БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

БЕЛОРУССКИЙ СТАНДАРТ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Кураленко Ульяна Анатольевна

Научный руководитель:
кандидат физ.-мат. наук,
доцент Д. Н. Чергинец

2017

В дипломной работе 59 страниц, 2 таблицы, 9 источников, 11 приложений.

КРИПТОГРАФИЯ, ЭЛЛИПТИЧЕСКАЯ КРИВАЯ, ПОРЯДОК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ, ФУНКЦИЯ ХЕШИРОВАНИЯ, ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Дипломная работа посвящена изучению использования в криптографии алгебраических свойств эллиптических кривых и применению их для изучения белорусского стандарта электронной цифровой подписи.

Цель дипломной работы – изучить группу точек эллиптической кривой и белорусские стандарты электронной цифровой подписи и функции хеширования, а также объяснить математическую основу алгоритма Шуфа и реализовать изученные методы и алгоритмы в пакете Mathematica.

В дипломной работе получены следующие результаты:

1. Описаны и реализованы методы и алгоритмы для работы с группой точек эллиптической кривой;
2. Описан и реализован алгоритм Шуфа поиска порядка кривой;
3. Описаны и реализованы основные алгоритмы функции хеширования СТБ 34.101.31;
4. Описаны и реализованы основные алгоритмы электронной цифровой подписи СТБ 34.101.45.

Дипломная работа носит программно-исследовательский характер. Результаты дипломной работы могут применяться при разработке средств криптографической защиты информации.

Дипломная работа выполнена автором самостоятельно.

Thesis project is presented in the form of an explanatory note of 59 pages, 2 tables, 9 references, 11 applications.

CRYPTOGRAPHY, ELLIPTIC CURVE, ORDER OF THE ELLIPTIC CURVE, HASH FUNCTION, ELECTRONIC DIGITAL SIGNATURE

The research object is to study the use of the algebraic properties of elliptic curves in cryptography and their application to the Belarusian standard of electronic digital signature.

The purpose of the thesis project is to study the group of elliptic curve points and Belarusian standards of electronic digital signature and hash function, and also to explain the mathematical basis of the Schoof's algorithm and to implement the studied methods and algorithms via Mathematica package.

The main results of the thesis project are as follows:

1. Methods and algorithms for working with elliptic curve groups are described and implemented;
2. A Schoof's algorithm for finding the order of an elliptic curve is described and implemented;
3. The main algorithms of the hash function СТБ 34.101.31 are described and implemented;
4. The basic algorithms of the electronic digital signature СТБ 34.101.45 are described and implemented;

The thesis project is a practical one. The results of the thesis project can be applied to the development of cryptographic data protection.

The thesis project was done solely by the author.