Задачи для лабораторных занятий по дисциплине «Методы алгебраической геометрии в криптографии» для специальности 10.05.01 «Компьютерная безопасность», 2023/2024 учебный год, IX семестр

А. В. Жаркова

1) Реализовать алгоритм генерации эллиптической кривой с

I. $j = 0$;

II. $j = 1728$.

2) I. Найти число точек эллиптической кривой с помощью алгоритма «giant step – baby step».

II. Реализовать неинтерактивный протокол аутентификации на основе доказательств с нулевым разглашением знания логарифма в группе точек эллиптической кривой.

3) Реализовать

I. адаптацию протокола цифровой подписи Шнорра на эллиптических кривых.

II. аналог генератора псевдослучайной последовательности Блюм – Блюма – Шуба на эллиптической кривой.

4) Задача реализуется письменно и программно.

I. Привести примеры протоколов Диффи – Хеллмана и Масси – Омуры для эллиптических кривых над полями $\mathbb{F}_5$, $\mathbb{F}_{13}$, $\mathbb{F}_{2^4}$.

II. Пусть E – эллиптическая кривая над полем $\mathbb{F}_{24}$, заданная уравнением $y^2 + y = x^3$. Показать, что для любой точки $P \in E$ имеет место равенство $3P = 0$. Это означает, что группа $G(E)$ имеет период 3. Сколько точек содержит группа $G(E)$? Какова ее алгебраическая структура?

5) …

…

Список источников

1) Жаркова, А. В. Методы алгебраической геометрии в криптографии : учебное пособие / А. В. Жаркова. – Москва : Издательство «Перо», 2022. – 111 с. ISBN 978-5-00204-595-2.

2) Молдовян, Н. А. Криптография: от примитивов к синтезу алгоритмов / Н. А. Молдовян. БХВ-Петербург, 2004. 448 с.

3) Молдовян, Н. А. Теоретический минимум и алгоритмы цифровой подписи / Н. А. Молдовян. СПб : БХВ-Петербург, 2010. 304 с.

4) Рябко Б. Я. Основы современной криптографии для специалистов в информационных технологиях [Текст] / Б.Я. Рябко, А.Н. Фионов. – М.: Науч. мир, 2004. – 172, [4] с. – Библиогр. – ISBN 5-89176-233-1 (в пер.).

5) Романьков В. А. Введение в криптографию. Курс лекций / В. А. Романьков. М. : ФОРУМ, 2012. - 240 с. - (Высшее образование). - ISBN 978-5-91134-573-0.

6) Ростовцев А. Г., Маховенко Е. Б. Теоретическая криптография [Текст] / А. Г. Ростовцев, Е. Б. Маховенко. СПб.: Профессионал, 2004. 465 с.

7) Смарт Н. Криптография [Текст] / Н. Смарт; пер. с англ. С.А. Кулешова; под ред. С. К. Ландо. – М.: Техносфера, 2006. – 525, [3] с.: рис., табл. – (Мир программирования). – ISBN 5-94836-043-1. – ISBN 0077099877 (англ.).