МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

АБДУЛГАНЕЕВА

Татьяна Юрьевна

ПРИМЕНЕНИЕ ЦЕЛОЧИСЛЕННОГО ПРОГРАММИРОВАНИЯ В КРИПТОГРАФИИ

Аннотация к дипломной работе

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

Минск, 2017

В дипломной работе 34 страниц, 3 рисунка, 7 источников.

ЦЕЛОЧИСЛЕННОЕ ПРОГРАММИРОВАНИЕ, РЕШЕТКИ, АЛГОРИТМ ЛЕНСТРЫ ЦЕЛОЧИСЛЕННОГО ПРОГРАММИРОВАНИЯ, РЮКЗАЧНЫЕ СИСТЕМЫ, КРИПТОСИСТЕМА МЕРКЕЛЯ-ХЕЛЛМАНА, СУПЕРВОЗРАСТАЮЩАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, АТАКА ШАМИРА.

В дипломной работе 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 дипломной работе получены следующие результаты:

1) Изучен и реализован алгоритм Ленстры для целочисленного решения неравенств;
2) Проведен криптоанализ шифра Меркля-Хеллмана при помощи алгоритма Шамира;
3) Реализованы другие атаки на рюкзачную криптосистему Меркля-Хеллмана.

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

Дипломная работа выполнена автором самостоятельно.

У дыпломнай працы 35 старонак, 3 малюнка, 7 крыніц.

ЦЭЛАЛІКАЕ ВЫХ ПРАГРАМАВАННЕ, РАШОТКІ, АЛГАРЫТМ ЛЕНСТРЫ ЦЭЛАЛІКАВАГА ПРАГРАМАВАННЯ, РЮКЗАЧНЫЕ СІСТЭМЫ, КРЫПТАСІСТЭМЫ МЕРКЕЛЬ-ХЕЛЛМАНА, СУПЕРВОЗРАСТАЮЩАЯ ПАСЛЯДОЎНАСЦЬ, АТАКА ШАМІРА.

У дыпломнай працы разгледжаны алгарытм атакі Шаміра, які ў першай сваёй частцы выкарыстоўвае алгарытм Ленстры цэлалікавага праграмавання.

Мэта работы - вывучыць і рэалізаваць атаку Шаміра на рюкзачную криптосистему Меркеля-Хеллмана.

У дыпломнай працы атрыманы наступныя вынікі:

1) Вывучаны і рэалізаваны алгарытм Ленстры для цэлалікавага рашэння сістэм;

2) Праведзены криптоанализ шыфра Меркеля -Хеллмана пры дапамозе алгарытму Шаміра;

3) Рэалізаваны іншыя атакі на рюкзачную криптосистему Меркеля-Хеллмана.

Дыпломная праца напісана на аснове даследавання работ розных замежных і айчынных аўтараў. Практычная частка працы рэалізавана ў пакеце Wolfram Mathematica.

Дыпломная праца выканана аўтарам самастойна.

Thesis project is presented in the form of an explanatory note of 35 pages, 7 references, 3 pictures.

INTEGRATED PROGRAMMING, LATTICE, LENSTRA' S INTEGER PROGRAMMING ALGORITHM, KNAPSACK INSTANCE, MERKLE-HELLMAN CRYPTOSYSTEM, SUPER-INCREASING 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 Lenstra algorithm for the integer solution of inequalities is studied and implemented;
2. Cryptanalysis of the Merkle-Hellman system using the Shamir algorithm;
3. Other attacks on the backpack cryptosystem of the Merkle-Hellman.

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.