МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к магистерской диссертации

АЛГОРИТМ ЛЕНСТРЫ РЕШЕНИЯ ЗАДАЧИ ЦЕЛОЧИСЛЕННОГО ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ И ЕГО ПРИМЕНЕНИЕ

Абдулганеева Татьяна Юрьевна

руководитель Чергинец Дмитрий Николаевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

В магистерской диссертации 57 страниц, 3 рисунка, 15 источников, одно приложение.

ЭЛЛИПСОИДЫ, ОКРУГЛЕНИЕ ПОЛИТОПОВ, АЛГОРИТМ ОТСЕЧЕНИЙ, РЕШЕТКИ, АЛГОРИТМ ЛЕНСТРЫ ЦЕЛОЧИСЛЕННОГО ПРОГРАММИРОВАНИЯ, РЮКЗАЧНЫЕ СИСТЕМЫ, КРИПТОСИСТЕМА МЕРКЕЛЯ-ХЕЛЛМАНА, БЫСТРОРАСТУЩАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, АТАКА ШАМИРА.

В магистерской диссертации рассмотрен алгоритм атаки Шамира, который в первой своей части использует алгоритм Ленстры целочисленного программирования.

Цель работы – изучить и реализовать атаку Шамира на рюкзачную криптосистему Меркеля-Хеллмана.

В магистерской диссертации получены следующие результаты:

1) Реализованы алгоритм поиска эллипсоида наименьшего объема для заданного отсекающего полупространств, алгоритм округления политопов;
2) Изучен алгоритм Ленстры для целочисленного решения неравенств;
3) Проведен криптоанализ шифра Меркля-Хеллмана при помощи алгоритма Шамира.

Магистерская диссертация написана на основе исследования работ различных зарубежных и отечественных авторов. Практическая часть работы реализована в пакете Wolfram Mathematica.

Работа выполнена автором самостоятельно.

Thesis project is presented in the form of an explanatory note of 57 pages, 15 references, 3 pictures.

ELLIPSOIDS, CIRCLE OF POLYTOPS, TRIMMING ALGORITHM, LATTICES, LENSTRA' S INTEGER PROGRAMMING ALGORITHM, KNAPSACK INSTANCE, MERKEL-HELLMAN CRYPTOSYSTEM, QUICK-GROWING SEQUENCE, ATTACK OF THE SHAMIR.

In the thesis project the algorithm of attack of the Shamir that use Lenstra' s integer programming algorithm is considered.

The work purpose – to study and realize attack of the Shamir on the Merkel-Hellman knapsack instance.

The main results of the thesis projects are as follows:

1. The algorithm for finding the smallest volume ellipsoid for a given cutting half-space, the rounding algorithm of polytopes are implemented;
2. The Lenstra algorithm for the integer solution of inequalities is studied and implemented;
3. Cryptanalysis of the Merkle-Hellman system using the Shamir algorithm.

The thesis project is written on the basis of complex research of works of foreign and Russian authors. The practical basis of research consists in realization algorithms in the Wolfram Mathematica package.

The thesis project was done solely by the author.