Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
Институт естественных и точных наук
Факультет математики, механики и компьютерных технологий
Кафедра прикладной математики и программирования
Направление подготовки: 09.04.04 Программная инженерия

РАБОТА ПРОВЕРЕНА
Рецензент, доцент каф. МиКМ, д.ф.-м.н.
_____/А.В. Кунгурцева
«____»_____20___г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой, д.ф.-м.н.,
профессор
_____/А.А.Замышляева
«____»_____20___ г.

Модификация протокола Диффи-Хеллмана и оценка его криптостойкости

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ–09.04.04.2020.108.ПЗ ВКР

Руководитель работы, профессор
каф. ПМиП, д.ф.-м.н., доцент
_____/Н.Д. Зюляркина
«____»_____2020 г.

Автор работы
Студент группы ЕТ-225
_____/А.Р. Волосников
«____»_____2020 г.
Нормоконтролер,
ст. преподаватель
_____/Н.С. Мидоночева
«____»_____2020 г.

Челябинск
2020

АННОТАЦИЯ

Волосников А.Р. Модификация протокола Диффи-Хеллмана и оценка ее криптостойкости – Челябинск: ЮУрГУ, ЕТ-225, 43 с., 3 ил., 1 табл., библиогр. список – 14 наим.

Выпускная квалификационная работа выполнена с целью модификации протокола Диффи-Хеллмана.

В первой главе проведен анализ стандартного протокола Диффи-Хеллмана.

Во второй главе разработана модификация протокола Диффи-Хеллмана на основе матричных групп. Так же в главе был разработан алгоритм генерации элементов большого порядка в группе матриц.

В третьей главе рассмотрена программная реализация данной модификации, выбрана среда для ее реализации, представлен код программы и таблица с примерами выведенных матриц и их порядков.

В четвертой главе проведена оценка криптостойкости матричной модификации.

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

IETF (Internet Engineering Task Force) – инженерный совет интернета;

IP – Internet Protocol;

IPSec – Internet Protocol Security;

IKE – протокол генерации ключей;

DHKE – протокол генерации ключей Диффи-Хеллмана;

ЭП – электронная подпись;

ЦП – цифровая подпись;

RSA (Rivest-Shamir-Adleman) – криптографический алгоритм с открытым ключом, основывающийся на сложности факторизации больших целых чисел;

DSA (Digital Signature Algorithm) – криптографический алгоритм с открытым ключом для создания ЭП. Основан на вычислительной сложности взятия логарифмов в конечных полях;

Elgamal (Шифросистема Эль-Гамаля) – криптосистема с открытым ключом, основанная на вычислительной сложности дискретных логарифмов в конечном поле. Криптосистема включает в себя и алгоритм шифрования, и алгоритм ЦП;

Diffie-Hellman (Обмен ключами Диффи-Хелмана) – криптографический протокол, позволяет двум и более абонентам получить общий секретный ключ, используя незащищенный канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования;

ECDSA (Elliptic Curve Digital Signature Algorithm) – алгоритм с открытым ключом для создания ЦП.

ВВЕДЕНИЕ

Развитие средств связи и совершенствование технологий коммуникации приводит к упрощению объединения различных субъектов связи в группы. Например, средства видеонаблюдения, контроля доступа и охранной сигнализации объединяются в единую систему физической защиты помещений; бытовые устройства, объединенные с системой защиты помещений, формируют систему «умный дом»; видеокамеры и радары объединяются в систему «умный город»; ученые, эксперты, специалисты объединяются в группы для обсуждения интересующих вопросов; рядовые пользователи сети Интернет объединяются в группы для общения, игр и т. п. Часто каналы связи, образованные между участниками не защищены физически от вмешательства. Это создает угрозу конфиденциальности и целостности данных, передаваемых по каналам. Для устранения этой угрозы могут применяться криптографические протоколы, базовым среди которых является протокол генерации общего секретного ключа. Возможным способом построения протокола генерации ключа является обобщение использующихся на практике двухточечных протоколов. Такой подход обоснован, например, тем, что для использующихся на практике двухточечных протоколов известны обеспечиваемые этими протоколами свойства безопасности, сформулированные инженерным советом интернета IETF (Internet Engineering Task Force).

1 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Криптографическими методами защиты информации называются специальные методы преобразования информации, результатами которого является недоступность информации без предъявления ключа криптограммы. В настоящее время именно криптографический метод защиты является самым надежным так как охраняется содержание (информация), а не доступ к ней.

Современные криптографические методы защиты информации можно разделить на четыре класса:

– симметричные криптосистемы, в которых для шифрования и дешифрования используется один и тот же ключ;

– криптосистемы с открытым ключом, использующие два ключа – открытый и закрытый (связаны друг с другом математически). Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только ограниченному числу лиц;

– системы электронной подписи (присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения);

– процессы управления ключами (процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями).

1.1 Криптосистемы с открытым ключом

В 1976 г. У. Диффи и М. Хеллман описали криптографические системы с открытым ключом (public key cryptosystem), в основание которых легли методы классической и современной алгебры. Предлагается рассматривать такую систему шифрования и/или электронной подписи, при которой открытый ключ передаётся по незащищенному от вмешательств извне каналу

и далее используется для проверки электронной подписи и для шифрования текста. При этом для создания электронной подписи и для расшифровки сообщения используется закрытый ключ.

В данной схеме шифрование использует открытый ключ, а расшифровывание – закрытый ключ. Расшифровывание без знания секретного ключа практически невозможно. Коммуникация по каналу связи предполагает передачу только одного ключа – открытого. Именно этот факт устраняет необходимость передачи ключа в специальном защищенном канале.

Основными видами асимметричных шифров являются:

– RSA;

– DSA;

– Elgamal;

– Diffie-Hellman;

– ECDSA и др.

Одним из главных преимуществ таких шифров является отсутствие необходимости предварительной передачи секретного ключа по защищённому каналу связи. В данном случае используется пара «закрытый ключ – открытый ключ», значения которых с одной стороны связаны, а с другой стороны вычисление закрытого ключа через открытый практически невозможно.

На практике ассиметричные криптосистемы используются в сочетании с другими алгоритмами. Связано это прежде всего с тем, что в чистом виде они требуют существенных вычислительных ресурсов.

Криптографические системы с открытым ключом применяются в различных стандартах ЦП и сетевых протоколах. Такие криптосистемы строятся путем выбора класса задач, для которого не известен эффективный алгоритм решения и в нем выделяется подзадача, для которой такой алгоритм существует. Далее выбранную задачу маскируют под задачу общего вида и выбирают ключ для шифрования. При этом в качестве секретного ключа

используется информация, позволяющая перевести выбранную задачу в исходный вид.

В данной работе более подробно рассматривается протокол Диффи-Хеллмана.

1.2 Протокол Диффи-Хеллмана

Протокол Диффи-Хеллмана – протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный канал связи. Полученный ключ используется для шифрования и дальнейшего обмена с помощью алгоритмов симметричного шифрования.

Схема открытого распределения ключей, предложенная Диффи и Хеллманом, произвела революцию в мире шифрования, так как убирала основную проблему криптографии – проблему распределения ключей.

