БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

РЮКЗАЧНЫЕ КРИПТОСИСТЕМЫ

Завьялова Мария Александровна

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

2016

РЕФЕРАТ

В дипломной работе 39 страниц, 10 рисунков, 15 источников, 5 приложений.

Ключевые слова: КРИПТОСИСТЕМА МЕРКЛА-ХЕЛЛМАНА, LLL-АТАКА, АТАКА ШАМИРА, АТАКА САЛОМАА, СЛОЖНОСТЬ АЛГОРИТМОВ, NP-ПОЛНОТА.

Объект исследования данной дипломной работы – это криптосистема Мекла-Хеллмана и ее криптостойкость. Целью исследования было изучение и формализация наиболее распространенных атак, оценка их сложности, экспериментальная проверка их работы. При работе с теоретическим материалом основными методами исследования являлись анализ, обобщение и формализация. В практической части были проведены несколько экспериментов и наблюдений, было сделано сравнение их результатов.

Актуальность проведения изысканий в данной области тесно связана с поиском возможных полиномиальных алгоритмов решения задачи о рюкзаке с инъективным вектором, доказательством существования односторонних функций с лазейкой, применением современных методик в области нейронных сетей и целочисленного программирования для совершенствования существующих атак, в частности, первой части атаки Шамира.

Результатами данной работы являются формализованные алгоритмы LLL-атаки, второй части атаки Шамира и атаки Саломаа, их реализация в пакете Mathematica, сравнительный анализ их производительности, экспериментальное подтверждение уязвимости криптосистемы Меркла-Хеллмана.

Дипломная работа носит практический характер и может быть использована в дальнейших исследованиях данной криптосистемы.

Дипломная работа выполнена автором совместно с руководителем.

ABSTRACT

There are 39 pages, 10 images, 15 sources, 5 applications in the thesis work.

Key Words: MERKLE-HELLMAN CRYPTOSYSTEM, LLL-ATTACK, SHAMOR ATTACK, SALOMAA ATTACK, COMPLEXITY OF ALGORITHMS, NP-COMPLETENESS.

The object of study in the thesis work is Merkle-Hellman cryptosystem and its cryptographical strongness. The purpose of research was to study the most common attacks, perform their formalization, estimate their complexity, experimentally verify their work. The main methods of research with theoretical materials were analysis, generalization and formalization. In the practice several experiments were held and some observations were deduced. On this basis the comparison of their results was also made.

The relevance of the research in this area is closely linked to the search for possible polynomial algorithms for solving the knapsack problem with the infective vector, proof of the existence of one-way functions with trapdoor, the use of modern techniques in the field of neural networks and integer programming to improve existing attacks, in particular, the first part of Shamir attack.

The results of this thesis work are formalized LLL-attack algorithm, the second part of the Shamir attack and the Salomaa attack, their implementation in Mathematica package, the comparative analysis of their performance, confirmation of the vulnerability of Merkle-Hellman cryptosystem by the experiment.

The thesis work is practical. Its results can be used in further studies of this cryptosystem.

The thesis work is performed by the author together with the supervisor.