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

# Криптосистемы на основе конечных полугрупп

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Кутина Виктора Николаевича

Научный руководитель
д. ф.-м. н., профессор _____ В.А. Молчанов
23.01.2021 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2021 г.

Саратов 2021

# ВВЕДЕНИЕ

В настоящее время, а именно в эру развития информационных технологий, существует острая необходимость в обеспечении информационной безопасности, поэтому так актуальна и важна наука криптография, занимающаяся защитой данных.

В повседневной жизни большинство людей сталкивается с практической криптографией, к примеру, с криптографическими системами, которые применяются для обеспечения безопасности денежных переводов, конфиденциальности данных при их передаче по сети Интернет и прочих сетевых транзакциях. Именно поэтому разработка и усовершенствование криптосистем является одним из наиболее важных направлений в криптографии. В мире постоянных коммуникаций, где пользовательские данные нуждаются в защите от злоумышленников, которые хотят этими данными завладеть, необходима разработка криптосистем устойчивых к взлому. К примеру, увеличить устойчивость криптосистемы можно при помощи некоторых классов универсальных алгебр. Базируясь, к примеру, на конечных полугруппах, криптографическую стойкость криптосистемы можно повысить за счет неразрешимости проблемы равенства слов. Эта проблема для многих классов алгебр была решена полностью, но для некоторых важных классов была доказана ее неразрешимость. Проблема равенства слов является трудно разрешимой и может использоваться в криптографии для построения криптографических систем на основе универсальных алгебр. Помимо этого, криптографическую стойкость криптосистемы можно повысить за счет использования при шифровании каждый раз новой сгенерированной полугруппы или группы.

Сгенерированные группы и полугруппы можно использовать также в протоколах обмена ключей. Например, задав коммутирующие перестановки или коммутирующие обратимые квадратные матрицы, можно сгенерировать абелеву группу, на основе которой строится протокол

обмена ключами Диффи-Хэллмана. Помимо этого, полугрупповая криптография является одной из альтернатив решения проблемы постквантовой криптографии.

Целью данной работы является разработка алгоритмов вычисления конечных полугрупп для применения их в построении полугрупповых и групповых криптосистем.

Решаемые задачи:

1. Разработать алгоритмы вычисления конечных полугрупп квадратных матриц заданного порядка и полугрупп преобразований.
2. Применить сгенерированные конечные группы квадратных матриц заданного порядка и полугруппы преобразований в построении обобщенной криптосистемы Эль-Гамаля.
3. Применить сгенерированные конечные полугруппы слов в построении криптосистемы, основанной на неразрешимости проблемы равенства слов.

Главной задачей работы является разработка программного продукта, который реализует понятный и удобный интерфейс для вычисления конечных полугрупп матриц и преобразований с помощью различных алгоритмов, а также для шифрования открытых текстов и дешифрования криптограмм с применением обобщенной криптосистемы Эль-Гамаля и криптосистемы, базирующейся на конечной полугруппе слов с эффективно разрешимой проблемой равенства слов.

Дипломная работа состоит из введения, трех разделов, заключения, списка использованных источников и одного приложения. Общий объем работы – 130 страниц, из них 60 страниц – основное содержание, включая 46 рисунков и 1 таблицу, список использованных источников из 22 наименований. Приложение в работе занимает 70 страниц и содержит исходный код разработанного программного комплекса, предназначенного для генерации конечных полугрупп и реализующего описанные полугрупповые криптосистемы,написанного на языке программирования Java, а также верстку

интерфейса подпрограмм (сконфигурированные xmlтеги) и текст конфигурационного файла pom.xml, необходимого для сборки и запуска программного комплекса.

## КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел дипломной работы посвящен рассмотрению основных понятий, касающихся полугрупп и групп, способов их задания и алгоритмов генерации полугрупп. Данный раздел содержит три подраздела, в первом из которых рассматриваются следующие начальные понятия общей алгебры, понятия, касающиеся полугрупп, групп иполей: полугруппа, симметрическая полугруппа бинарных отношений на множестве, абелева полугруппа, моноид, нулевой элемент полугруппы, нейтральный элемент полугруппы, обратимый элемент полугруппы, идемпотент, таблица Кэли, подполугруппа, порождающее множество полугруппы, циклическая полугруппа, группа, абелева группа, кольцо, коммутативное кольцо, поле.

