Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Криптосистема публичного ключа на основе теории групп

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 632 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Байбакова Сергея Александровича

Научный руководитель

профессор, д.ф.-м.н. _____ В.А. Молчанов

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н. _____ В.Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

Большинство криптографических протоколов и схем основаны на трудных математических задачах или предполагаемом существовании односторонних функций. В эпоху, когда ведутся попытки создания квантовых компьютеров, поиск новых криптографических систем является актуальной задачей.

Алгоритмически неразрешимые и трудноразрешимые задачи теории групп могут использоваться в качестве основы для криптосистем. Существуют специальные типы криптографических систем, которые могут быть построены на основе проблемы равенства слов.

Целью работы является построение криптосистемы публичного ключа на основе трудноразрешимых проблем теории групп. Для этого рассматриваются следующие задачи:

1) изучение представления полугрупп и групп словами;
2) изучение трудноразрешимых проблем теории групп;
3) описание протокола передачи конфиденциальных сообщений по открытому каналу на основе трудноразрешимых проблем теории групп;
4) программная реализация на языке программирования C++ криптосистемы публичного ключа на основе трудноразрешимых проблем теории групп.

Основы для построения криптосистемы публичного ключа с помощью трудноразрешимых проблем теории групп изложены в работах [12], [13] и [18].

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы — 65 страниц, из них 48 страниц — основное содержание, включая 19 рисунков и 1 таблицу, список использованных источников из 18 наименований.

В первом разделе рассматриваются алгебраические структуры, использующиеся в данной работе. Приводится способ задания группы с помощью образующих элементов и определяющих соотношений. В качестве примера такого представления рассматривается группа кос.

Во втором разделе рассматриваются неразрешимые и трудноразрешимые алгоритмические проблемы теории групп, которые могут быть использованы в качестве основы для криптографических систем. В работе особую важность имеет проблема равенства слов.

В третьем разделе работы рассматривается применение теории групп для построения криптосистемы публичного ключа. Описывается протокол передачи конфиденциальных сообщений по открытому каналу на основе трудноразрешимых проблем теории групп.

В заключительном разделе работы приводится программная реализация криптосистемы публичного ключа на основе трудноразрешимых проблем теории групп.

КРАТКОЕ СОДЕРЖАНИЕ

Копредставление полугруппы (группы) — один из методов определения полугруппы (группы) указанием множества образующих элементов и определяющих соотношений. Копредставление часто называют заданием полугруппы (группы).

Алфавитом называют конечное множество элементов $X = \{x_1, \dots, x_n\}$.

Слово на алфавите символов $X = \{x_1, \dots, x_n\}$ — это пустая или конечная последовательность символов из $X \cup X^{-1}$, где $X^{-1} = \{x_1^{-1}, \dots, x_n^{-1}\}$ — алфавит, состоящий из обратных элементов для алфавита X. Если на множестве X не введена операция взятия обратного элемента, будем считать, что $X^{-1} = \{\emptyset\}$. Пустое слово обозначим символом 1.

Расширенным алфавитом X^* над алфавитом $X = \{x_1, \dots, x_n\}$ назовем совокупность всех слов из X. Алфавитом X^+ назовем алфавит X^* без пустого слова.

Над алфавитом X^* определена бинарная операция, которая называется *конкатенацией* (умножением). Конкатенацией двух слов u и v является новое слово $w = uv$, представляющее собой последовательность символов слова u, продолженных справа последовательностью символов слова v, с сохранением порядка символов.

Множество слов X^+ с введенной операцией конкатенации образует полугруппу, которая называется *полугруппой слов* над алфавитом X^+.

Теорема о представлении полугрупп словами. Любая полугруппа S является фактор-полугруппой некоторой полугруппы слов X^+, то есть $S \cong X^+/\varepsilon$ для некоторой конгруэнции ε полугруппы X^+ [7].

Если все слова полугруппы можно записать в виде конкатенации элементов $x_1, \dots, x_n$, то такие элементы $x_1, \dots, x_n$ называются *образующими полугруппы*.

