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

Обобщённая система Диффи–Хеллмана

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Антипина Алексея Юрьевича

Научный руководитель
д. ф.-м. н., профессор _____ В. А. Молчанов
22.01.2024 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2024 г.

Саратов 2024

ВВЕДЕНИЕ

Протокол Диффи–Хеллмана, предложенный Уитфилдом Диффи и Мартином Хеллманом в 1976 году, представляет собой ключевой элемент в сфере криптографии, играющий важную роль в обеспечении безопасности обмена информацией в открытых сетях. Этот алгоритм решает проблему безопасного обмена ключами, что делает его фундаментальным в создании защищенных интернет-протоколов и технологий.

Принцип действия протокола Диффи–Хеллмана заключается в том, чтобы позволить двум сторонам безопасно согласовать общий секретный ключ, используемый для шифрования и расшифрования сообщений. Это достигается путем обмена открытыми параметрами и генерации общего секрета, который даже в случае перехвата данных не может быть легко восстановлен без соответствующих секретных ключей.

Применение протокола Диффи–Хеллмана охватывает широкий спектр областей, от веб-безопасности до виртуальных частных сетей. Он является основой для протоколов TLS/SSL, используемых в защищенных соединениях в интернете, и интегрируется в протоколы IPsec для обеспечения безопасности передачи данных в виртуальных сетях.

Уникальная особенность алгоритма заключается в том, что стороны могут создавать общий ключ, даже если часть информации была подслушана. Это устраняет необходимость в предварительной передаче ключа, что делает протокол Диффи–Хеллмана удобным и безопасным средством обеспечения конфиденциальности и целостности информации в открытых сетях. Сегодня, в эру всеобщей цифровизации, алгоритм Диффи–Хеллмана продолжает играть ключевую роль в обеспечении безопасности интернет-коммуникаций и обмена данными. Классический протокол Диффи–Хеллмана базируется на проблеме дискретного логарифма для числовых групп, которая может быть довольно эффективно решена с помощью теоретико-числовых методов и квантовых алгоритмов.

Протокол Диффи–Хеллмана, несмотря на свою важность в сфере криптографии и широкое применение в обеспечении безопасности обмена информацией, обладает определенными недостатками, которые могут подвергнуть его угрозам взлома. Один из основных недостатков заключается в отсутствии аутентификации сторон, что делает протокол уязвимым к атакам посередине (Man-in-the-Middle), где злоумышленник может несанкционированно встать на пути обмена ключами и изменить передаваемые данные. Это может привести к созданию общего ключа с злоумышленником вместо предполагаемой легитимной стороны.

Целью данной работы является реализация усложненных версий алгоритма Диффи–Хеллмана и исследование их криптостойкости.

В первой части диплома приведены основные алгебраические конструкции, используемые в работе, описание классического протокола Диффи–Хеллмана и описание усложненных его версий. Приводятся примеры структур, с помощью которых повышается криптостойкость алгоритма.

Во второй части программно реализованы все рассмотренные версии протокола Диффи–Хеллмана, усложненные с помощью таких алгебраических структур, как групповое кольцо и матричная полугруппа над групповым кольцом.

Дипломная работа состоит из введения, 2 разделов, заключения, списка использованных источников и приложения. Общий объем работы – 61 страница, из них 48 страниц – основное содержание, включая 29 рисунков и 2 таблицы, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе «Теоретическая часть» представлена фундаментальная теория, включая описания алгоритмов и алгебраических структур. Кроме того, проведен сравнительный анализ производительности алгоритма Диффи–Хеллмана на различных платформах.

В подразделе 1.1 «Классический алгоритм Диффи–Хеллмана» представлена классическая версия алгоритма, включая его ключевые характеристики. Кратко описаны особенности алгебраических структур, которые будут использованы в последующем.

В подразделах 1.2 «Полупрямые произведения и расширения с автоморфизмами» и 1.3 «Симметрическая группа» приводятся определения полупрямого произведения и симметрической группы, которые будут использоваться в алгоритмах.

Пусть G, H – две группы, $Aut(G)$ – группа автоморфизмов G, и $p: H \to Aut(G)$ – гомоморфизм. Тогда полупрямое произведение G и H – это множество

$$\Gamma = G \ltimes H = \{(g, h): g \in G, h \in H\}$$

с групповой операцией $\cdot$, заданной

$$(g, h) \cdot (g', h') = \left(g^{p(h')} \cdot g', h \cdot h'\right).$$

Здесь $g^{p(h')}$ обозначает образ g под действием автоморфизма $p(h')$, и, когда описывается произведение $h \cdot h'$ двух морфизмов, это означает, что сначала применяется h.

