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

Анализ алгоритмов факторизации целых чисел и их применение в криптографии

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Змеевой Вероники Александровны

Научный руководитель
д. ф.-м. н., профессор _____ В. А. Молчанов
19.01.2026 г.

Заведующий кафедрой
д. ф.-м. н., профессор _____ М. Б. Абросимов
19.01.2026 г.

Саратов 2026

ВВЕДЕНИЕ

Безопасность современных криптографических систем в значительной степени зависит от вычислительной сложности математических задач. Одной из таких задач является факторизация, которая представляет собой процесс разложения большого числа на простые множители. Шифрсистема RSA, один из самых популярных алгоритмов шифрования с открытым ключом, опирается на сложность целочисленной факторизации для обеспечения своей надежности.

На протяжении длительного времени разрабатывались различные методы и техники для взлома RSA и других шифрсистем, основанных на целочисленной факторизации. К ним относятся как классические алгоритмы, такие как методы Полларда и квадратичное решето, так и более современные подходы, такие как решето числового поля и атака Винера на основе цепных дробей. Эти методы могут быть использованы для преодоления шифрования и нарушения безопасности системы.

Актуальность данной темы обусловлена быстрым развитием вычислительных технологий и методов криптоанализа. Несмотря на то, что RSA считается надёжным при правильной реализации и достаточной длине модуля, уязвимости могут возникнуть из-за ошибок в генерации ключей, атак по побочным каналам или математических недостатков, таких как малые показатели степени или близкие простые множители. С каждым годом вычислительная мощность техники увеличивается, что позволяет взломать всё более сложные шифры и находить большие простые числа за короткий промежуток времени.

Целью данной дипломной работы является разработка интерактивной образовательной платформы для наглядной визуализации в учебных и исследовательских целях алгоритмов факторизации чисел и атак на криптосистему RSA.

Уникальность данной работы заключается в том, что она объединяет теоретический криптоанализ с практическими инструментами, что позволяет

провести сравнительный анализ эффективности различных методов факторизации, с особым вниманием к атаке Винера, через практические демонстрации.

В отличие от предыдущих исследований, которые фокусировались только на алгоритмической сложности или теории атак, данный проект объединяет оба аспекта в доступном веб-приложении. Пользователи смогут экспериментировать с генерацией ключей, факторизацией и моделированием атак, написанием собственного кода.

Дипломная работа сочетает в себе теоретические аспекты и практические инструменты, способствует более глубокому пониманию криптографических уязвимостей и предлагает эффективные методы обеспечения безопасности в будущем.

Задачи дипломной работы включают в себя:

- Рассмотреть математические основы факторизации, включающие роль простых чисел в RSA и классы сложности факторизации;
- Ознакомиться с классическими и современными методами факторизации, включая алгоритмы $\rho-$ и $(p-1)$ Полларда, квадратичное решето и решето числовых полей, а также факторизацию по эллиптической кривой;
- Исследовать атаки Винера и Дюжелла на RSA;
- Провести сравнительный анализ практической эффективности алгоритмов факторизации, атак со слабыми ключами RSA, используя оценки временной сложности;

Создать веб-платформу, которая будет включать в себя теоретическую и практическую части для образовательных целей.

Дипломная работа состоит из введения, 2 разделов, заключения, списка использованных источников и 7 приложений. Общий объем работы – 108 страниц, из них 75 страниц – основное содержание, включая 45 рисунков и 1 таблицу, список использованных источников из 27 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе «Алгоритмы факторизации и их криптографические приложения» представлены основные теоретические сведения об алгоритмах факторизации целых чисел и их сложности. Также описаны атаки на шифрсистему RSA на основе цепных дробей.

В подразделе 1.1 «Сложность задачи факторизации» приводятся различные классы алгоритмов факторизации и их вычислительные сложности.

В подразделе 1.2 «Алгоритмы факторизации целых чисел» описываются основы факторизации целых чисел.

В подразделе 1.2.1 «Алгоритм факторизации Ферма» приводятся формулы, на которых основан механизм факторизации Ферма.

В подразделе 1.2.2 «Алгоритм факторизации ρ-метода Полларда» описываются алгоритм вычисления целозначного квадратного корня, теорема о парадоксе дней рождений и алгоритм ρ-метода Полларда с обоснованием.

