Лабораторная работа №5

Математические основы защиты информации и информационной безопасности

Мануэл Марсия Педру

2026

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Цель работы

Цель работы

Изучить шифры простой замены и научиться их реализовывать.

Выполнение лабораторной работы

#2.1 Реализация вычисления символа Якоби Символ Якоби — теоретико-числовая функция двух аргументов, введённая К. Якоби в 1837 году. Является квадратичным характером в кольце вычетов. Символ Якоби обобщает символ Лежандра на все нечётные числа, большие единицы. Символ Кронекера — Якоби, в свою очередь, обобщает символ Якоби на все целые числа, но в практических задачах символ Якоби играет гораздо более важную роль, чем символ Кронекера — Якоби.

#2.2 Реализация алгоритма, реализующего тест Ферма Тест простоты Ферма в теории чисел — это тест простоты натурального числа ?, основанный на малой теореме Ферма.

#2.3 Реализация алгоритма, реализующего тест

Соловэя-Штрассена Тест Соловея—Штрассена — вероятностный тест простоты, открытый в 1970-х годах Робертом Мартином Соловеем совместно с Фолькером Штрассеном. Тест всегда корректно определяет, что простое число является простым, но для состав- ных чисел с некоторой вероятностью он может дать неверный ответ. Основное 8 преимущество теста