Определяющим соотношением (правилом) на множестве $X = \{x_1, \dots, x_n\}$ назовем равенство вида $u = v$, где $u, v \in X^*$. Если слово w может быть представлено в виде $w_1 u w_2$, то выполняется равенство $w = w_1 v w_2$, где $w_1, w_2 \in X^*$. Если $u = v$, то $v = u$.

Пусть X — множество образующих элементов полугруппы S. На X задано множество определяющих соотношений ρ. Если все выполняющиеся на S соотношения получены с помощью применения конечного числа определяющих соотношений ρ, то выражение $< X : \{u = v : (u, v) \in \rho\} >$ называется *копредставлением полугруппы* S.

Множество слов $(X \cup X^{-1})^*$ с введенной операцией конкатенации и выделенным нейтральным элементом 1 (пустое слово) образует полугруппу слов над алфавитом $(X \cup X^{-1})^*$. Фактор-алгебра $(X \cup X^{-1})^*/\delta$ полугруппы слов над алфавитом $(X \cup X^{-1})^*$ по конгруэнции δ, порожденной множеством соотношений вида: $xx^{-1} = 1$ и $x^{-1}x = 1$, где $x \in X$, является группой, которая называется свободной группой с порождающим множеством X и обозначается $F(X)$.

Если все слова группы можно записать в виде конкатенации элементов $x_1, \dots, x_n$ и их обратных, то такие элементы $x_1, \dots, x_n$ называются *образующими группы*.

Теорема о представлении групп словами. Любая группа G с множеством образующих элементов X изоморфна фактор-полугруппе $F(X)/H$ для некоторой нормальной подгруппы H группы $F(X)$. Подгруппа H задается своим множеством образующих R. Тогда фактор-полугруппа $F(X)/H$ определяется выражением $< X : \{r = 1 : r \in R\} >$, которое называется *копредставлением группы* G [6].

Рассмотрим трехмерное пространство с началом координат в точке O и тремя взаимно перпендикулярными координатными осями x, y и z соответственно. Зафиксируем две прямые в плоскости Oxz таким образом,

чтобы данные прямые были параллельны оси Ox и одна располагалась ниже другой. На каждой из прямой зафиксируем n точек. Точки верхней прямой обозначим $\mathrm{X}_1, \ldots, \mathrm{X}_n$, а точки нижней прямой — $\mathrm{Y}_1, \ldots, Y_n$.

Математическая коса состоит из n нитей. Под *нитью* будем понимать ломаную в пространстве.

Косой называют объект в пространстве, состоящий из n попарно непересекающихся нисходящих нитей, соединяющих точки $\mathrm{X}_1, \ldots, \mathrm{X}_n$ с точками $\mathrm{Y}_1, \ldots, Y_n$ в произвольном порядке.

Множество классов эквивалентности кос из n нитей с заданной описанным выше способом операцией умножения образует группу, которая называется *группой кос* и обозначается B_n [4]. Данная группа некоммутативна.

В теории кос можно всю геометрию заменить алгебраическими преобразованиями. Группа кос B_n задается с помощью образующих и определяющих соотношений, а элементы группы заменяются словами.

Обозначим через b_i косу, состоящую из n нитей, i-я нить которой проходит над $(i+1)$-й, создавая ровно одно переплетение, а остальные нити вертикальны. Тогда геометрическую интерпретацию косы в виде объекта в пространстве можно заменить словом, составленным из символов $b_1, \ldots, b_{n-1}$ и $b_1^{-1}, \ldots, b_{n-1}^{-1}$. Согласно определению получаем, что $b_1, \ldots, b_{n-1}$ являются образующими группы B_n.

Для группы кос справедливы следующие соотношения:

1) $b_i b_j = b_j b_i$, если $|i-j| \geq 2, 1 \leq i, j \leq n-1$

2) $b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1}$ для $1 \leq i \leq n-2$

3) $b_i b_i^{-1} = b_i^{-1} b_i = 1$ для $1 \leq i \leq n-1$

Теорема Артина. Две косы a и b, заданные своими записями через образующие элементы, являются эквивалентными тогда и только тогда, когда коса b может быть получена из косы a последовательным применением преобразований 1-3 [5].