В чистом виде алгоритм Диффи-Хеллмана уязвим для модификации данных в канале связи, в том числе для атаки человек посередине, поэтому схемы с использованием этого протокола применяют дополнительные методы односторонней или двусторонней аутентификации.

1.2.1 История создания системы распределения ключей

В 1970 году Мартин Хеллман, молодой профессор, занимавшийся вопросами проектирования электрических систем в Стенфордском университете в Пало-Альто. Хеллман увлекся проблемой в 1968 году, когда работал в IBM в Пенсильвании.

Хеллман рассказывает, что он прозрел после того, как прочитал статьи Клода Шенона по теории информации и криптографии, которые опубликовались в 1948 и 1949 годах. В статьях Шенона вопросы кодирования рассматривались в связи с задачей снижения электростатических помех, мешающих передаче радиосигналов. «Шифрование, - заметил Хеллман, - решает диаметрально противоположную задачу. Вы вносите искажения при помощи ключа. Для того, кто слышит сигнал и не знает ключа, он будет

выглядеть максимально искаженным. Но получатель, которому известен секретный ключ, может убрать эти помехи».

Пока Хеллман искал пути для решения проблемы, некий студент из MIT по имени Уайтфилд Диффи заинтересовался тем же самым. Но поиски Диффи начались значительно раньше. - «Я увлекся шифрованием, когда мне было всего десять лет, - вспоминает он. - У меня был учитель, который посвящал проблеме шифрования буквально целые дни. Я шел домой, а там меня ждали книги по этому предмету. Отец приносил мне их из библиотеки колледжа».

К 1973 году Диффи стал лаборантом и раздражал профессоров Стенфорда по искусственному интеллекту тем, что тратил все время и энергию на шифрование. Наконец, он оставил в покое своего учителя, взял отпуск и, одержимый своей идеей, отправился в путешествие по Восточному и Западному побережьям, где встречался с экспертами по шифрованию и разыскивал редкие манускрипты.

А в это самое время Ральф Меркл, студент Университета Беркли (шт. Калифорния), занимающийся исключительно проектированием электрических систем, бродил по университетскому городку, с мыслями о шифровании.

«Я думал о том, как обеспечить защиту коммуникаций между терминалом и компьютером, - рассказывает Меркл. - Я понял, что, если оба, и терминал, и компьютер, используют случайные числа, восстановить ключ при передаче по открытым линиям связи будет невозможно».

Пытаясь объединить разрозненные идеи по шифрованию данных, Хеллман продолжал искать единомышленников. Однако получилось наоборот: в сентябре 1973 года его нашел Диффи. Их получасовая встреча плавно перешла в обед у Хеллмана, причем разговоры затянулись далеко за полночь.

Хеллман и Диффи начали вместе работать над созданием алгоритма обеспечения защиты транзакций покупки и продажи, выполняемых с домашних терминалов. «Я ломал голову над тем, как получить сообщение и преобразовать его таким образом, чтобы его воспринимали только те, кому

предназначено, а посторонним информация была недоступна, - сказал Диффи. - Затем я понял, что при помощи сертификатов и подписи можно создать сообщение, которое сможет прочитать только один человек».

Хеллман и Диффи сообщили, что первая их статья по теории цифровых подписей вышла в декабре 1975 года. Представлена она была полгода спустя в Нью-Йорке на Национальной компьютерной конференции.

Оставаясь неизвестным для конечных пользователей, открытый ключ использует открытый и секретный ключи для шифрования и дешифрования текста вместе с ЦП, а также для проверки личности того, кто отправил. В его основе лежат сложные математические преобразования.

После Беркли в 1975 году Меркл сформулировал задачу защиты коммуникаций, несвязанную с подписью и сертификатом. Он взялся за решение проблемы распространения открытого ключа, исходя из предпосылки применения смешения случайных чисел. Изучив статью Диффи-Хеллмана, Меркл встретился со вторым, который уговорил Меркла перенести свою работу в Стенфорд.

В 1976 г. Мерклу удалось при помощи Диффи и Хеллмана решить задачу распространения открытого ключа и развить аппарат ЦП. Они создали и запатентовали систему, получившую имя Диффи-Хеллмана. Открытие обеспечило всем троим внимание со стороны средств массовой информации.

Но внимание это улетучилось так же быстро, как и возникло. Изобретатели опередили свое время: задача, которую они решили, еще не была сформулирована.

1.2.2 Система распределение ключей Диффи-Хеллмана

Зарождение криптографии с двумя ключами и криптосистемы с открытым ключом связаны с использованием функции возведения в большую дискретную степень по модулю простого большого числа:

$$f(\mathrm{x}) = \alpha\,\mathrm{x}(mod\ p),$$

где x – целое число. $1 < x < p - 1$, p – k-битовое простое число, α – первообразный корень по модулю p.

Используя эту функцию, учеными была показана возможность построения практически стойких секретных систем, которые не требуют передачи секретного ключа. Система, которую они предложили, получила название метода открытой передачи ключей. В ней каждый абонент выбирает случайным образом секретный ключ x и вырабатывает открытый ключ y соответствующий выбранному секретному ключу, в соответствии с формулой

$$y = \alpha^x (mod\ p).$$

Системой Диффи-Хеллмана называется способ с использованием дискретного возведения в степень для обмена секретными ключами между пользователями сети с применением только открытых сообщений.

Выбирается большое простое число p и соответствующий ему первообразный корень $a < p$.

Для обеспечения стойкости системы открытого шифрования на число p накладывается следующее условие: разложение числа $p - 1$ на множители должно содержать, как минимум, один большой простой множитель; размер числа p должен быть больше или равен 512 бит.

Механизм распределения секретных ключей по открытому каналу состоит в следующем. Каждый абонент выбирает x – случайный секретный ключ и вырабатывает y – открытый ключ, соответствующий выбранному секретному ключу, в соответствии с формулой

$$y = \alpha^x (mod\ p).$$

Два абонента A и B могут установить секретную связь без передачи секретного ключа следующим образом. Абонент A берет из справочника открытый ключ y_B абонента B и, используя свой секретный ключ xA, вычисляет общий секретный ключ:

$$Z_{AB} = (y_B)^{X_A} = (\alpha^{X_B})^{X_A} = \alpha^{X_B X_A} (mod\ p).$$

Аналогично поступает абонент B:

$$Z_{BA} = (y_A)^{X_B} = (\alpha^{X_A})^{X_B} = \alpha^{X_B X_A} (mod\ p).$$

Таким образом, два абонента сформировали одинаковый секретный ключ Z_{AB} не используя какой-либо заранее оговоренный общий секрет. Владея только им, известным секретом и используя его в качестве мастер-ключа, два этих абонента могут зашифровывать направляемые друг другу фразы. Указанные выше вычисления легко осуществимы для достаточно больших значений p, a, y и x (например, имеющих в двоичном представлении длину 4096 бит и более). Атакующему известны значения $y_B = \alpha^{X_B} (mod\ p)$ и $y_A = \alpha^{X_A} (mod\ p)$, но для того, чтобы вычислить Z_{AB}, он должен решить задачу дискретного логарифмирования и определить одно из значений – xA либо xB. Легко найти большие значения p (более 1024 бит), для которых задача дискретного логарифмирования является практически нерешаемой. Если будут найдены вычислительно эффективные методы решения задачи дискретного логарифмирования, то метод Диффи-Хеллмана окажется несостоятельным – поэтому говорят, что данный метод основан на сложности дискретного логарифмирования. В настоящее время задача дискретного логарифмирования практически неразрешима. Это дает возможность широкого применения алгоритма Диффи-Хеллмана и многочисленных систем ЦП, основанных на сложности вычисления дискретных логарифмов.

