Презентация по лабораторной работе №5

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

Простые числа широко применяются в криптографии с открытым ключем. Алгоритмы определения простоты числа являются составнями частями многих криптографических алгоритмов.

Объект и предмет исследования

- Вероятностные алгоритмы проверки чисел на простоту
- Тест Ферма
- Тест Соловэя-Штрассена
- Тест Миллера-Рабина

Цели и задачи

- Изучить вероятностные алгоритмы проверки чисел на простоту
- Реализовать
  - Тест Ферма
  - Тест Соловэя-Штрассена
  - Тест Миллера-Рабина

Материалы и методы

- Язык программирования Python

Результаты

Тестирование реализованных алгоритмов

```
for i in range(10):
    n = np.random.randint(4, 100)*2 + 1
    print('Ферма ', ferma(n))
    print('Соловэй-Штрассен ', s_sh(n))
    print('Миллер-Рабин ', m_r(n))
    print()
```

```
Ферма  Число 77 составное
Соловэй-Штрассен  Число 77 составное
Миллер-Рабин  Число 77 составное

Ферма  Число 105 составное
Соловэй-Штрассен  Число 105 составное
Миллер-Рабин  Число 105 составное

Ферма  Число 15 составное
Соловэй-Штрассен  Число 15 составное
Миллер-Рабин  Число 15 составное

Ферма  Число 147 составное
Соловэй-Штрассен  Число 147 составное
Миллер-Рабин  Число 147 составное

Ферма  Число 141 составное
Соловэй-Штрассен  Число 141 составное
Миллер-Рабин  Число 141 составное

Ферма  Число 89, вероятно, простое
Соловэй-Штрассен  Число 89 составное
Миллер-Рабин  Число 89 составное

Ферма  Число 139, вероятно, простое
Соловэй-Штрассен  Число 139 составное
Миллер-Рабин  Число 139 составное

Ферма  Число 183 составное
Соловэй-Штрассен  Число 183 составное
Миллер-Рабин  Число 183 составное

Ферма  Число 27 составное
Соловэй-Штрассен  Число 27 составное
Миллер-Рабин  Число 27 составное

Ферма  Число 199, вероятно, простое
Соловэй-Штрассен  Число 199 составное
Миллер-Рабин  Число 199 составное
```