МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Сравнительный анализ схемы шифрования NTRU с другими системами шифрования с открытым ключом

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Елистратова Георгия Дмитриевича

Научный руководитель
д.ф.-м.н., профессор _____ В. А. Молчанов
22.01.2022 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2022 г.

Саратов 2022

ВВЕДЕНИЕ

В настоящее время очень много организаций работают с большими базами данных через общедоступную сеть. Безопасность информации — важный вопрос, ответить на который сегодня пытается ассиметричная криптография.

В виду растущей информатизации общества и повышения ценности информации сегодня и в ближайшем будущем криптография становится тем, с чем сталкивается каждый. Это особенно актуально для криптографических систем с открытым ключом, которые в настоящее время широко применяются в различных сетевых протоколах, электронных подписях и системах электронных платежей.

NTRUEncrypt – это криптографическая система с открытым ключом, изначально называвшаяся NTRU, была изобретена в 1996 году. В отличие от своих именитых предшественников таких как RSA или El-Gamal, NTRU работает не над кольцом вычетов по модулю целого числа N, а над кольцом многочленов степени $n-1$, приведенных по модулю x^n-1. Исследования криптосистемы NTRU говорят о преимуществе ее использования по сравнению с наиболее популярными на сегодня криптосистемами с открытым ключом, что является поводом рассмотреть ее подробнее.

Еще одной причиной обратить внимание на криптосистему NTRU стали результаты исследований Питера Шора о существовании полиномиальных алгоритмов решения задач дискретного логарифмирования и разложения числа на множители на так называемых квантовых вычислителях. Кроме того, теоретически доказано, что с помощью алгоритма Шора дискретный логарифм можно вычислить за полиномиальное время. Квантовая модель вычислений является вполне реальной, хотя споры о возможности создания квантового компьютера не утихают.

Цель работы – провести сравнительный анализ основных параметров следующих известных криптосистем с открытым ключом: RSA, криптосистема Эль-Гамаля над группой точек эллиптической кривой и NTRUEncrypt.

Решаемые задачи:

1) рассмотреть теоретико-числовые задачи, на основе которых строятся известные криптосистемы с открытым ключом;

2) изучить алгоритмы построения известных криптосистем с открытым ключом;

3) разработать программный комплекс на языке программирования Java для реализации и сравнительного анализа рассматриваемых криптосистем;

4) провести оценку производительности алгоритмов на основе сравнения времени выполнения следующих операций: генерация ключей, шифрование и дешифрование.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и приложения. Общий объем работы – 100 страниц, из них 61 страница – основное содержание, включая 20 рисунков и 15 таблиц, список использованных источников из 26 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе дипломной работы рассматриваются элементы теории чисел, теории групп и теории колец. Данный раздел содержит 4 подраздела. В первом подразделе рассматривается понятие и свойства делимости целых чисел, алгоритмы Евклида, а также функция Эйлера. Второй подраздел посвящен основам теории групп. Третий подраздел содержит основы теории колец. В четвертом подразделе описывается кольцо многочленов, его операции и свойства этих операций.

Второй раздел посвящен криптосистемам с открытым ключом. Этот раздел содержит шесть подразделов. Первый подраздел описывает задачу факторизации целых чисел, на которой базируется алгоритм RSA. Второй подраздел содержит информацию о криптосистеме RSA, в нем рассматриваются основные операции криптосистемы такие как: генерация ключа, шифрование и дешифрование. В третьем подразделе рассматриваются основные понятия алгебраической геометрии, необходимые для понимания алгоритмов, использующих эллиптические кривые. В четвертом подразделе описывается задача дискретного логарифмирования на эллиптической кривой, а также сравниваются криптосистемы над простым конечным полем и криптосистемы на эллиптической кривой над конечным полем. Пятый подраздел посвящен криптосистеме Эль-Гамаля над группой точек эллиптической кривой (ECC). Шестой раздел содержит информацию о криптосистеме NTRU. В нем описываются параметры криптосистемы и рекомендации к их выбору, рассматриваются основные операции: генерация ключа, шифрование и дешифрование, а также описаны некоторые методы улучшения работоспособности алгоритма. Кроме того, шестой подраздел описывает одну из модификаций алгоритма NTRU, включенную в стандарт P1363A.

В третьем разделе дипломной работы рассматривается программная реализация криптосистем с открытым ключом. Программный комплекс разработан на языке Java для реализации и сравнительного анализа криптосистем с открытым ключом (RSA, ECC, NTRU). Для создания графического интерфейса применяется платформа JavaFX. Проект собран с помощью фреймворка Maven. Так же использована библиотека GSON для работы с json объектами и библиотека Bouncy Castle для использования некоторых криптографических функций. Среда разработки – IntelliJ IDEA.

