простые числа, используется в криптографии.

Объект и предмет исследования

- Наибольший общий делитель чисел
- Алгоритм Евклида
- Расширенный алгоритм Евклида
- Бинарный алгоритм Евклида
- Расширенный бинарный алгоритм Евклида

Цели и задачи

- Изучить алгоритмы нахождения наибольшего общего делителя
- Реализовать
  - Алгоритм Евклида
  - Расширенный алгоритм Евклида
  - Бинарный алгоритм Евклида
  - Расширенный бинарный алгоритм Евклида

Материалы и методы

- Язык программирования Python

Результаты

Тестирование алгоритмов нахождения наибольшего общего делителя

In [74]:

```
import numpy as np
for i in range(50):
    a, b = np.random.randint(1, 100), np.random.randint(1, 100)
    a, b = max(a,b), min(a,b)
    res1 = alg1(a, b)
    res2 = alg2(a, b)
    res3, a1, b1 = alg3(a, b)
    #res4, a2, b2 = alg4(a, b)
    if a*a1 + b*b1 != res3 or res2 != res1 or res1 != res2:
        print('Ошибка')
        print()
```

Рис. 1: Тестирование алгоритмов нахождения нахождения наибольшего общего делителя