Не следует забывать про проблему аутентификации открытых ключей. Корректность протоколов с использованием асимметричных шифров может быть обеспечена только в случае, если все открытые ключи в справочнике являются подлинными. Если открытый ключ одного из абонентов нарушителю удастся подменить, то секретные сообщения, посланные данному абоненту, будут доступны и нарушителю.

Таким образом, шифры с двумя ключами обеспечивают решение проблемы распределения секретных ключей, однако проблема аутентификации сохраняется и имеет фундаментальный характер, хотя

требование подтверждения подлинности (аутентификации) относится уже к открытому, а не к секретному ключу. В неявном виде аутентификация открытого ключа включает в себя аутентификацию секретного ключа.

1.3 Классический протокол Диффи-Хеллмана

Предположим, существует два абонента: Алиса и Боб. Этим абонентам известны некоторые два числа g и p, которые не являются секретными и могут быть известны также другим заинтересованным лицам. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют случайные числа: Алиса – число a, Боб – число b. Затем Алиса вычисляет остаток от деления:

$$A = g^a \, mod \, p$$

и пересылает его Бобу, затем Боб вычисляет остаток от деления:

$$B = g^b \, mod \, p$$

и передаёт Алисе. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их (то есть, у него нет возможности вмешаться в процесс передачи).

На втором этапе Алиса на основе имеющегося у неё a и полученного по сети B вычисляет значение:

$$B^a \, mod \, p = g^{ab} \, mod \, p.$$

Боб на основе имеющегося у него b и полученного по сети A вычисляет значение:

$$A^b \, mod \, p = g^{ab} \, mod \, p.$$

У Алисы и Боба получилось одно и то же число:

$$K = g^{ab} \, mod \, p.$$

Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой (за разумное время) проблемой вычисления по перехваченным $g^a \, mod \, p$ и $g^b \, mod \, p$, если

числа p, a, b выбраны достаточно большими. Работа алгоритма показана на рисунке 1.

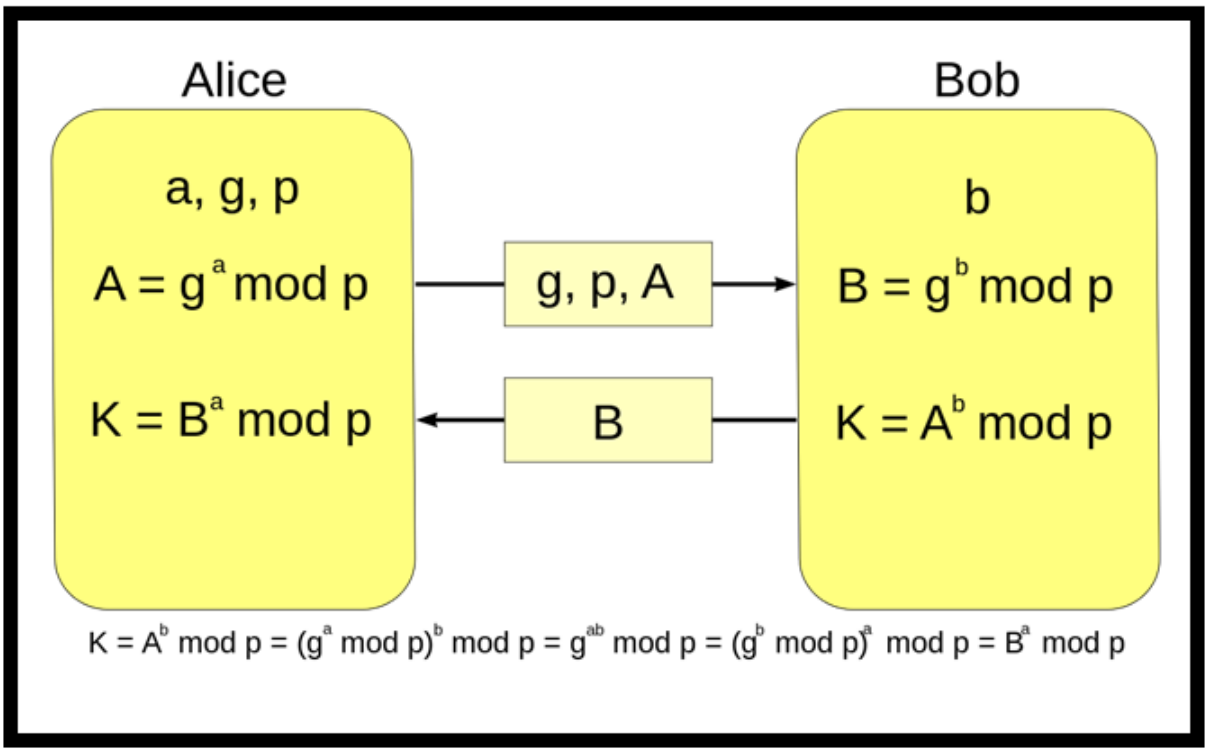

Рисунок 1 – Алгоритм Диффи-Хеллмана,
где K – итоговый общий секретный ключ

1.3.1 Алгоритм работы протокола

При работе алгоритма каждая сторона:

- генерирует случайное натуральное число a, которое является закрытым ключом;
- вместе со второй стороной устанавливаются открытые параметры p и g (обычно значения p и g генерируются на одной стороне и передаются другой), где p – случайное простое число, $(p-1)/2$ также должно быть случайным простым числом (для повышения безопасности), g является первообразным корнем по модулю p (также является простым числом);
- вычисляет открытый ключ A, используя преобразование над закрытым ключом: $A = g^a \, mod \, p$;
- обе стороны обмениваются открытыми ключами друг с другом;

• вычисляет общий секретный ключ K, используя открытый ключ удаленной стороны B и свой закрытый ключ a: $K = B^a \, mod \, p$, К получается равным с обеих сторон, потому что: $B\hat{}a \, mod \, p \; = \; (g\hat{}b \, mod \, p)\hat{}a \, mod \, p \; = \; g\hat{}(ab) \, mod \, p \; = \; (g\hat{}a \, mod \, p)\hat{}b \, mod \, p \; = \; A\hat{}b \, mod \, p$.

В практических реализациях для a и b используются числа порядка 10^{100} и p порядка 10^{300}. Число g не обязано быть большим и обычно имеет значение в пределах первого десятка.

1.3.2 Криптографическая стойкость

Криптографическая стойкость алгоритма Диффи-Хеллмана – это сложность вычисления $K = g^{ab} \, mod \, p$ по известным $p, g, A = g^a \, mod \, p$ и $B = = g^b \, mod \, p$, которая основывается на сложности задачи дискретного логарифмирования.

Протокол Диффи-Хеллмана отлично противостоит пассивному нападению, но в случае реализации атаки «человек посередине» он не устоит. В самом деле, в протоколе ни Алиса, ни Боб не могут точно определить, кем является их собеседник, поэтому вполне возможно представить случай, при котором Боб и Алиса установили связь с Меллори, который Алисе выдает себя за Боба, а Бобу представляется Алисой.