В подразделе 1.2.3 «Алгоритм факторизации $(p-1)$-метода Полларда» приводится алгоритм $(p-1)$-метода Полларда с обоснованием и опредлением B-гладких чисел.

В подразделе 1.2.4 «Алгоритм Бриллхарта-Моррисона – метод цепных дробей» рассматриваются алгоритм Диксона и его модификация на основе цепных дробей – алгоритм Бриллхарта-Моррисона.

В подразделе 1.2.5 «Алгоритм факторизации на основе метода квадратичного решета» описывается алгоритм факторизации на основе метода квадратичного решета.

В подразделе 1.3 «Атаки на RSA, основанные на факторизации» приводятся различные способы взлома ключей RSA на основе методов квадратичного решета, цепных дробей и методе эллиптических кривых.

В подразделе 1.3.1 «Атаки на RSA с использованием цепных дробей» содержит описание атак, с помощью цепных дробей.

В подразделе 1.3.1.1 «Определения теории цепных дробей» приводятся основные и фундаментальные определения теории цепных дробей: конечная цепная дробь, разложение в цепную дробь и подходящие дроби.

В подразделе 1.3.1.2 «Атака Винера» описаны условия и пример атаки Винера для уязвимых ключей системы RSA.

В подразделе 1.3.1.3 «Модификации атаки Винера» приведены новые формулы для улучшения атаки Винера от Верхула и ван Тилборга, Дюжелла с новыми оценками для размера ключей.

Во втором разделе работы «Разработка интерактивной платформы для анализа факторизации и RSA» приводится программная реализация алгоритмов Ферма, ρ-Полларда, $p-1$-Полларда и Бриллхарта-Моррисона и квадратичного решета. В данном разделе демонстрируется интерфейс платформы и пример работы интерактивных разделов. Кроме того, здесь проведен анализ алгоритмов факторизации.

В подразделе 2.1 «Описание технологического стека платформы» рассматриваются инструменты, использованные при создании платформы. Платформа реализована, как клиентское приложение, основной язык – TypeScript, основной фреймворк – React и сборщик Vite. Для реализации криптографических алгоритмов и вычислительно сложных операций факторизации был выбран язык Python с технологией Pyodide для запуска интерпретатора Python прямо в браузере.

В подразделе 2.2 «Реализация алгоритмов факторизации» с подразделами 2.2.1-2.2.5 подробно описываются функции на языке Python для алгоритмов факторизации и решения для оптимизации каждого кода.

В подразделе 2.3 «Сравнение алгоритмов факторизации» анализируются алгоритмы факторизации с разными характеристиками.

Алгоритм QS показывает самую высокую общую успешность (43.8%), что подтверждает его универсальность. Столбчатые диаграммы показывают, что в диапазоне 64-128 бит Ферма, ρ-Поллард, $p-1$-Поллард и CFRAC имеют сопоставимое или лучшее время выполнения по сравнению с QS. О Однако по

мере увеличения битовой длины (128-192 бит и 192-256 бит) производительность алгоритмов Ферма, ρ-Полларда, $p-1$-Полларда резко ухудшается (среднее время увеличивается на несколько порядков), в то время как QS сохраняют свою относительную эффективность. Итоговый график, показывающий результаты сравнения в виде сводных метрик представлен на рисунке ниже.