Симметрическая группа S_m не является абелевой (некоммутативная) при $m \geq 3$. Порядок данной группы $|S_m| = m!$ – количество всех перестановок из m элементов. Единичная (тождественная) подстановка обозначается

$$e = \begin{pmatrix} 1 & 2 & m \\ 1 & 2 & m \end{pmatrix}$$

и для нее выполняется $(\forall \pi \in S_m)\ \pi e = e\pi = \pi$.

В подразделе 1.4 «Протокол обмена ключами» описывается алгоритм Диффи–Хеллмана, усложненный использованием произвольного автоморфизма.

1. Алиса вычисляет $(g,\varphi)^m = (\varphi^{m-1}(g)\dots\varphi^2(g)\cdot\varphi(g)\cdot g, \varphi^m)$ и отправляет только первый компонент этой пары Бобу. Таким образом, она отправляет Бобу только элемент $a = \varphi^{m-1}(g)\dots\varphi^2(g)\cdot\varphi(g)\cdot g$ из (полу)группы G.

2. Боб вычисляет $(g,\varphi)^n = (\varphi^{n-1}(g)\dots\varphi^2(g)\cdot\varphi(g)\cdot g, \varphi^n)$ и отправляет только первый компонент этой пары Алисе. Таким образом, он отправляет Алисе только элемент $b = \varphi^{n-1}(g)\dots\varphi^2(g)\cdot\varphi(g)\cdot g$ из (полу)группы G.

3. Алиса вычисляет $(b,x)\cdot(a,\varphi^m) = (\varphi^m(b)\cdot a, x\cdot\varphi^m)$. Ее ключ теперь $K_A = \varphi^m(b)\cdot a$. На самом деле она не «вычисляет» $x\cdot\varphi^m$, потому что она не знает автоморфизм $x = \varphi^n$. Напомним, что он ей не передавался. Но ей это не нужно для вычисления K_A.

4. Боб вычисляет $(a,y)\cdot(b,\varphi^n) = (\varphi^n(a)\cdot b, y\cdot\varphi^n)$. Его ключ теперь $K_B = \varphi^n(a)\cdot b$. На самом деле он не «вычисляет» $y\cdot\varphi^n$, потому что он не знает автоморфизм $y = \varphi^m$. Напомним, что он ему не передавался. Но ему это не нужно для вычисления K_B.

5. Поскольку $(b,x)\cdot(a,\varphi^m) = (a,y)\cdot(b,\varphi^n) = (g,\varphi)^{m+n}$, должно быть, что $K_A = K_B = K$, общий секретный ключ.

В отличие от «стандартного» обмена ключами Диффи–Хеллмана, правильность здесь основана на равенстве $h^m\cdot h^n = h^n\cdot h^m = h^{m+n}$, а не на равенстве $(h^m)^n = (h^n)^m = h^{mn}$. В «стандартной» настройке Диффи–Хеллмана этот хитрый метод не сработал бы, потому что, если общий ключ K был бы всего лишь произведением двух открыто переданных элементов, то любой, включая подслушивающего, мог бы вычислить K.

В подразделе 1.5 «Групповые кольца» вводится определение группового кольца. Где оно определяется как множество всех формальных сумм

$$r = \sum_{g_i \in G} r_i g_i,$$

где r_i – элементы из кольца R, G – группа, записанная умножением, а R – любое коммутативное кольцо с ненулевой единицей. Для группового кольца также определяются операции сложения и умножения и приводятся примеры этих операций.

В подразделе 1.6 «Протокол обмена ключами Диффи–Хеллмана на основе полугруппы матриц над групповым кольцом» приводится алгоритм на основе полугруппы матриц над групповым кольцом $M_3(Z_n[S_m])$. Хотя S_m является относительно небольшой группой для небольших значений m, размер группового кольца $Z_n[S_m]$ растет достаточно быстро, даже для малых значений n и m. Полугруппа $M_3(Z_7[S_5])$ из матриц размером 3 × 3 имеет порядок $(7^{5!})^9 \approx 10^{913}$.

1) Выбирается открытая матрица $M \in M_3(Z_n[S_m])$, где n – мощность кольца, m – мощность множества, на котором рассматривается симметрическая группа.

2) Алиса выбирает закрытый большой положительный целый параметр a и вычисляет M^a. Она отправляет M^a Бобу.

3) Боб выбирает закрытый большой положительный целый параметр b и вычисляет M^b. Он отправляет M^b Алисе.

4) Алиса вычисляет общий секретный ключ $K_a = (M^b)^a$.

5) Боб вычисляет общий секретный ключ $K_b = (M^a)^b$.

6) Секретные ключи Алисы и Боба равны $K = K_A = K_B$.