1.4 Протокол Диффи-Хеллмана на эллиптических кривых

Протокол Ди́ффи-Хеллмана на эллиптических кривых – криптографический протокол, позволяющий двум сторонам, имеющим пары открытый/закрытый ключ на эллиптических кривых, получить общий секретный ключ, используя незащищённый от прослушивания канал связи. Этот секретный ключ может быть использован как для шифрования дальнейшего обмена, так и для формирования нового ключа, который затем может использоваться для последующего обмена информацией с помощью

алгоритмов симметричного шифрования. Это вариация протокола Диффи-Хеллмана с использованием эллиптической криптографии.

1.4.1 Алгоритм работы протокола

Пусть существуют два абонента: Алиса и Боб. Предположим, Алиса хочет создать общий секретный ключ с Бобом, но единственный доступный между ними канал может быть подслушан третьей стороной. Изначально должен быть согласован набор параметров (p, a, b, G, n, h) для общего случая и $(m, f(x), a, b, G, n, h)$ для поля характеристики 2). Так же у каждой стороны должна иметься пара ключей, состоящая из закрытого ключа d (случайно выбранное целое число из интервала $[1, n-1]$ и открытого ключа Q (где $Q = = d * G\}$ – это результат проделывания d раз операции суммирования элемента G. Пусть тогда пара ключей Алисы будет (dA, QA), а пара Боба (dB, QB). Перед исполнением протокола стороны должны обменяться открытыми ключами.

Алиса вычисляет $(x_k, y_k) = d_A \cdot Q_B$. Боб вычисляет $(x_k, y_k) = d_B \cdot Q_A$. Общий секрет – xk (x – координата получившейся точки). Большинство стандартных протоколов, базирующихся на ECDH, используют функции формирования ключа для получения симметричного ключа из значения xk.

Вычисленные участниками значения равны, так как $d_A \cdot Q_B = d_A \cdot d_B \cdot G = d_B \cdot d_A \cdot G = d_B \cdot Q_A$. Из всей информации, связанной со своим закрытым ключом, Алиса сообщает только свой открытый ключ. Таким образом никто, кроме Алисы, не может определить её закрытый ключ, кроме участника, способного решить задачу дискретного логарифмирования на эллиптической кривой. Закрытый ключ Боба аналогично защищён. Никто, кроме Алисы или Боба, не может вычислить их общий секрет, кроме участника, способного разрешить проблему Диффи-Хеллмана.

Открытые ключи бывают либо статичными (и подтверждённые сертификатом) либо эфемерные (сокращённо ECDHE). Эфемерные ключи

используются временно и не обязательно аутентифицируют отправителя, таким образом, если требуется аутентификация, подтверждение подлинности должно быть получено иным способом. Аутентификация необходима для исключения возможности атаки посредника. Если Алиса либо Боб используют статичный ключ, опасность атаки посредника исключается, но не может быть обеспечена ни прямая секретность, ни устойчивость к подмене при компрометации ключа, как и некоторые другие свойства устойчивости к атакам. Пользователи статических закрытых ключей вынуждены проверять чужой открытый ключ и использовать функцию формирования ключа на общий секрет, чтобы предотвратить утечку информации о статично закрытом ключе. Для шифрования с другими свойствами часто используется протокол MQV.

При использовании общего секрета в качестве ключа зачастую желательно хешировать секрет, чтобы избавиться от уязвимостей, возникших после применения протокола.

1.5 Схема быстрой ЭЦП, основанная на алгоритме Диффи-Хеллмана

Быстрая цифровая подпись – вариант цифровой подписи, использующий алгоритм с гораздо меньшим (в десятки раз) числом вычислений модульной арифметики по сравнению с традиционными схемами ЭЦП. Схема быстрой электронной подписи, как и обычная, включает в себя алгоритм генерации ключевых пар пользователя, функцию вычисления подписи и функцию проверки подписи.

Пусть G – абелева группа, $G_{\mathrm{q,k}}$ – её циклическая подгруппа с генератором g порядка q, где q – большое простое число. Пусть lg и lp – параметры безопасности, причём $l_q = |q|$. Пусть $H: \{0,1\}^* \to G_{g,q}$, $L: \{0,1\}^* \to$ $\to Z_q^*$ и $G: \{0,1\}^* \to Z_q^*$ – хеш-функции. Схема подписи представляет собой следующее:

- генерация ключа:

пользователь выбирает случайный секретный ключ $x \in z_q^*$ и вычисляет открытый ключ $y = g_x$.

• создание подписи:

входными данными являются секретный ключ $x \in z_q^*$ и сообщение $x \in \{0,1\}^*$.

Далее сторона, создающая подпись:

1. Выбирает случайное число $k \in z_q^*$ и случайный бит $\mathrm{b_m} \in \{0,1\}$;

2. Вычисляет $h = H(m, b_m)$;

3. Вычисляет $u = h^x$;

4. Вычисляет $v = (g^n \cdot h)^k$, где $n = L(m, g, h, y, u)$;

5. Вычисляет $r = G = (m, g, h, y, u, v)$;

6. Вычисляет $s = k - xr \, mod \, q$.

Подписью сообщения m является $\sigma = (u, r, s, b_m)$.

• проверка подписи:

чтобы проверить подпись σ сообщения m, делается следующее:

1. σ представляется как (u, r, s, b_m);
2. Вычисляется $h = H(m, b_m)$ и $n = L(m, g, h, y, u)$;
3. Вычисляется $v' = (g^n \cdot h)^s \cdot (y^n \cdot u)^r$;
4. Проверяется, выполняется ли $r = G = (m, g, h, y, u, v')$.

Если равенство на шаге 4 выполняется, подпись проходит проверку.

1.6 Вывод по первой главе

В результате проведенного анализа, была выполнена следующая работа:

• анализ и описание классического алгоритма Диффи-Хеллмана;

• анализ существующих модификаций;

• описание алгоритма оценки криптографической стойкости алгоритма.

2 МОДИФИКАЦИЯ ПРОТОКОЛА ДИФФИ-ХЕЛЛМАНА

2.1 Описание модификации

Суть работы модифицированного алгоритма шифрования сводится к следующему. Абоненты Алиса (A) и Боб (B) выбирают матрицу большого порядка над кольцом вычетов Z_n. Эта матрица является общедоступной. Независимо друг от друга абоненты A и B вырабатывают секретные случайные числа x и y соответственно. x и y в диапазоне от 2 до $|M| - 1$. Абонент A вычисляет матрицу $A = M^x$ и посылает ее Бобу, который, в свою очередь, вычисляет матрицу $B = M^y$ и посылает ее Алисе. Далее каждый из абонентов A и B возводит полученные матрицы в свои секретные степени x и y. В результате выполненных операций Алиса приобретает секретную матрицу зашифрования $K = B^x = M^{xy}$, а Боб – матрицу расшифрования $K = A^x = M^{xy}$.