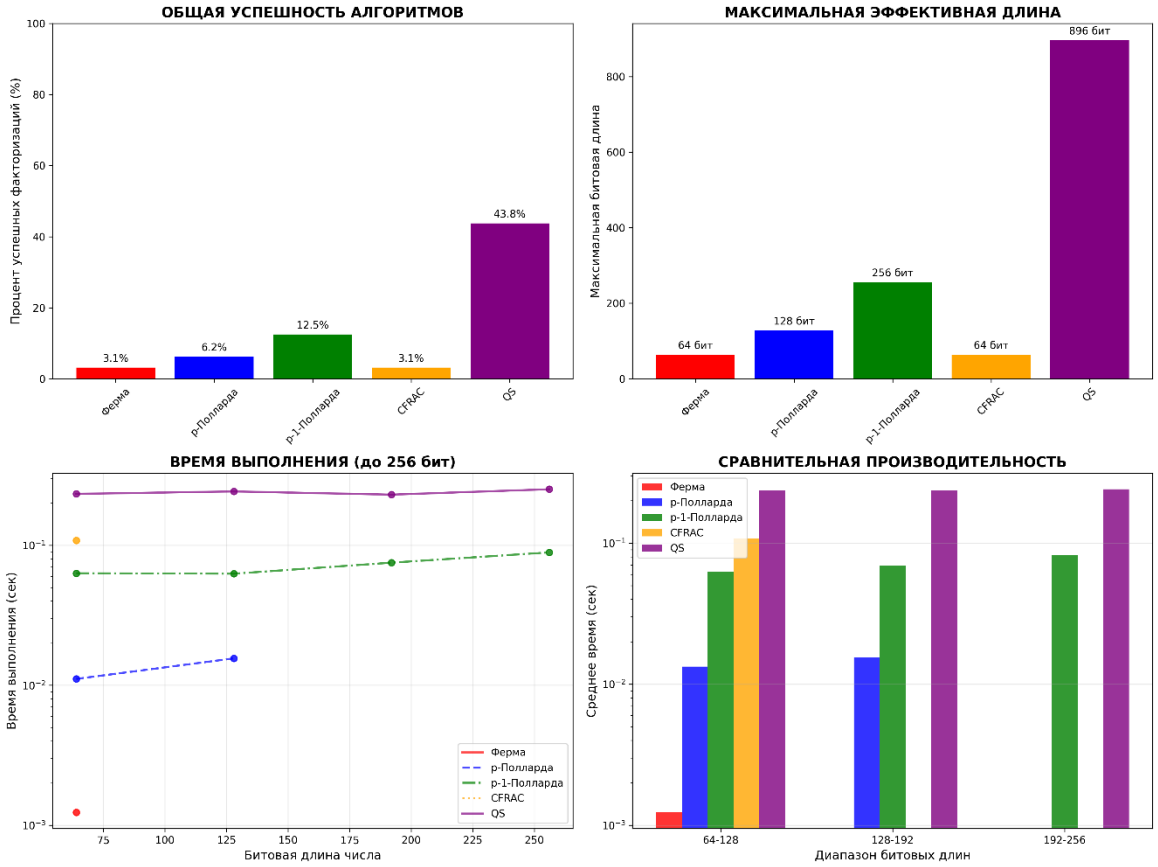

Рисунок 1 – Сводные метрики производительности

В подразделе 2.4 «Реализация атаки Винера» описываются функции на языке Python для атаки Винера.

В подразделе 2.5 «Описание работы приложения» рассматривается интерфейс и функционал платформы. На рисунке ниже представлена главная страница платформы с возможностью перехода к теории и практике.

Рисунок 2 – Главная страница платформы

В подразделе 2.5.1 «Теоретические блоки» описывается пользовательский интерфейс страницы с 8-ю теоретическими блоками с вопросами на проверку и возможностью экспорта в формате PDF для каждого раздела. Страница с теоретическими блоками представлена на рисунке ниже.