В этом же разделе приведены следующие понятия, касающиеся полугрупп слов и копредставления полугруппы: алфавит, буквы алфавита, слово, пустое слово, операция конкатенации слов, полугруппа слов, моноид слов, множество порождающих символов полугруппы слов, соотношения полугруппы слов, определяющие соотношения полугруппы слов, копредставление полугруппы слов. Здесь же приводитсяизвестная теорема, играющая важную роль в представлении конечных полугрупп.

Теорема 1 (О представлении полугрупп словами).

Любая полугруппа $S$является фактор-полугруппой некоторой полугруппы слов $A^+$, то есть$S \cong A^+/\varepsilon$для некоторой конгруэнции $\varepsilon$ полугруппы $A^+$.

Во втором подразделе рассматриваются задания полугрупп и групп матрицамии преобразованиями, приведены примеры полугрупп, заданных матрицамии преобразованиями, а также определены следующие понятия: преобразование множества, полугруппа всех преобразований на множестве, тождественное преобразование, перестановка, матрица, военный порядок (militaryorder).Здесь также приводится известная теорема Кэли о представлении

полугрупп преобразованиями, которая играет важную роль в вычислении конечных полугрупп.

Третий подраздел содержит описание общего подхода к генерации полугрупп, а также включает в себя еще два подраздела: в первом подразделе описана схема простого алгоритма генерации конечных полугрупп, во втором подразделе рассматривается понятие редукции и приведена схема расширенного алгоритма генерации конечных полугрупп, позволяющего получить список определяющих соотношений генерируемой конечной полугруппы. В этом же подразделе показано, как редукции можно использовать для определения моноидов:

Предложение 1.Пусть$\rho$ – редукция на множестве слов $A^*$, а $R$–множество ее редуцированных слов. Тогда множество$R$соперациейумножения, определенной как $u \cdot v = \rho(uv)$, является моноидом.

Второй раздел дипломной работы посвящен описаниюкриптосистем на основе конечных полугрупп и рассмотрению связанных с этими криптосистемами понятий. Этот раздел содержит три подраздела, в первом из которых определены следующие понятия: шифрование, криптографическая система, симметричные криптосистемы, ассиметричные криптосистемы (криптосистемы с открытым ключом), односторонняя функция, трудновычислимая задача, а также рассмотрены преимущества криптосистем с открытым ключом. Во втором подразделе описывается обобщенная криптосистема Эль-Гамаля, которая базируется на конечных группах, а также рассматриваются следующие понятия: дискретный логарифм, проблема вычисления дискретного логарифма, обобщенная проблема дискретного логарифмирования, связанная с действиями полугруппы (группы) на множестве.Втретьем подразделе определена проблема равенства слов в конечных полугруппах и рассматривается схема полугрупповой криптосистемы на основе проблемы равенства слов, а именно общие параметры криптосистемы, шифрование и дешифрование в рамках этой криптосистемы.

Третий раздел содержит описание реализованного в ходе выполнения дипломной работы программного комплекса, здесь же приводятся примеры входных параметров для всех подпрограмм разработанного программного комплекса, а также подробное описание интерфейса каждой подпрограммы.

Данный раздел содержит в себе четыре подраздела, в первом подразделе описывается функционал программного комплекса и перечислены средства, с помощью которых был разработан программный комплекс, здесь же стоит отметить, что разработанный программный комплекс является кроссплатформенным.

Во втором подразделе описан интерфейс подпрограммы генерации конечных полугрупп, приведены примеры генераций полугрупп преобразований и полугрупп квадратных матриц, приведен пример выгрузки сгенерированной полугруппы в файл в формате JSON.