С целью противодействия атаке типа «человек посередине» в модифицированном DH-алгоритме предлагаются следующие меры. Как известно, в системах криптографической защиты данных желательно не допускать легко устанавливаемой зависимости между последовательно используемыми ключами (в рассматриваемом алгоритме – матрицами) шифрования. С этой целью представляется целесообразным обновлять матрицы шифрования K после некоторого фиксированного или согласованного между абонентами A и B вариативного периода (сеанса) передачи данных по правилу $K = K \cdot MZ$, где $MZ = M^z$, причем z − секретное случайное натуральное число, вырабатываемое абонентом A. Аналогично осуществляется модификация матрицы расшифрования K.

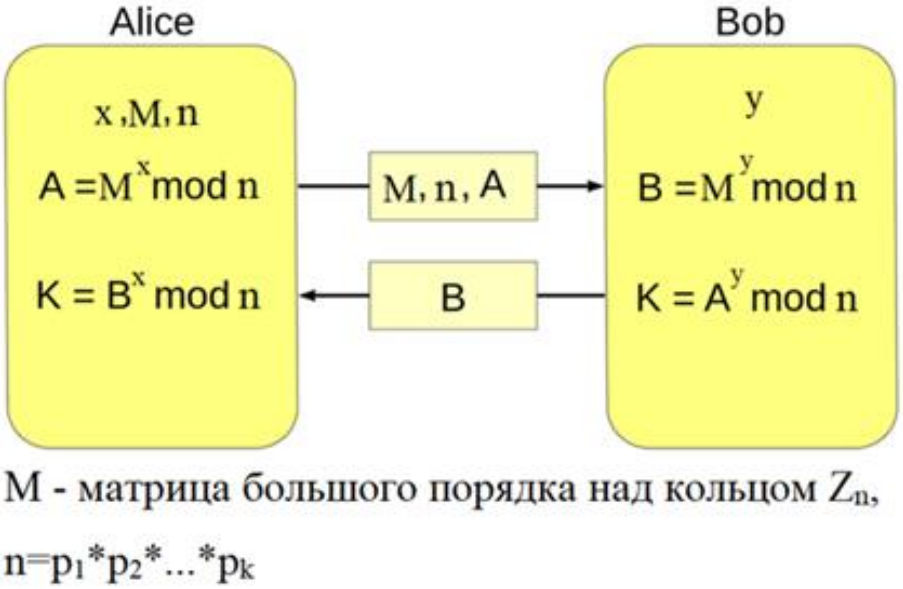

Рисунок 2 – Модифицированный алгоритм Диффи-Хеллмана,
где K – итоговый общий секретный ключ

2.2 Матрицы больших порядков над кольцами вычетов $GL_m(Z_n)$

2.2.1 Порядок группы $GL_m(Z_n)$

Пусть K – это коммутативное кольцо с единицей. Обозначим через $M_m(K)$ – кольцо квадратных матриц размера m с элементами из K, а через $GL_m(K)$ множество обратимых элементов этого кольца. Заметим, что $GL_m(K)$ является группой относительно умножения матриц.

Если кольцо K является полем, то элемент из $M_m(K)$ будет обратим тогда и только тогда, когда его определитель отличен от нуля. Если в качестве K выбрано кольцо вычетов Z_n, то матрица из $M_m(K)$ будет обратима тогда и только тогда, когда её определитель обратим в Z_n.

Из курса линейной алгебры известно, что матрица $A \in M_n(Z_p)$ обратима тогда и только тогда, когда ее столбцы линейно независимы. Поэтому нам нужно посчитать количество $n \times n$ матриц с линейно независимыми столбцами. В обратимой матрице, первый столбец может быть любым, но не нулевым. Таким образом, число возможных вариаций первого столбца равно $p^n - 1$. После того, как первый столбец выбран, второй столбец

также может быть любым, но не повторять первый. Тогда возможные варианты второго столбца $p^n - p$. После того, как первый и второй столбец выбраны, выбираем третий столбец, но при этом не должен быть одинаковым с первым и вторым. Таким образом, количество возможных вариантов третьего столбца $p^n - p^2$. Продолжая подобным образом, получим что для $(k+1)$ колонки число возможных вариантов будет $p^n - p^k$.

Следовательно, общее число обратимых матриц в $M_n\ (Z_p)$ определяется по формуле:

$$\left|GL\ (n, Z_p)\right| = (p^n - 1)(p^n - p)(p^n - p^2)\ \ldots\ (p^n - p^{n-1}).$$

В частности,

$$|GL\ (2, Z_2)| = 3 \times 2 = 6,$$

$$|GL\ (2, Z_3)| = 8 \times 6 = 48,$$

$$|GL\ (3, Z_2)| = 7 \times 6 \times 4 = 168.$$

Теорема. Пусть $G = GL_n(Z_m)$, где $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$.

Тогда $G \cong GL_n\left(Z_{p_1^{k_1}}\right) \times GL_n\left(Z_{p_2^{k_2}}\right) \times \ldots \times GL_n\left(Z_{p_s^{k_s}}\right)$.

Доказательство.

Пусть элемент $g \in G$, $g_1 \in GL_n\left(Z_{p_1^{k_1}}\right), g_2 \in GL_n\left(Z_{p_2^{k_2}}\right), \ldots, g_s \in GL_n\left(Z_{p_s^{k_s}}\right)$,

Где элементы $g_1, g_2, \ldots, g_s$ определяются исходя из равенств:

$$g_1 = g(mod\ p_1^{k_1})\ldots$$

$$g_s = g(mod\ p_s^{k_s}).$$

Докажем, что $\varphi: g \to (g_1, g_2, \ldots, g_s)$ является биекцией.

Инъекция очевидна.

Докажем сюръекцию.

Пусть $(g_1, g_2, \ldots, g_s) \in GL_n\left(Z_{p_1^{k_1}}\right) \times GL_n\left(Z_{p_2^{k_2}}\right) \times \ldots \times GL_n\left(Z_{p_s^{k_s}}\right)$.

Тогда по китайской теореме об остатках существует единственный элемент $g \in G$, для которого $\varphi(g) = (\mathrm{g}_1, \mathrm{g}_2, \ldots, \mathrm{g}_s)$.

Проверим сохранение операции:

Пусть $g, g' \in G$, $gg' = g''$:

$$\varphi(g) = (g_1, g_2, \dots, g_s),$$
$$\varphi(g') = (g_1', g_2', \dots, g_s'),$$
$$\varphi(g'') = (g_1'', g_2'', \dots, g_s'').$$

Так как по определению выполняются равенства

$$g_i = g(mod\ p_i^{k_i}),$$
$$g_i' = g'(mod\ p_i^{k_i}),$$
$$g_i'' = g''(mod\ p_i^{k_i}),$$
$$g_i'' = gg'(mod\ p_i^{k_i}),$$

то

$$\varphi(g \cdot g') = \varphi(g) \cdot \varphi(g').$$

Следствие. Порядок группы $G = GL_n(Z_m)$, $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_s^{k_s}$ определяется по формуле:

$$|G| = \left|GL_n\left(Z_{p_1^{k_1}}\right)\right| \cdot \left|GL_n\left(Z_{p_2^{k_2}}\right)\right| \cdot \dots \cdot \left|GL_n\left(Z_{p_s^{k_s}}\right)\right|.$$

2.2.2 Порядок элементов в группе $GL_m(Z_n)$

Порядком элемента в группе называется такое наименьшее натуральное m, что $g^m = e$. Если такого m не существует, то порядок считается равным бесконечности.)