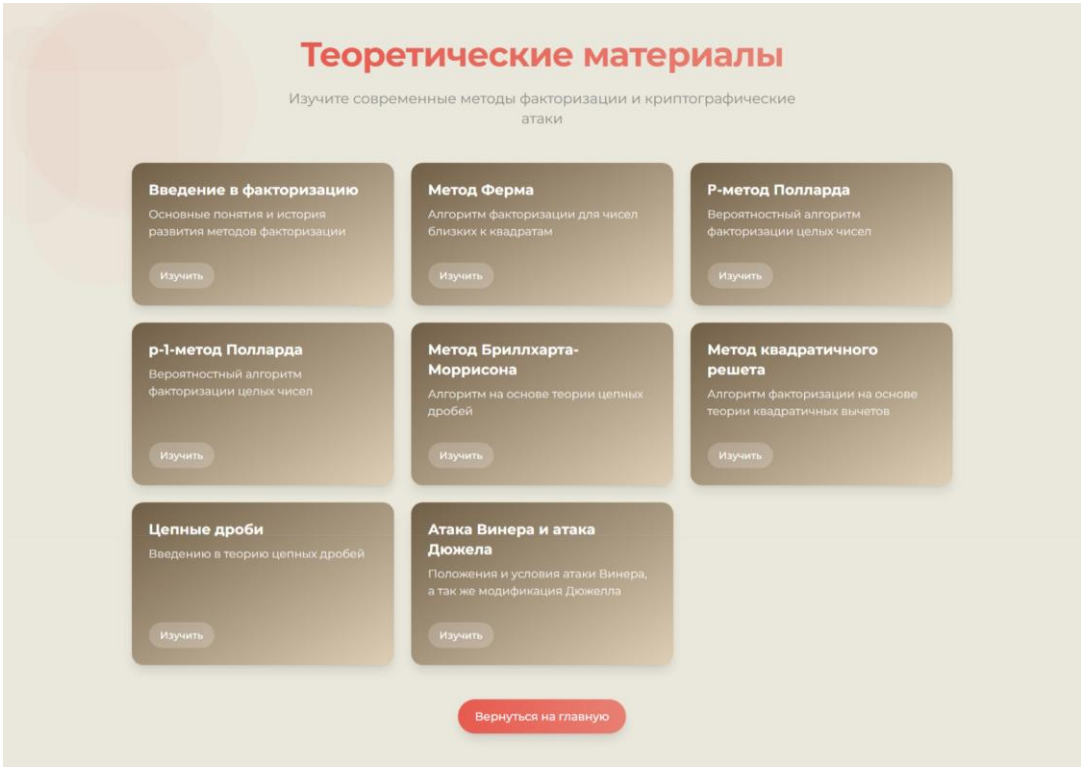

Рисунок 3 – Теоретические блоки платформы

В подразделе 2.5.2 «Практические разделы» описывается пользовательский интерфейс страницы практических модулей, которая содержит модули сравнения, генератор ключей, пошаговую реализацию атаки Винера и криптографическую песочницу. Интерфейс страницы практических модулей представлен на рисунке ниже.

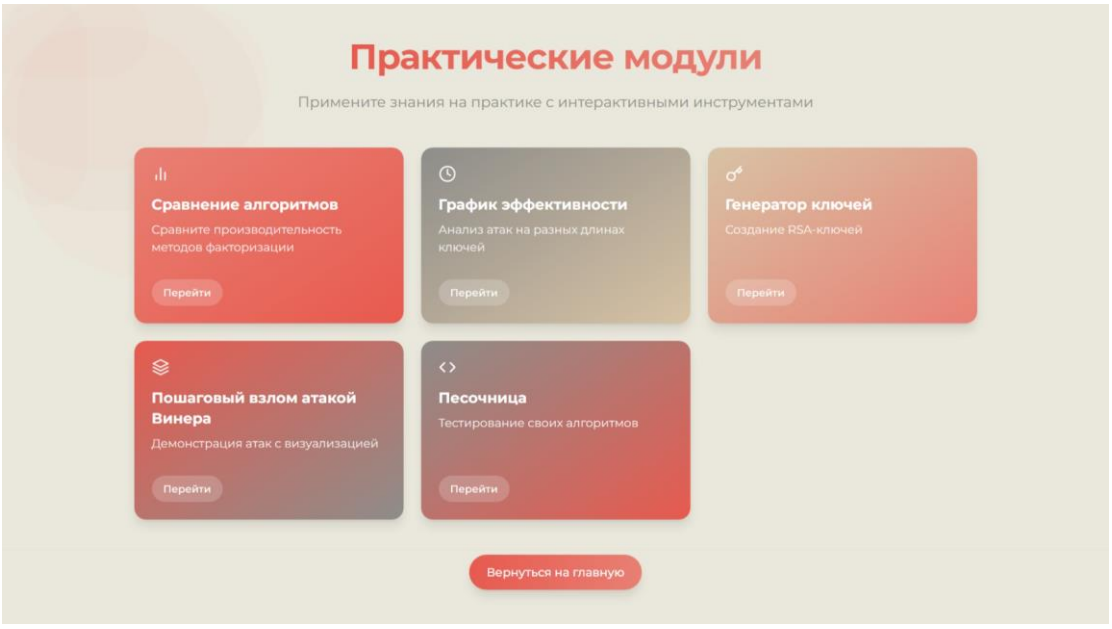

Рисунок 4 – Практические модули платформы

На платформе есть страница модуля сравнения по 4 алгоритмам со столбчатой диаграммой и вводом пользовательского числа для разложения.

