Отчёт по лабораторной работе №7 Математические основы защиты информации и информационной безопасности

Дискретное логарифмирование в конечном поле

Выполнил: Мануэл Марсия Педру,
НФИмд-02-25, 1032255503

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Изучить алгоритм дискретного логарифмирования в конечном поле и научиться его реализовывать.

2 Выполнение лабораторной работы

2.1 Реализация алгоритма, реализующего P-Метод Полларда для задач дискретного логарифмирования

Дискретное логарифмирование — задача обращения функции g^x в некоторой конечной мультипликативной группе G.

Наиболее часто задачу дискретного логарифмирования рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. Эффективные алгоритмы для решения задачи дискретного логарифмирования в общем случае неизвестны.

Выполним реализацию этого алгоритма на языке python (рис. 2.1 - рис. 2.3):

Реализация алгоритма, реализующего P-Метод Полларда для задач дискретного логарифмирования

Рис. 2.1: Реализация алгоритма, реализующего P-Метод Полларда для задач дискретного логарифмирования

Реализация алгоритма, реализующего P-Метод Полларда для задач дискретного логарифмирования

Рис. 2.2: Реализация алгоритма, реализующего P-Метод Полларда для задач дискретного логарифмирования

Реализация алгоритма, реализующего P-Метод Полларда для задач дискретного логарифмирования

Рис. 2.3: Реализация алгоритма, реализующего P-Метод Полларда для задач дискретного логарифмирования

Проверим работу алгоритмов (рис. 2.4):

Проверка

Рис. 2.4: Проверка

3 Список литературы. Библиография