Обозначим через $w(G)$ множество порядков элементов группы G.

Порядки элементов группы $PGL_n(q)$, где q – примарное число, описывает следующая теорема.

Теорема. Пусть $G = PGL_n(q)$, где $n \geq 2$, q – степень простого числа p. Положим $d = (n, q-1)$. Тогда $w(G)$ состоит из всех делителей следующих чисел:

1) $\frac{\mathrm{q^n - 1^n}}{\mathrm{q-1}}$;

2) $[q^{n_1}-1,\ q^{n_2}-1,\dots,q^{n_s}-1]$ для любых $s\geq 2$ и $n_1,n_2,\dots,n_s>0$, таких, что $n_1+\ n_2+\ \dots+n_s=n$;

3) $p^k[q^{n_1}-1,\ q^{n_2}-1,\dots,q^{n_s}-1]$ для любых $s\geq 1\ и\ k,n_1,n_2,\dots,n_s>0$, таких, что

$p^{k-1}\ +\ 1+\ n_1+\ n_2+\ \dots+n_s=n$;

4) p^k , если $p^{k-1}\ +\ 1=n$ для $k\ >\ 0$.

Если известны порядки элементов в факторгруппе, то можно получить оценку для порядков элементов исходной группы с помощью следующей теоремы.

Теорема. Пусть G – конечная группа, N – нормальная подгруппа группы G, $|N|\ =\ d$, $\bar{G}=G/N$ – факторгруппа группы G.

$x\in G$, $\bar{x}$ – соответствующий ему элемент из $\bar{G}$ $(\bar{x}\ =\ xN)$.

Пусть $|\bar{x}|_{\bar{G}}=k$. Тогда $|x|_G\leq kd$.

Доказательство.

Пусть $|x|\ =\ m$, а порядок элемента $\bar{x}$ равен k. Тогда $\bar{x}^k\ =\ e_{\bar{G}}$, и $x^k\in N$.

Обозначим за d порядок подгруппы N. Тогда $(x^k)^d=e$.

Из равенства $x^{kd}=e$ следует, что $kd\geq m$, так как m – порядок элемента x, значит $|x|_G\leq kd$, что и требовалось доказать.

Для нахождения элементов больших порядков в группе $GL_n(Z_m)$, где $m=p_1^{k_1}\cdot p_2^{k_2}\cdot\dots\cdot p_s^{k_s}$ достаточно иметь информацию об элементах больших порядков в группах $GL_n\left(Z_{p_1^{k_1}}\right),GL_n\left(Z_{p_2^{k_2}}\right),\dots,GL_n\left(Z_{p_s^{k_s}}\right)$.

Теорема. Пусть $G=GL_n(Z_m)$, $m=p_1^{k_1}\cdot p_2^{k_2}\cdot\dots\cdot p_s^{k_s}$, $G_1=GL_n\left(Z_{p_1^{k_1}}\right),G_2=GL_n\left(Z_{p_2^{k_2}}\right),\dots,G_s=GL_n\left(Z_{p_s^{k_s}}\right),G=G_1\times\dots\times G_s$.

$$g\in G,g=g_1\cdot\dots\cdot g_s,\ g_i\in G_i\,.$$

Тогда $|g|_G=\text{НОК}\left(|g_1|_{G_1},|g_2|_{G_2},\dots,|g_s|_{G_s}\right)$.

2.3 Алгоритм генерации элементов большого порядка в группе матриц

Теорема. В группе $G = GL_n(Z_m)$, $m = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ существует элемент порядка НОК $(p_1^n - 1, p_2^n - 1, \ldots, p_s^n - 1)$.

Доказательство.

Представим группу $G = GL_n(Z_m)$ в виде:

$$G = GL_n(p_1) \times GL_n(p_2) \times \ldots \times GL_n(p_s).$$

Рассмотрим первую группу $GL_n(p_1)$.

Пусть $f(x)$ – примитивный многочлен степени n над полем F_{p_1} ($f(x)$ является минимальным многочленом примитивного элемента α из поля $\mathrm{F}_{\mathrm{p_1}^{\mathrm{n}}}$).

Допустим, что $f(x)$ является характеристическим многочленом линейной рекуррентной последовательности. Тогда: $f(x) = x^n - a_{n-1}x^{n-1} - \ldots - a_1 x - a_0$, где $a_0 \neq 0$.

Пусть матрица последовательности A над F_{p_1} имеет вид:

$$\mathrm{A} = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & \mathrm{a}_0 \\ 0 & 1 & 0 & \cdots & 0 & \mathrm{a}_1 \\ 0 & 0 & 1 & \cdots & 0 & \mathrm{a}_2 \\ \cdots & \cdots & \cdots & \cdots & 0 & \cdots \\ 0 & 0 & 0 & \cdots & 1 & \mathrm{a}_{n-1} \end{bmatrix}.$$

Рассмотрим линейную рекуррентную последовательность с характеристическим многочленом $f(x)$, являющуюся импульсной функцией.

Тогда, по теореме, доказанной в [10], период $r = ord\, f(x) = {p_1}^n - 1$.

С другой стороны, r делит $|A|$ следовательно $|A|$ делится на ${p_1}^n - 1$.

Следовательно, $|A| = {p_1}^n - 1$.

Таким образом в группе $GL_n(p_1)$ существует элемент порядка $p_1^n - 1$.

Рассмотрим вторую группу $GL_n(p_2)$ в которой существует элемент порядка $p_1^n - 1$.

Проводя подобные действия получаем, что в группе $GL_n(p_2)$ существует элемент порядка $p_2^n - 1$.

Рассматривая всю группу $G = GL_n(p_1) \times GL_n(p_2) \times \ldots \times GL_n(p_s)$, получаем что для каждой подгруппы существует элемент порядка $p_s^n - 1$.

Тогда для всей группы G существует элемент порядка НОК $(p_1^n - 1, p_2^n - 1, \dots, p_s^n - 1)$.

Пример. Рассмотрим группу $GL_3(15)$ и найдем в ней элемент порядка НОК $(33 - 1, 53 - 1) = 1612$. Для этого построим элементы x_1 и x_2 в группах $GL_3(3)$ и $GL_3(5)$ соответственно, которые имеют порядки $3^3 - 1$ и $5^3 - 1$. Рассмотрим примитивный многочлен $f(x) = x^3 + 2x + 1$ над Z_3 и примитивный многочлен $g(x) = x^3 + 4x + 3$ над Z_5. Этим многочленам в группах $GL_3(3)$ и $GL_3(5)$ будет соответствовать матрица $\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Её и возьмём в качестве искомого элемента x. С помощью сопряжения можно усложнить вид полученного элемента. Пусть $y = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 7 & 2 \\ 0 & 0 & 4 \end{pmatrix}$. Тогда в $GL_3(15)$ найдем элемент $z = x^y$. Получим, что $z = \begin{pmatrix} 4 & 11 & 11 \\ 13 & 3 & 7 \\ 0 & 13 & 8 \end{pmatrix}$.

Как и исходный элемент x полученный элемент z будет иметь порядок 1612.