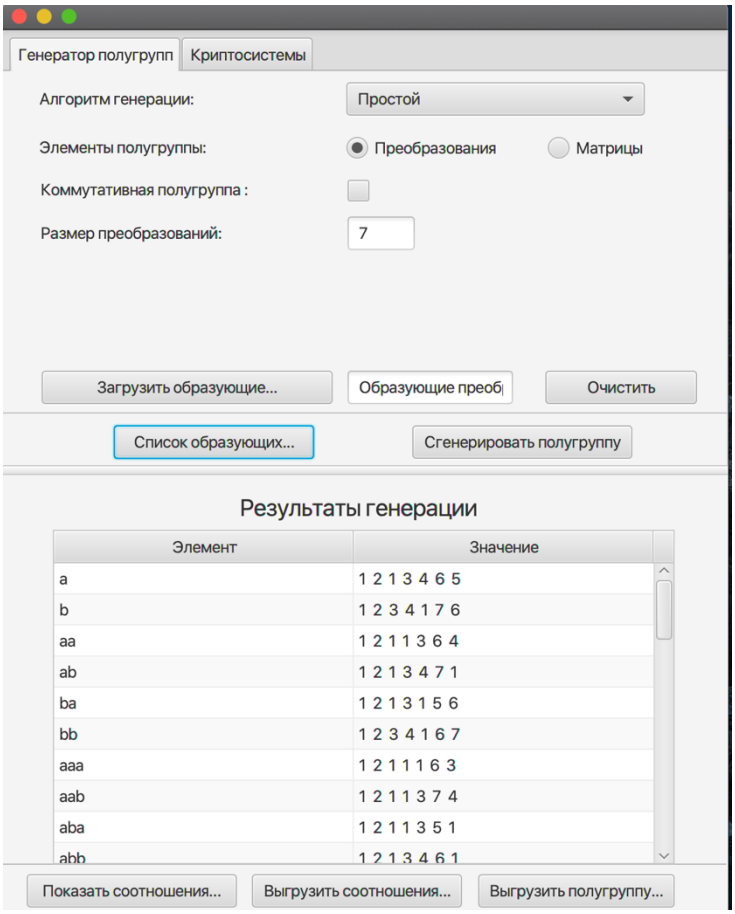


Рисунок 1 – Интерфейс подпрограммы генерации конечных полугрупп

Здесь же приводится пример выбора в качестве порождающих элементов полугруппы случайных коммутирующих преобразований для генерации

коммутативных полугрупп. В этом же подразделе приведен пример соотношений, порожденных сгенерированной полугруппой, показана возможность просмотра и выгрузки порожденных соотношений в текстовый файл в формате JSON, а также сравнивается количество соотношений, порожденных одной полугруппой, сгенерированной простым и расширенным алгоритмами.

В третьем подразделе описывается интерфейс подпрограммы, реализующей шифрование и дешифрование в рамках обобщенной криптосистемы Эль-Гамаля, приводится пример загрузки, сгенерированной ранее группы и генерации открытого ключа по случайно выбранному секретному ключу, а также примеры шифрования открытого текста и дешифрования криптограммы в рамках данной криптосистемы.

