БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

Анализ криптосистемы RSA

Катлинский Илья Геннадьевич

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

2014

Дипломный проект представлен в виде пояснительной записки объемом 61 страница, содержит 4 таблицы, 9 источников, 5 приложений.

Ключевые слова: КРИПТОСИСТЕМА, RSA, ПРОСТОЕ ЧИСЛО, ФАКТОРИЗАЦИЯ, КРИПТОАНАЛИЗ, ТЕСТ НА ПРОСТОТУ, ТЕОРЕМА КОППЕРСМИТА, ШИФР, КРИПТОАТАКА

Цель работы: изучение алгоритмов построения и поиска больших простых чисел, алгоритмов факторизации и анализ шифра RSA.

Дипломный проект является обобщением основных знаний и математических методов, связанных с криптосистемой RSA, работа также включает в себя реализацию основных алгоритмов, описанных в данной работе, в среде “Mathematica”.

Во введении содержится информации о криптосистемах с открытым ключом, даются основные определения, осуществляется введение в криптосистему RSA, выполняется постановка задачи.

В главе 1 “Построение простых чисел” рассмотрена проблема построения простых чисел, описаны алгоритмы, позволяющие строить простые числа, кроме того уделено внимание тестам чисел на простоту. В рамках главы реализованы алгоритмы Миллера-Рабина и Диемитко.

В главе 2 “Проблема факторизации целых чисел” описаны основные подходы к факторизации чисел, рассмотрены и разобраны основные алгоритмы факторизации и примеры их работы, указаны скорости работы этих алгоритмов, проведено сравнение алгоритмов. В рамках главы реализованы некоторые из рассмотренных алгоритмов факторизации.

В главе 3 “Криптосистема RSA” рассмотрены основные алгоритмы криптосистемы RSA - создание ключей, шифрование и дешифрование, описаны

основные подходы к криптоанализу RSA. Рассмотрены LLL-алгоритм, а также теорема Копперсмита, используемые при факторизации чисел при известной их аппроксимации, описаны алгоритмы, использующие теорему Копперсмита для факторизации чисел. В рамках главы реализованы криптоатаки на шифр RSA, LLL-алгоритм, теорема Копперсмита, примеры атак с использование теоремы Копперсмита.

The thesis project is presented in the form of an explanatory note of 61 pages, contains 4 tables, 9 references, 5 applications.

Key words: CRYPTOSYSTEMS, RSA, PRIME NUMBER, FACTORIZATION, CRYPTOANALYSIS, SIMPLICITY TEST, COPPERSMITH THEOREM, CIPHER, CRYPTOATTACK

Goal: study of algorithms for constructing and searching large primes, factorization algorithms and analysis RSA cipher.

The thesis of project is a generalization of the basic knowledge and mathematical methods associated with the cryptosystem RSA, work also includes an implementation of the basic algorithms described in this paper, in the application “Mathematica”.

The introduction contains information about public-key cryptosystems, the basic definitions related to the project theme, provides an introduction to the cryptosystem RSA, as well as the formulation of the problem.

In Chapter 1 “Building primes” the problem of constructing primes and algorithms to build primes described, also attention paid to Primality. Within chapter Miller-Rabin and Diemitko algorithms were implemented.

In Chapter 2 “The Factorization Problem” primes basic approaches to the factorization properties were described, the main factorization algorithms and examples of their work were examined and dismantled, the comparison algorithms was made. Under chapter some of the considered factorization algorithms were implemented.

In Chapter 3 “Cryptosystem RSA” the basic algorithms cryptosystem RSA was described - key generation, encryption and decryption, the main approaches to cryptanalysis RSA. LLL-algorithm was discussed, as well as Coppersmith theorem which is used in the factorization of numbers in approximation algorithms. Under

Chapter attacks on cipher RSA, LLL-algorithm theorem Coppersmith, examples of attacks using Coppersmith's theorem implemented.