Функционально программа проста. Пользователь может выбирать алгоритм и размер ключа при работе с ним, создавать новые ключи или загружать уже существующие, набрать свое сообщение, зашифровывать его в файл, а также расшифровывать получившиеся файлы в текстовые сообщения. В центре окна находится информационная строка, которая будет сообщать пользователю о результатах его действий. Кроме того, там выводится время выполнения операций шифрования, дешифрования и генерации ключей. Третий раздел дипломной работы содержит примеры и подробно объясняет, как пользоваться указанными функциями программного комплекса.

Рассмотренные алгоритмы работают с ключами разной длины и имеют к ним различные требования, поэтому выбор пользователя ограничен списком параметров в соответствии с выбранной им криптосистемой. Список параметров приведен в таблице 1.

Таблица 1 – доступные пользователю алгоритмы и размеры ключей

RSA длина ключа	ECC эл. кривая и длина ключа	NTRU набор параметров и длина ключа
1024 бит	secp128r1, 128 бит	ees401ep1, 401 бит
2048 бит	secp192r1, 192 бит	ees449ep1, 449 бит
3072 бит	secp224r1, 224 бит	ees677ep1, 677 бит
7680 бит	secp256r1, 256 бит	ees1087ep1, 1087 бит
15360 бит	secp384r1, 384 бит	
	secp521r1, 512 бит	

В четвертом разделе приводится сравнительный анализ криптосистем с открытым ключом. Входящими данными являются два текстовых файла. Первый небольшого размера 1059 байт, абзац текста. Размер второго больше, примерно 20 Кбайт. Приводятся таблицы с экспериментально полученными данными и графики зависимости времени выполнения операций: генерации ключа, шифрования и дешифрования, от длины ключа для различных криптосистем, объясняется разница в результатах.

Для упрощения сравнения стойкости различных алгоритмов стандартом X9.98 введены 4 обширных уровня защищенности: «112 бит», «128 бит», «192 бита», «256 бит». Данные уровни стойкости отображают минимальную сложность атаки «грубая сила» – от 2^{112} до 2^{256} операций. Для различных алгоритмов с каждым из этих уровней связаны соответствующая минимальная длина ключа и размеры параметров. Таблица 2 показывает соотношение между длиной ключа и уровнем защищенности. Таким образом, сравнение криптосистем по классам стойкости является более убедительным.

Таблица 2 – Соответствие длины ключа (в битах) алгоритмов RSA, ECC и NTRU с эквивалентным классом защищенности

	Длина ключа (бит)		
Класс защищенности	RSA	ECC	NTRU
112 бит	2048	224	401
128 бит	3072	256	449
192 бит	7860	384	677
256 бит	15360	521	1087

В результате работы представлен анализ схем шифрования. Для этого построены графики зависимости времени выполнения операций шифрования, дешифрования и генерации ключа от уровня защищенности.