В подразделе 1.7 «Распространенные атаки на алгоритм Диффи–Хеллмана» приводятся основные и самые распространенные атаки на алгоритм Диффи–Хеллмана. Первый атака использует алгоритм «шаг младенца – шаг великана». Один из известных методов атаки на «классическую» проблему дискретного логарифма, предложенный Шенксом. Эта атака вычислительно

невозможна, так как наши матрицы являются достаточно сложными объектами и для их хранения потребуется очень много дискового пространства.

Вторая атака основывается на алгоритме Полига–Хеллмана для решения проблемы дискретного логарифма. Этот алгоритм основан на порядке элемента группы и обобщенной китайской теореме об остатках, чтобы разбить задачу на более мелкие подзадачи. Однако в этой ситуации порядок матриц в $M_3(Z_5[S_5])$ не связан с размером всего кольца $M_3(Z_5[S_5])$, поэтому китайская теорема об остатках действительно не помогает разбить эту проблему на более мелкие части.

Третий алгоритм – это $\rho -$ алгоритм Полларда. Однако при применении алгоритма поиска цикла Флойда в атаке $\rho -$ алгоритма Полларда необходимо знание порядка циклической группы, порожденной M. В нашей ситуации не только порядок M неизвестен, но, что более важно, поскольку случайный M с огромной вероятностью не будет обратимым, соображения о порядке не применимы. Следовательно, не применима атака $\rho -$ Полларда, по крайней мере, в ее стандартной форме.

В подразделе 1.8 «Матрицы над групповыми кольцами и расширения внутренними автоморфизмами» приводится алгоритм, объединяющий две предыдущие версии.

1) Алиса и Боб соглашаются на общих матрицах $M \in G$ и $H \in M_3(Z_7[S_5])$. Алиса выбирает секретное положительное целое число m, а Боб выбирает секретное положительное целое число n.

2) Алиса вычисляет $(M, \varphi_H)^m = (H^{-m+1}MH^{m-1}\dots H^{-2}MH^2H^{-1}MH \cdot M, \varphi_H^m)$ и отправляет только первый компонент этой пары Бобу. Таким образом, она отправляет Бобу только матрицу:

$$A = H^{-m+1}MH^{m-1}\dots H^{-2}MH^2H^{-1}MH \cdot M = H^{-m}(HM)^m.$$

3) Боб вычисляет $(M, \varphi_H)^n = (H^{-n+1}MH^{n-1}\dots H^{-2}MH^2H^{-1}MH \cdot M, \varphi_H^n)$ и отправляет только первый компонент этой пары Алисе. Таким образом, он отправляет Алисе только матрицу:

$$B = H^{-n+1}MH^{n-1}\dots H^{-2}MH^{2}H^{-1}MH \cdot M = H^{-n}(HM)^{n}.$$

4) Алиса вычисляет $(B, x) \cdot (A, \varphi_H^m) = (\varphi_H^m(B) \cdot A, x \cdot \varphi_H^m)$. Ее ключ теперь $K_{Alice} = \varphi_H^m(B) \cdot A = H^{-(m+n)}(HM)^{(m+n)}$. Стоит обратить внимание, что она фактически не вычисляет $x \cdot \varphi_H^m$, потому что она не знает автоморфизма $x \cdot \varphi_H^n$. Напомним, что он не был передан ей. Но ей это и не нужно для вычисления K_{Alice}.

5) Боб вычисляет $(A, y) \cdot (B, \varphi_H^n) = (\varphi_h^n(A) \cdot B, y \cdot \varphi_H^n)$. Его ключ теперь $K_{Bob} = \varphi_H^n(A) \cdot B = H^{-(m+n)}(HM)^{(m+n)}$. Боб фактически не вычисляет $y \cdot \varphi_H^n$, потому что он не знает автоморфизма $y \cdot \varphi_H^m$.

6) Поскольку $(B, x) \cdot (A, \varphi_H^m) = (A, y) \cdot (B, \varphi_H^n) = (M, \varphi_H)^{(m+n)}$, у нас должен быть $K_{Alice} = K_{Bob} = K$, общий секретный ключ.

В подразделе 1.9 «Вычислительная сложность» описывается вычислительная сложность для объединенного алгоритма. Поскольку стороны фактически вычисляют степени элемента G, они могут использовать метод «возведение в квадрат и умножение», как в стандартном протоколе Диффи–Хеллмана. Таким образом, в любой из рассматриваемых реализаций протокола сложность вычисления $(g, \varphi)^n$ составляет $O(\log(n))$ умножений (полу)группы, так же, как и в стандартном протоколе Диффи–Хеллмана.