Теорема. В группе $GL_{2^m}(Z_m)$, $m = p_1 \cdot p_2 \cdot \dots \cdot p_s$ существует элемент x порядка НОК $(p_1^n - 1, p_2^n - 1, \dots, p_s^n - 1)$.

Доказательство.

Представим группу $G = GL_{2^m}(Z_m)$ в виде:

$$G = GL_{2^m}(p_1) \times GL_{2^m}(p_2) \times \dots \times GL_{2^m}(p_s).$$

В каждой из подгрупп найдем элементы $x_1 \in GL_{2^m}(p_1), x_2 \in GL_{2^m}(p_2) \dots x_s \in GL_{2^m}(p_s)$ порядка $q^{\,m} - 1$, где $q = (p_1, p_2, \dots, p_s)$.

Найдем элемент x_1 в подгруппе $GL_{2^m}(p_1)$,

Выберем $\alpha \in F_{p_1}$, такое, что $\alpha^2 \notin \mathrm{F}_{\mathrm{p}_1}^2$, и $\omega \in GL_{2^m}(p_1)$ следующего вида

$$\omega = \begin{pmatrix} 0 & \dots & 0 & \alpha & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \cdots & 0 & 0 & \cdots & \alpha \\ 1 & \vdots & 0 & 0 & \vdots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \cdots & 1 & 0 & \cdots & 0 \end{pmatrix}.$$

Централизатор ω изоморфен $GL_{2^{m-1}}({p_1}^2)$.

Таким образом, показано, что группа $GL_{2^m}(p_1)$ содержит подгруппу $GL_{2^{m-1}}({p_1}^2)$. Используя доказанное вложение, построим цепочку подгрупп:

$$GL_{2^m}(p_1) \geqslant GL_{2^{m-1}}({p_1}^2) \geqslant GL_{2^{m-2}}({p_1}^4) \geqslant \cdots \; GL_1({p_1}^m - 1) \simeq F^*_{{p_1}^m},$$

где

$$C_{GL_{2^m}(p_1)}(\omega) = \left\{ g = \begin{pmatrix} A & \alpha B \\ B & A \end{pmatrix} \mid det\, g \neq 0;\; A, B \in M_{2^{m-1} \times 2^{m-1}}(p_1) \right\}.$$

Так как группа $F^*_{{p_1}^m}$ – циклическая, то в ней существует порождающий элемент x. Порядок элемента x равен ${p_1}^m - 1$. Этому элементу в исходной группе будет соответствовать элемент g, $|g| = {p_1}^m - 1$.

Повторяя действие, в каждой из подгрупп найдем элементы $x_1 \in GL_{2^m}(p_1), x_2 \in GL_{2^m}(p_2) \dots x_s \in GL_{2^m}(p_s)$ порядка ${q}^m - 1$, где $q = (p_1, p_2, \dots, p_s)$.

По китайской теореме об остатках:

Для любого $x_1 \in GL_{2^m}(p_1), x_2 \in GL_{2^m}(p_2) \dots x_s \in GL_{2^m}(p_s)$ существует единственный элемент $x \in GL_{2^m}(p_1 \cdot p_2 \cdot \dots \cdot p_s)$, такой что

Причем,

$$x \equiv x_1 (mod\ p_1),$$
$$x \equiv x_2 (mod\ p_2),$$
$$\dots$$
$$x \equiv x_s (mod\ p_s).$$

Следовательно порядок элемента вычисляется по формуле

$$|x|_{GL_{2^m}(p_1 \cdot p_2 \cdot \dots \cdot p_s)} = \text{НОК}\left(|x_1|_{GL_{2^m}(p_1)}, \dots, |x_s|_{GL_{2^m}(p_s)}\right).$$

Пример. Рассмотрим группу $GL_2(143)$ и найдем в ней элемент порядка $HOK(11^2 - 1, 13^2 - 1) = 840$. Для этого построим элементы $x1$ и $x2$ в группах $GL_2(11)$ и $GL_2(13)$ соответственно, которые имеют порядки $11^2 -$

1 и $13^2 - 1$. Для этого найдем примитивные элементы в полях F_{121} и F_{169}. Поле F_{121} можно построить, используя многочлен $f(x) = x^2 + 1$, а поле F_{169} можно построить с помощью многочлена $f(x) = x^2 + 11$. Примитивными элементами в них будут $2 + 3\beta$ и $3 + 5\beta$, где β корень соответствующего многочлена. Этим элементам соответствуют матрицы $\begin{pmatrix} 2 & 3 \\ 8 & 2 \end{pmatrix}$ и $\begin{pmatrix} 3 & 5 \\ 10 & 3 \end{pmatrix}$ в группах $GL_2(11)$ и $GL_2(13)$. Используя китайскую теорему об остатках, находим требуемый элемент x из группы $GL_2(143)$. Он будет иметь вид $\begin{pmatrix} 68 & 135 \\ 140 & 68 \end{pmatrix}$. Непосредственная проверка показывает, что $|x| = 840$.

Отметим, что предложенные методы построения элементов большого порядка связаны с задачей нахождения примитивных многочленов и примитивных элементов конечных полей.

2.4 Вывод по второй главе

В результате анализа классического протокола Диффи-Хеллмана был разработан модифицированный матричный протокол Диффи-Хеллмана.

Модификация заключается в применении матричных групп над кольцами вычетов, для этого:

1) производится факторизация числа n;

2) $n = p_1 \cdot p_2 \cdot \ldots pk, pi$ – простое число;

3) в группах $GL_m(p_1)$, $GL_m(p_2)$, …, $GL_m(p_k)$ находятся матрицы $\mathrm{GL_m(p_1)}$, имеющие большой порядок;

4) с помощью Китайской теоремы об остатках находится матрица A большого порядка над кольцом Zn:

$$A = A_1(mod\ p1),\ A = A_2(mod\ p2),\ \ldots,\ A = A_k(mod\ p_k);$$

5) на основе получившейся матрицы A производится модификация протокола Диффи-Хеллмана.

3 ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МОДИФИКАЦИИ

3.1 Описание средств разработки

Проект реализован с помощью системы GAP, позволяющая производить вычисления с гигантскими числами, их допустимые значения ограничены только объемом доступной памяти. Далее, система работает с разного вида полями, p-адическими числами, многочленами от многих переменных, рациональными функциями, векторами и матрицами. Пользователю доступны различные функции, например элементарные теоретико-числовые функции, разнообразные функции для работы с множествами и списками и многие другие.

Группы могут быть заданы в различной форме, например, как группы подстановок, матричные группы, группы, заданные порождающими элементами и определяющими соотношениями. Более того, построив, например, групповую алгебру, можно вычислить ее мультипликативную группу, и даже задать ее подгруппу, порожденную конкретными обратимыми элементами групповой алгебры. Ряд групп может быть задан непосредственным обращением к библиотечным функциям (например, симметрическая и знакопеременная группы, группа диэдра, циклическая группа и др.).

Функции для работы с группами включают определение порядка группы, вычисление классов сопряженных элементов, центра и коммутанта группы, верхнего и нижнего центрального рядов, ряда коммутантов, Силовских подгрупп, максимальных подгрупп, нормальных подгрупп, решеток подгрупп, групп автоморфизмов, и т. д. Для ряда конечных групп доступно определение их типа изоморфизма.