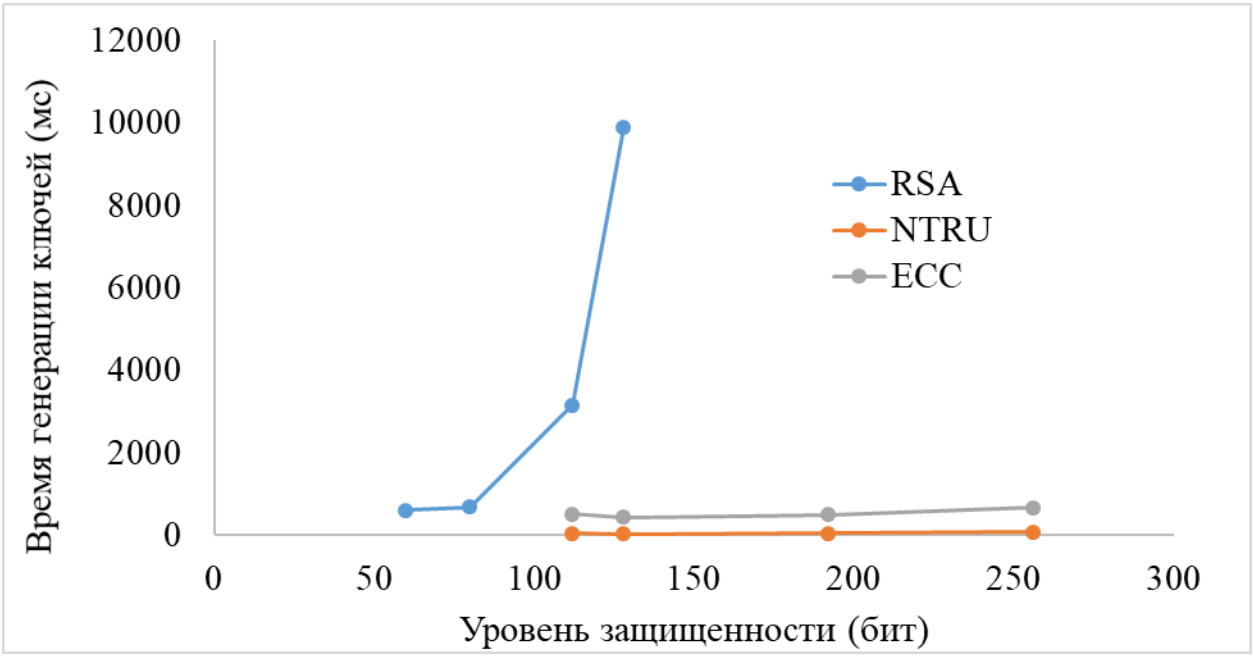

Рисунок 1 – График зависимости времени генерации ключей (в мс) от уровня защищенности алгоритмов RSA, ECC и NTRU

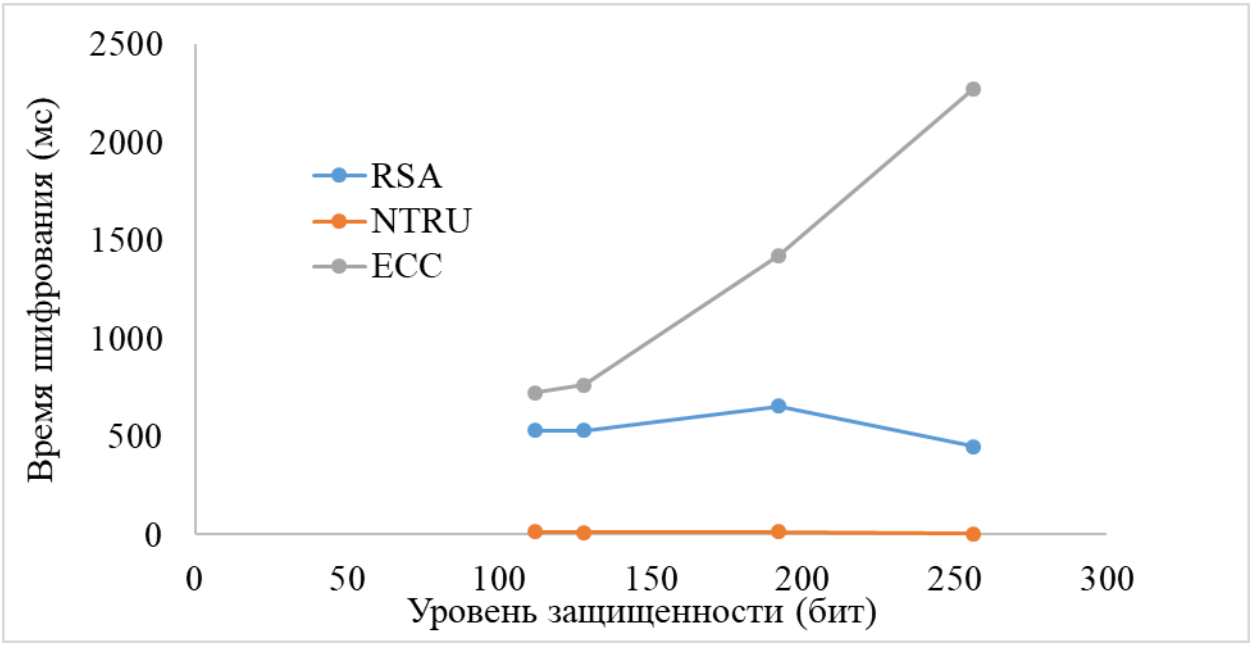

Рисунок 2 – График зависимости времени шифрования (в мс) от уровня защищенности алгоритмов RSA, ECC и NTRU