Проблема равенства для группы, заданной с помощью системы образующих элементов и определяющих соотношений, заключается в том, чтобы найти алгоритм, позволяющий для любой пары слов в алфавите, состоящем из образующих группы и обратных к ним элементов, определить, представляют заданные слова один и тот же элемент группы или разные элементы. Другими словами, ответить на вопрос, можно ли получить из одного слова другое с помощью определяющих соотношений [8].

Теорема. Проблема равенства слов разрешима для группы кос B_n при любых n [8].

В данной работе для решения проблемы равенства в группе кос используется алгоритм, предложенный французским математиком Патриком Деорнуа [14]. Алгоритм Деорнуа эффективно реализуется на компьютере.

Рассмотрим криптосистему публичного ключа, основанную на проблеме равенства слов. Пусть задано конечное множество образующих элементов X и конечное множество определяющих соотношений R. Заданные множества X и R являются копредставлением некоторой группы G, в которой разрешима проблема равенства слов. Выбираются два неэквивалентных слова $w_0, w_1 \in G$. Копредставление группы (X, R) является закрытым ключом, а слова w_0 и w_1 — открытым ключом.

Пусть пользователь A — отправитель сообщения, B — получатель.

Общие параметры:

1. Закрытый ключ: (X, R) — копредставление группы G, в которой разрешима проблема равенства слов.
2. Открытый ключ: два неэквивалентных слова $w_0, w_1 \in G$.

Протокол передачи конфиденциальных сообщений по открытому каналу:

1. Пользователь A зашифровывает исходное сообщение. Каждому биту текста $i \in \{0,1\}$ ставится в соответствие зашифрованное слово,

эквивалентное слову w_i. В результате получаем список слов, который является зашифрованным сообщением.

2. Пользователь A передает пользователю B по открытому каналу зашифрованное сообщение.
3. Пользователь B, используя информацию о копредставлении группы G и информацию о кодировании бит словами (слова w_0 и w_1), применяет алгоритм расшифрования. Каждое слово из списка зашифрованного сообщения приводится к нормальной форме. Полученные слова посимвольно сравниваются с w_0 и w_1, также приведенными к нормальной форме. Слова эквивалентные w_0 соответствуют нулевому биту, а эквивалентные w_1 соответствуют единичному биту. Таким образом, пользователь B восстанавливает исходный текст.

Разработана программа на языке C++, в которой реализованы алгоритмы шифрования и расшифрования сообщений. В качестве основы для построения криптосистемы на выбор пользователю предоставляются две алгебраических структуры: коммутативная группа и группа кос.

ЗАКЛЮЧЕНИЕ

В настоящее время надежные и криптостойкие алгоритмы шифрования имеют большое значение, так как проблема информационной безопасности является одной из приоритетных проблем в современном мире. Актуальной задачей является поиск новых криптографических алгоритмов.

В данной работе построена криптосистема публичного ключа на основе теории групп. Рассмотрены трудноразрешимые проблемы теории групп, а также их применение в криптографии. Исследована задача шифрования и расшифрования текстовых сообщений на основе трудноразрешимых проблем теории групп. Описан протокол для передачи конфиденциальных сообщений по открытому каналу на основе трудноразрешимых проблем теории групп.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Адян С. И. Алгоритмические проблемы для групп и полугрупп [Электронный ресурс] / С. И. Адян, В. Г. Дурнев // Успехи мат. наук, 2000. Т. 55, № 2. 64-78 с. Загл. с экрана. Яз. рус.

2. Верещагин Н. К. Языки и исчисления [Электронный ресурс] / Н. К. Верещагин, А. Шень. Москва: МЦНМО, 2012. 189-190 с. Загл. с экрана. Яз. рус.

