БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к магистерской диссертации

«АТАКИ НА КРИПТОСИСТЕМУ RSA ПРИ ПОМОЩИ LLL-АЛГОРИТМА»

КАТЛИНСКИЙ Илья Геннадьевич

Научный руководитель:
кандидат физико-математических наук,
доцент Чергинец Дмитрий Николаевич

Минск, 2015

КРИПТОСИСТЕМА, RSA, ПРОСТОЕ ЧИСЛО, ФАКТОРИЗАЦИЯ, КРИПТОАНАЛИЗ, ТЕОРЕМА КОППЕРСМИТА, LLL-АЛГОРИТМ, АТАКА ВИНЕРА, ЗАДАЧА О МАЛОМ ОБРАТНОМ, ОБОБЩЕННАЯ АТАКА ВИНЕРА, ОПТИМИЗАЦИЯ ОБОБЩЕННОЙ АТАКИ ВИНЕРА

Диссертация представлена в виде пояснительной записки объемом 69 страниц, содержит 1 изображение, 8 источников, 4 приложения.

Цель работы: изучение LLL-алгоритма, рассмотрение примеров использования LLL-алгоритма для атак на шифр RSA, анализ обобщенной атаки Винера, оптимизация этой атаки и ее теоретическое обоснование. Реализация основных алгоритмов атак на шифра RSA при помощи LLL-алгоритма.

Данная диссертация является обобщением основных знаний и подходов, связанных с атаками на шифр RSA с использованием LLL-алгоритма, работа также включает в себя реализацию основных алгоритмов, описанных в данной работе, в среде «Mathematica». Основное направление работы - исследование обобщенной атаки Винера. Новизна работы заключается в проведении оптимизации обобщенной атаки, формулировке и доказательстве теорем, дающих теоретическое обоснование корректности предложенной оптимизации. Формулируется и доказывается теорема о количестве операций алгоритма обобщенной атаки.

Во введении содержится информация о криптосистеме RSA, ее актуальности, об LLL-алгоритме и обобщенной атаке Винера. А также выполняется постановка задачи.

В главе 1 «Криптосистема RSA» рассмотрены основные алгоритмы шифра RSA и подходы к криптоанализу шифра RSA.

В главе 2 «Введение в LLL-алгоритм» рассмотрен алгоритм ортогонализации Грамма-Шмидта, LLL-алгоритм, теоремы о базисе и приведенном базисе. Также рассмотрена теорема Копперсмита и алгоритм Копперсмита для одномерного случая.

В главе 3 «Атаки на RSA» рассмотрены примеры атак на шифр RSA, использующие LLL-алгоритм и теорему Копперсмита. Кроме того внимание уделяется атаке Винера.

В главе 4 «Обобщение атаки Винера» рассматривается задача о малом обратном, обобщенная атака Винера.

В главе 5 «Оптимизация параметров обобщенной атаки Винера» особое внимание уделено оптимизации обобщенной атаки Винера, а также теоретическому обоснованию корректности предложенной оптимизации. Делается сравнение с атакой Винера, приводится подробный пример обобщенной атаки и пример вычисления оптимальных параметров атаки.

CRYPTOSYSTEMS, RSA, PRIME NUMBER, FACTORIZATION, CRYPTO-ANALYSIS, COPPERSMITH THEOREM, LLL-ALGORITHM, WIENER ATTACK, SMALL INVERSE PROBLEM, GENERALIZED WIENER ATTACK, OPTIMIZATION OF GENERALIZED WIENER ATTACK

The dissertation is presented in the form of an explanatory note of 69 pages, contains 1 image, 8 references, 4 applications.

Purpose: study LLL-algorithm, review usage of LLL-algorithm for attacks on RSA cipher, analysis of Wiener generalized attack, optimization of this attack and its theoretical justification. The implementation of the basic algorithms of attacks on RSA cryptosystem using LLL-algorithm.

This dissertation is a generalization of the basic knowledge and approaches related to the attacks on the RSA cipher using LLL-algorithm, the work also includes implementation of basic algorithms described in this paper in « Mathematisca ». The focus of work is to research generalized Wiener attack. The novelty of dissertation is optimization of generalized attack, formulation and proving of theorems giving theoretical justification for the correctness of the proposed optimization. Formulation and proving of a theorem about number of operations in generalized Wiener attack is also included.

Introduction contains information about RSA cryptosystem, its relevance, also it contains information about the LLL-algorithm and the generalized Wiener attack, as well as the formulation of the problem.

Chapter 1 «RSA cryptosystem» contains basic RSA encryption algorithms and approaches for cipher cryptanalysis of RSA.

Chapter 2 «Introduction in LLL-algorithm» contains algorithm of Gram-Schmidt orthogonalization, LLL-algorithm, theorems about the basis and a reduced basis. Also Coppersmith theorem and Coppersmith algorithm for one-dimensional case are described.

Chapter 3 «Attacks on RSA» contains examples of attacks on RSA cipher using LLL-algorithm and Coppersmith's theorem. Also attention is paid to the Wiener attack.

Chapter 4 «Generalized Wiener attack» contains description of small inverse problem and generalized Wiener attack.

In Chapter 5 «Optimization of Generalized Wiener Attack» particular attention is paid to the optimization of generalized Wiener attack, as well as the theoretical justification of the correctness of supplied optimization. Also comparison with the Wiener attack included in this chapter together with detailed example of generalized Wiener attack and example of optimal parameters search.