В подразделе 1.10 «Параметры и генерация ключей» определяются параметры генерации ключей и приводится пример для генерация обратимой матрицы H.

Также стоит отметить, что всегда существует опасение (также в стандартном протоколе Диффи–Хеллмана) относительно порядка открытого элемента: если порядок слишком мал, то атака методом перебора может быть выполнимой. В этой ситуации эта озабоченность значительно смягчается тем, что передачи представляют собой произведения степеней двух различных матриц, а не степеней одной матрицы. Таким образом, даже если порядок одной из матриц случайно оказывается мал, это не означает, что произведение $H^{-m}(HM)^m$ попадет в цикл маленького размера. Кроме того, поскольку

матрица M необратима, у нее нет «порядка», а скорее цикл: $M^r = M^s$ для некоторых положительных $r \neq s$. Матрицы HM и $H^{-m}(HM)^m$ также необратимы, поэтому у них тоже нет порядка, а только цикл. Обнаружение цикла, в общем, вычислительно гораздо сложнее, чем вычисление порядка обратимого элемента.

В разделе 1.11 «Экспериментальные вычисления» представлены результаты сравнительного анализа производительности операции умножения при различных мощностях матричных полугрупп в групповом кольце $M_n(Z_p[S_m])$ и мультипликативной группы Z_p. Для более наглядного представления построены четыре графика для мощностей платформ, соответствующих значениям 10^3, 10^5, 10^7, 10^{10}.

Мощность платформы вычисляется по формуле $|M_n(Z_p[S_m])| = (p^{m!})^{n^2}$. Также можно вывести формулу оценки временной сложности операции умножения в матричной полугруппе над групповым кольцом $M_n(Z_p(G))$. Так как битовая сложность операции умножения в группе вычетов Z_p равна $O(log^2 p)$, то битовая сложность операции умножения в полугруппе $M_n\left(Z_p(G)\right)$ равна $O(m * log^2 p * n^3)$, где $m = |G|$. В нашем случае G – это симметрическая группа. Вместо симметрической группы можно использовать другие группы небольшой мощности такие как альтернирующая, линейная, циклическая группы.

Сложность операции в классическом алгоритме Диффи–Хеллмана будет равна $O(p^2)$, но значение параметра p будет гораздо больше значения параметров в предлагаемой платформе.

Из этого можем сделать выводы, что преимущество матричной полугруппы над групповым кольцом $M_n(Z_p[S_m])$ над группой вычетов Z_p, используемой в классическом алгоритме Диффи–Хеллмана, заключается в несущественном увеличении времени при значительном увеличении мощности

используемой платформы. Это достигается за счет небольших значений параметров n, m, p.

Во втором разделе «Практическая часть» приведены примеры работы программы, в которой реализованы 3 усложненные версии алгоритма Диффи–Хеллмана. Программа была написана на языке Python в среде разработки PyCharm Community Edition 2021.2. В качестве средства для создания интерфейса использовались библиотеки Tkinter и CustomTkinter. В программе применяется модуль Permutation из библиотеки Sympy.combinatorics для работы с симметричными группами.

Первый алгоритм усложнен автоморфизмом группы. В качестве автоморфизма используется $\varphi(x) = g^{-1}xg$ $(x \in G)$, то есть сопряжение элементом $g \in G$ таким образом, что $g^{-1}hg \neq h$ по крайней мере для некоторого $h \in G$. В качестве платформы используется мультипликативная группа Z_p, как и в классическом алгоритме Диффи–Хеллмана.

Второй алгоритм усложнен использованием отличной структурой от Z_p. В качестве платформы используются полугруппы матриц над групповым кольцом $M_n(Z_p[S_m])$, где пользователи выбирают параметры для генерации платформы, от которых будет зависеть ее мощность. Для повышения эффективности программы заранее производится вычисление произведений элементов S_m и сохранение их в таблице Кэли с целью оптимизации производительности.

Третий алгоритм представляет собой сочетание особенностей первого и второго методов. В его основе лежат полугруппы матриц над групповым кольцом $M_n(Z_p[S_m])$, используемые во втором алгоритме, но с дополнительной сложностью, внесенной функцией сопряжения. Поскольку функция сопряжения при работе с матрицами обладает свойством некоммутативности, она создает дополнительные сложности для потенциальных атак и значительно усиливает уровень криптостойкости системы.

ЗАКЛЮЧЕНИЕ

В теоретической части данной работы описаны усложненные алгоритмы Диффи–Хеллмана и алгебраические структуры, которые для этого используются.

В практической части реализована программа с интерфейсом, которая включает в себя три модификации алгоритма Диффи–Хеллмана, усложненные с помощью таких алгебраических структур, как групповые кольца и матричные полугруппы над групповыми кольцами.