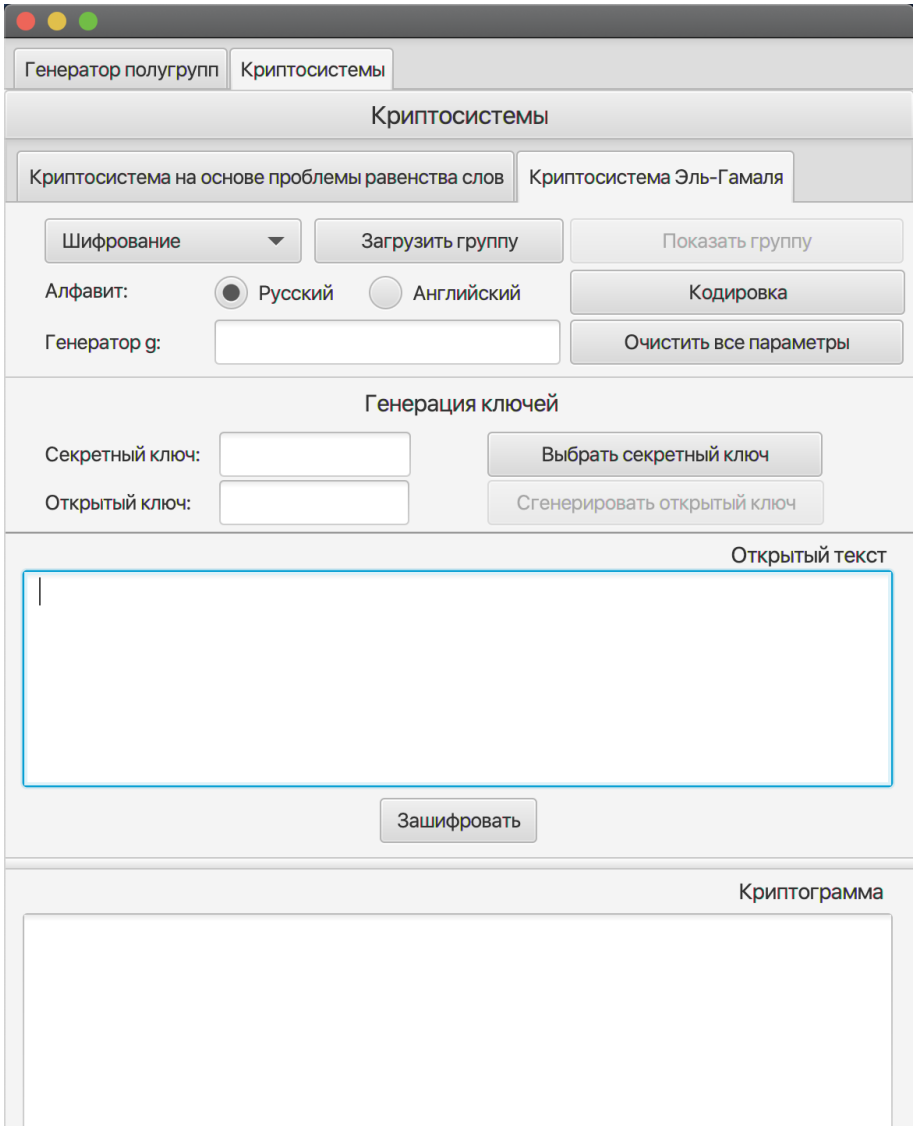


Рисунок 2 – Интерфейс обобщенной криптосистемы Эль-Гамаля

В четвертом подразделе описывается интерфейс подпрограммы, реализующей шифрование и дешифрование в рамках полугрупповой криптосистемы на основе проблемы равенства слов, приводится пример загрузки общих параметров данной криптосистемы, а именно полугруппы и соотношений открытого ключа, а также примеры шифрования открытого текста и дешифрования криптограммы в рамках данной криптосистемы.