Следующий практический модуль – страница с графиком эффективности для 5 алгоритмов и вводом пользовательского числа для отображения на числовой прямой. График можно приближать и есть функция отключения конкретных методов.

Модуль генерации RSA ключей – возможность генерации ключей в двух режимах. Автоматический режим предоставляет 512, 768 и 1024 бит для размера ключа. Ключи можно экспортировать в форматах PEM и DER.

Модуль атаки Винера позволяет использовать автоматическую генерацию и собственные данные. Для каждого шага можно подробнее посмотреть детали шага с подходящей дробью и кандидатами. График приближается и увеличивается, атаку можно поставить на паузу, что полезно при взломе больших значений.

Последний из доступных в этой версии приложения модуль – криптографическая песочница. Доступны простейшие сохраненные скрипты для генерации ключей RSA, факторизации модуля N и пустое поле для своего кода. Скрипты можно сохранять, а также загружать уже существующие скрипты с компьютера.

ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы разработана веб-платформа для изучения алгоритмов факторизации и тестирования, создания собственных скриптов и генерации ключей. Данный проект полностью соответствует поставленным задачам и достигает целей, которые были определены в начале исследования.

Перед началом разработки был проведен комплексный анализ теоретических материалов и существующих реализаций алгоритмов. Это позволило определить ключевые функциональные требования и требования к производительности. В результате анализа было выявлено, что существует множество алгоритмов факторизации, каждый из которых эффективен в определённом диапазоне размеров чисел и при определённых условиях. Субэкспоненциальные алгоритмы стали наиболее эффективными для факторизации больших чисел, а также ведется активное внедрение квантовой криптографии, что повлияет на существующие способы защиты информации.

Для реализации проекта был выбран современный технологический стек. Клиентская часть была разработана с использованием фреймворка React, библиотеки Tailwind CSS для стилизации компонентов и Redux для управления состоянием приложения. Такой подход позволил создать удобный и интуитивно

понятный интерфейс. Для выполнения скриптов алгоритмов был использован инструмент Pyodide, что позволило отказаться от серверной части проекта для безопасности и простоты работы.

В процессе изучения теоретических материалов и для подготовки к реализации платформы были разработаны алгоритмы факторизации Ферма, ρ-Полларда, $p-1$-Полларда и Бриллхарта-Моррисона и квадратичного решета на языке python.

В процессе разработки платформы успешно реализована многокомпонентная система, включающая следующие модули:

- теоретические блоки с вопросами, возможностью экспорта и указанными источниками;
- модуль сравнения алгоритмов Ферма, ρ-Полларда, $p-1$-Полларда и Бриллхарта-Моррисона, представленный в виде столбчатой диаграммы для наглядного представления времени выполнения факторизации для введенного пользователем числа;
- модуль сравнения алгоритмов Ферма, ρ-Полларда, $p-1$-Полларда и Бриллхарта-Моррисона и квадратичного решета на графике с возможностью включения/отключения алгоритма в сравнение и отображением пользовательского числа на числовой прямой;
- генератор ключей для шифрсистемы RSA в автономном и ручном режиме по пользовательским параметрам с экспортом в форматах .PEM и .DER;
- интерактивный модуль для пошагового взлома шифрсистемы RSA атакой Винера с отображением шагов, детальным пояснением каждого из них и возможностью запуска как автоматически сгенерированных параметров, так и пользовательских;
- среда для разработки на языке python с импортом, экспортом и уже представленными на платформе скриптами для атаки на RSA и генератором ключей.

Разработанная веб-платформа имеет значительный потенциал для дальнейшего развития и совершенствования. Среди перспективных направлений доработки можно выделить добавление алгоритмов решета числового поля и алгоритмов на эллиптических кривых. Благодаря чистоте архитектуры и простоте хранения теории в файлах JSON с библиотекой katex платформу можно расширять и добавлять всё большее число теоретических блоков для смежных тем, интегрировать дискретное логарифмирование и возможность изучения механизма электронных подписей.

Практическая значимость разработанной платформы определяется возможностью ее применения в различных образовательных сценариях.

Понимание особенностей и ограничений различных методов факторизации позволяет оптимизировать процессы факторизации в прикладных задачах, например, в криптоанализе или при тестировании криптосистем на прочность.

Таким образом, разработанная веб-платформа для изучения методов факторизации представляет собой полноценное решение для комплексного погружения в тему.