

Защита лабораторной 5

по предмету мат. основы защиты информации

Дидусь К.В.

Российский университет дружбы народов, Москва, Россия

Информация

- Диудусь Кирилл Валерьевич
- Студент кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- 1132223499@rudn.ru
- <https://github.com/kirilldi/>



Введение

Актуальность

- Изучение базовых принципов шифрования
- Важность знания основ шифрования для работы в сфере информационных технологий

Цели и задачи лабораторной

Целью данной лабораторной работы является ознакомление с алгоритмом для вероятностной проверки числа на простоту и его реализация в программном виде.

Материалы и методы

- ТУИС РУДН
- Язык программирования Python

Выполнение лабораторной

В ходе выполнения лабораторной работы было реализовано 3 вариации алгоритма для вероятностной проверки числа на простоту, использующих различные тесты.

Среди них:

- тест Ферма
- тест Соловэя-Штрассена
- тест Миллера-Рабина

Программный код представлен в качестве листинга в конце отчета.

Вывод

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомился с алгоритмом для вероятностной проверки числа на простоту, а так же мне удалось реализовать вариации этого алгоритма на языке программирования Python.