3. Григорьев Д. Ю. Алгебраическая криптография: новые конструкции и их надежность относительно доказуемого взлома [Электронный ресурс] / Д. Ю. Григорьев, А. Кожевников, С. И. Николенко. Санкт-Петербург: С.-Петербургское отделение Математического института им. В. А. Стеклова, Алгебра и анализ, 2008. 119-147 с. Загл. с экрана. Яз. рус.

4. Мантуров В. О. Лекции по теории узлов и их инвариантов [Электронный ресурс] / В. О. Мантуров. Москва: Эдиториал УРСС, 2001. 91-127 с. Загл. с экрана. Яз. рус.

5. Мантуров В. О. Экскурс в теорию кос [Электронный ресурс] / В. О. Мантуров. Москва: Математическое просвещение, 2010. 1-9 с. Загл. с экрана. Яз. рус.

6. Молчанов В. А. Алгебра и теория чисел [Электронный ресурс] / В. А. Молчанов. Саратов: Саратовский государственный социально-экономический университет, 2009. 120-153 с. Загл. с экрана. Яз. рус.

7. Молчанов В. А. Дискретная математика / В. А. Молчанов. Саратов: Саратовский государственный социально-экономический университет, 2013. 28-39 с.

8. Прасолов В. В. Узлы, зацепления, косы и трехмерные многообразия [Электронный ресурс] / В. В. Прасолов, А. Б. Сосинский. Москва: МЦНМО, 1997. 70-81 с. Загл. с экрана. Яз. рус.

9. Романьков В. А. Алгебраическая криптография [Электронный ресурс] / В. А. Романьков. Омск: Омский государственный университет им. Ф. М. Достоевского, 2013. 22-37 с. Загл. с экрана. Яз. рус.

10. Романьков В. А. Диофантова криптография на бесконечных группах [Электронный ресурс] / В. А. Романьков. Омск: Омский государственный университет им. Ф. М. Достоевского, 2012. 19-21 с. Загл. с экрана. Яз. рус.

11. Сосинский А. Б. Узлы и косы [Электронный ресурс] / А. Б. Сосинский. Москва: МЦНМО, 2001. 3-13 с. Загл. с экрана. Яз. рус.

12. Anshel I. An algebraic method for public-key cryptography [Электронный ресурс] / I. Anshel, M. Anshel, D. Goldfeld // Mathematical research letters, 1999. 287-291 с. Загл. с экрана. Яз. англ.

13. Birget Jean-Camille On public-key cryptosystems based on combinatorial group theory [Электронный ресурс] / Jean-Camille Birget, Spyros S. Magliveras, Michal Sramka // Tatra Mountains Mathematical Publications, 2006. Vol. 33(1). 137-148 с. Загл. с экрана. Яз. англ.

14. Dehornoy P. A fast method for comparing braids [Электронный ресурс] / P. Dehornoy // Advances in Mathematics, 1997. Vol. 125(2). 200-235 с. Загл. с экрана. Яз. англ.

15. Lukkarila V. A Mathematica-package for algebraic braid groups [Электронный ресурс] / V. Lukkarila. Turku: Turku Centre for Computer Science, 2005. 1-14 с. Загл. с экрана. Яз. англ.

16. Magnus W. Combinatorial group theory: presentations of groups in terms of generators and relations [Электронный ресурс] / W. Magnus, A. Karrass, D. Solitar. New York: Dover Publications, 1966. 1-104 с. Загл. с экрана. Яз. англ.

17. Paterson M. S. The set of minimal braids is co-NP-complete [Электронный ресурс] / M. S. Paterson, A. A. Razborov // Journal of Algorithms, 1991. Vol. 12(3). 393-408 с. Загл. с экрана. Яз. англ.

18. Wagner N. R. A public-key cryptosystem based on the word problem [Электронный ресурс] / N. R. Wagner, M. R. Magyarik. Philadelphia: Drexel University, Mathematics and Computer Science, 1985. 19-36 с. Загл. с экрана. Яз. англ.