

# Презентация лабораторной работы № 5.

## Вероятностные алгоритмы проверки чисел на простоту

дисциплина: Математические основы защиты информации и информационной безопасности

---

Наливайко Сергей Максимович

## Цель работы

---

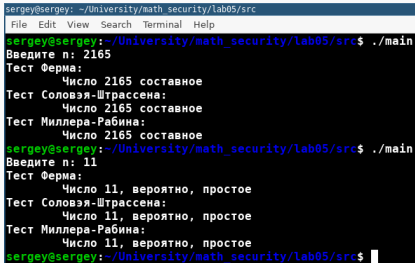
Научиться реализовывать вероятностные алгоритмы проверки чисел на простоту.

- Реализовать алгоритм, реализующий тест Ферма.
- Реализовать алгоритм вычисления числа Якоби.
- Реализовать алгоритм, реализующий тест Соловея-Штрассена.
- Реализовать алгоритм, реализующий тест Миллера-Рабина.

## Выполнение лабораторной работы

---

# Реализация вероятностных алгоритмов



```
sergey@sergey: ~/University/math_security/lab05/src
File Edit View Search Terminal Help
sergey@sergey:~/University/math_security/lab05/src$ ./main
Введите n: 2165
Тест Ферма:
    Число 2165 составное
Тест Соловья-Штрассена:
    Число 2165 составное
Тест Миллера-Рабина:
    Число 2165 составное
sergey@sergey:~/University/math_security/lab05/src$ ./main
Введите n: 11
Тест Ферма:
    Число 11, вероятно, простое
Тест Соловья-Штрассена:
    Число 11, вероятно, простое
Тест Миллера-Рабина:
    Число 11, вероятно, простое
sergey@sergey:~/University/math_security/lab05/src$
```

Figure 1: Вероятностные алгоритмы проверки чисел на простоту

## Выводы

---

В ходе лабораторной работы мы реализовывали вероятностные алгоритмы проверки чисел на простоту.