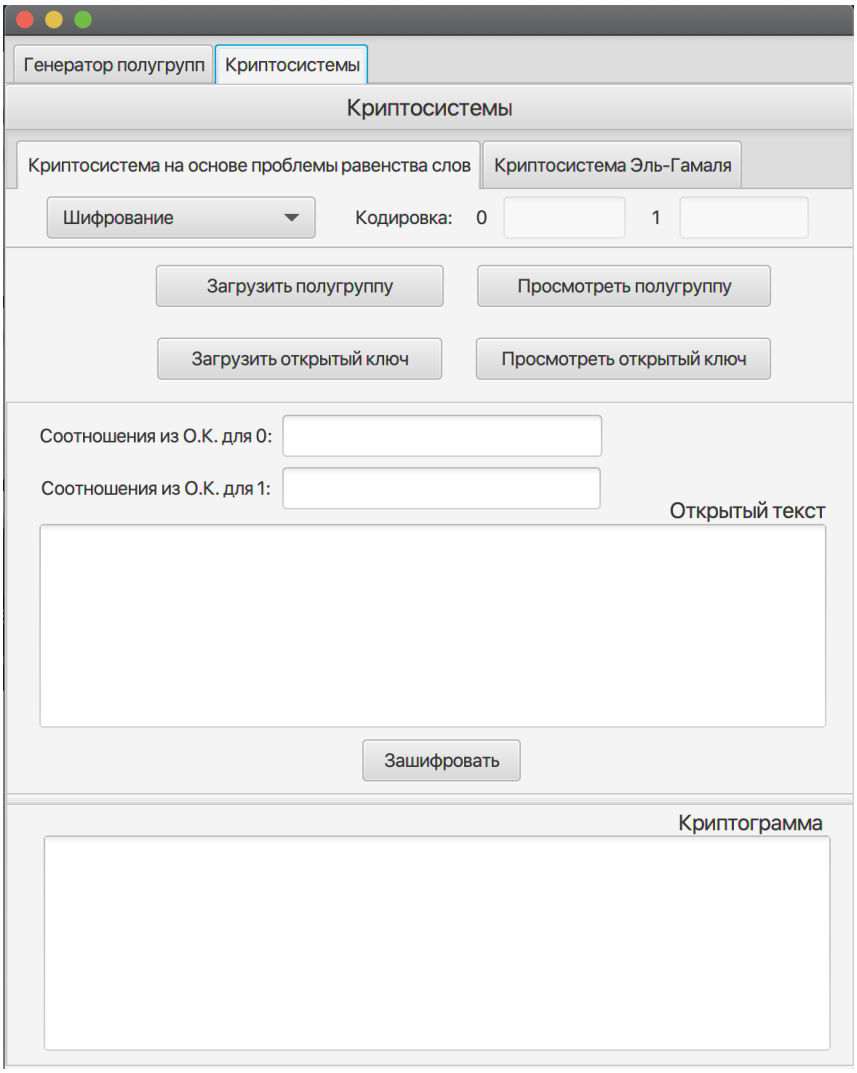


Рисунок 3 – Интерфейс полугрупповой криптосистеме на основе проблемы равенства слов

# ЗАКЛЮЧЕНИЕ

В ходе выполнения работы рассмотрены простой и расширенный алгоритмы генерации конечных полугрупп квадратных матриц с элементами кольца вычетов, а также полугрупп преобразований конечного множества. С помощью конечных полугрупп реализованы следующие полугрупповые криптосистемы с открытым ключом: обобщенная криптосистема Эль-Гамаля и криптосистема, базирующаяся на проблеме неразрешимости равенства слов.

В практической части работы реализована программа на языке программирования Java, имеющая доступный и простой интерфейс для генерации конечных полугрупп квадратных матриц и конечных полугрупп преобразований, с возможностью выгрузки полученных полугрупп и их определяющих соотношений в формате JSON. Помимо этого, программа реализует обобщенную криптосистему Эль-Гамаля, базирующуюся на группах матриц или перестановок, а также криптосистему, базирующуюся на проблеме неразрешимости равенства слов в полугруппе. Разработанные криптосистемы имеют два режима: шифрования и дешифрования. Также разработанная программа является кроссплатформенной, то есть работает на большинстве операционных систем.

Стоит отметить, что в зависимости от порождающих элементов можно генерировать не только полугруппы, но и другие алгебраические структуры, к примеру, моноиды или группы, которые также можно применять в других криптосистемах. Генерируя заранее большое количество полугрупп или групп (в зависимости от используемой криптосистемы) с помощью разработанной подпрограммы генерации конечных полугрупп и применяя при шифровании каждый раз новую сгенерированную полугруппу или группу можно повысить криптографическую стойкость криптосистемы.

Все поставленные в рамках данной работы задачи выполнены полностью.

Полученные результаты могут использоваться для проведения экспериментов над конечными полугруппами и алгебраическими

криптосистемами, а также в учебном процессе при изучении алгебраической криптографии.