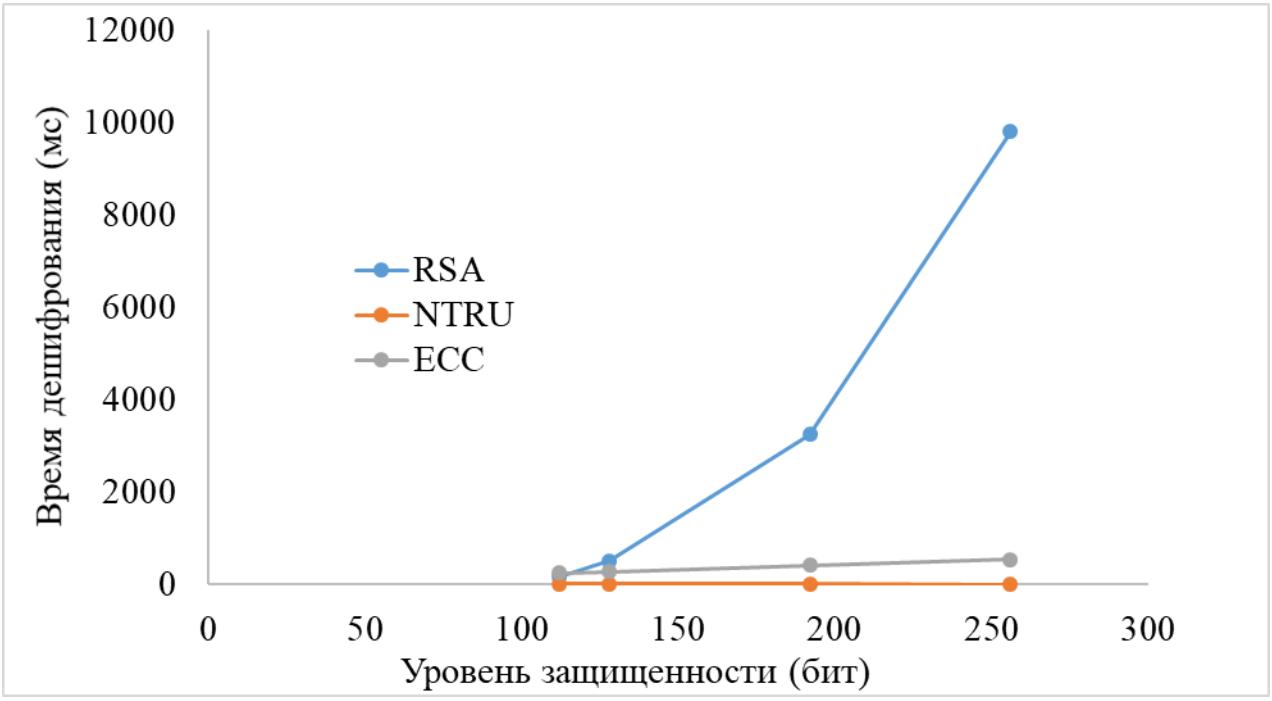

Рисунок 3 – График зависимости времени дешифрования (в мс) от уровня защищенности алгоритмов RSA, ECC и NTRU

Наихудшим образом, с учетом всех операций, проявила себя система RSA. Сложность проблемы факторизации целых чисел, на которой основан алгоритм RSA, является субэкспоненциальной. Алгоритмы ECC и NTRU основаны на экспоненциальных проблемах, благодаря этому они могут предложить аналогичный уровень безопасности, но с использованием ключей меньшей длины.

Необходимость использовать ключи большей длины для поддержания соответствующего уровня защищенности не позволяет RSA конкурировать с криптосистемами ECC и NTRU. Сравнивая NTRU с алгоритмом на базе эллиптических кривых, NTRU при сохранении высокого уровня стойкости решает проблему низкой скорости шифрования. На рисунках 1-3 хорошо видно, что криптосистема NTRU имеет преимущество перед остальными криптосистемами по всем показателям.

Из полученных результатов эксперимента можно четко заключить, что производительность NTRU лучше RSA и ECC по показателям генерации ключей, шифрованию и дешифрованию для тех же уровней безопасности.

ЗАКЛЮЧЕНИЕ

В ходе работы изучены алгоритмы известных криптосистем с открытым ключом, такие как: RSA, схема Эль-Гамаля над группой точек эллиптической кривой и NTRUEncrypt, а также рассмотрены теоретико-числовые задачи, на основе которых строятся рассматриваемые криптосистемы с открытым ключом;

В практической части работы разработан программный комплекс на языке Java для реализации и сравнительного анализа рассматриваемых криптосистем. Программный комплекс представлен в виде оконного приложения для MS-Windows и выполнен на платформе JavaFX что значительно упрощает его использование. Программный комплекс позволяет производить оценку производительности алгоритмов на основе сравнения времени выполнения следующих операций: генерации ключей, шифрования и расшифрования.

Поставленные задачи полностью решены.

Программный комплекс может применяться в учебных целях, а также в прикладных задачах, связанных с разработкой и анализом криптосистем с открытым ключом.