Теория представлений групп также входит в область применения системы GAP. Здесь имеются инструменты для вычисления таблиц характеров конкретных групп, действий над характерами и интерактивного построения

таблиц характеров, определения теоретико-групповых свойств на основании свойств таблицы характеров группы. Модулярные представления групп (т.е. представления над полем, характеристика которого делит порядок группы) также могут быть исследованы с помощью GAP.

3.2 Код программы

```
k:=2;
q:=12673;
w:=Factors(q);
e:=Length(w);
a:=[];
j:=[];
o:=[];
for i in [1..e] do
a[i]:=GL(k,w[i]);
od;
for l in [1..e] do
y:=a[l];
t:=ConjugacyClasses(y);
h:=1;
for i in t do
p:=Elements(i);
if Order(p[1])>h then
h:=Order(p[1]);
o[l]:=Order(p[1]);
j[l]:=p[1];
fi;
od;
od;
```

```
L:=Lcm(o);
v:=[];
for i in [1..e] do
v[i]:=[];
for l in [1..k] do
v[i][l]:=[];
for u in [1..k] do
v[i][l][u]:=Int(j[i][l][u]);
od;
od;
od;
z:=[];
for i in [1..k] do
z[i]:=[];
for l in [1..k] do
r:=[];
for u in [1..e] do
r[u]:=v[u][i][l];
od;
z[i][l]:=ChineseRem(w,r);
od;
od;
x:=5;
y:=3;
A:=z^x;
B:=z^y;
KA:=B^x mod q;
KB:=A^y mod q;
Print("Размерность матрицы:"," ",k,"x",k,"\n");
Print("Факторы введённого вами числа q=",w,"\n");
```

Print("Матрицы в полях равных факторам:"," ",v[1],",", v[2],",", v[3],"\n");

Print("Открытый ключ:",z,"\n");

Print("Порядок матрицы:"," ",L,"\n");

Print("Закрытый ключ x и y соответственно:"," ",x," ","и"," ",y,"\n");

Print("Общий закрытый ключ K=",KA,"\n");

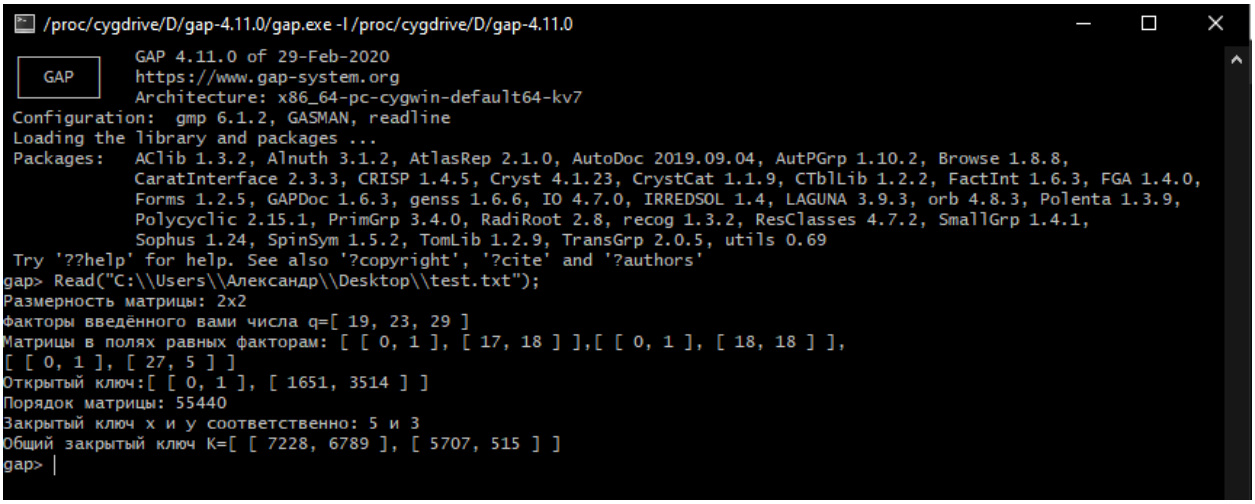

Рисунок 3 – Результат выполнения кода,
где $KA = KB = K$ – общий секретный ключ

3.3 Матрицы наибольших порядков над кольцами вычетов

Таблица 1 – Матрицы наибольших порядков над кольцами вычетов

Размерность матрицы m	n	Матрица наибольшего порядка над Z_n	Порядок матрицы
1	2	3	4
2	19	$\begin{pmatrix} 0 & 1 \\ 17 & 18 \end{pmatrix}$	360
2	23	$\begin{pmatrix} 0 & 1 \\ 18 & 18 \end{pmatrix}$	528

Продолжение таблицы 1

1	2	3	4
2	29	$\begin{pmatrix} 0 & 1 \\ 27 & 5 \end{pmatrix}$	840
2	7	$\begin{pmatrix} 0 & 1 \\ 4 & 6 \end{pmatrix}$	48
2	11	$\begin{pmatrix} 0 & 1 \\ 9 & 7 \end{pmatrix})$	120
3	5	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 2 & 1 & 3 \end{pmatrix}$	124
3	3	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}$	26
2	567	$\begin{pmatrix} 0 & 1 \\ 31 & 458 \end{pmatrix}$	1440
2	1025	$\begin{pmatrix} 0 & 1 \\ 158 & 194 \end{pmatrix}$	1680
2	12673	$\begin{pmatrix} 0 & 1 \\ 1651 & 3514 \end{pmatrix}$	55440
2	1001	$\begin{pmatrix} 0 & 1 \\ 284 & 909 \end{pmatrix}$	1680

3.4 Вывод по третьей главе

В качестве средств разработки была выбрана система GAP. В данной главе:

- написана программа, реализующая модифицированный алгоритм;
- проведены расчеты для некоторого количества матриц размерности m в поле n;
- выведены матрицы наибольшего порядка в этих кольцах; представлен их порядок.

4 ОЦЕНКА КРИПТОСТОЙКОСТИ МАТРИЧНОЙ МОДИФИКАЦИИ

4.1 Методы дискретного логарифмирования

Дискретное логарифмирование – задача обращения функции g^x в некоторой конечной мультипликативной группе G.

Наиболее часто задачу дискретного логарифмирования рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. Эффективные алгоритмы для решения задачи дискретного логарифмирования в общем случае неизвестны.

Для заданных g и a решение x уравнения $g^x = a$ называется дискретным логарифмом элемента a по основанию g. В случае, когда G является мультипликативной группой кольца вычетов по модулю m, решение называют также индексом числа a по основанию g. Индекс числа a по основанию g гарантированно существует, если g является первообразным корнем по модулю m.

Пусть в некоторой конечной мультипликативной абелевой группе G задано уравнение $g^x = a$.

Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа x, удовлетворяющего уравнению. Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы. Это сразу даёт грубую оценку сложности алгоритма поиска решений сверху – алгоритм полного перебора нашёл бы решение за число шагов не выше порядка данной группы.

Чаще всего рассматривается случай, когда $G = (g)$, то есть группа является циклической, порождённой элементом g. В этом случае уравнение всегда имеет решение. В случае же произвольной группы вопрос о разрешимости задачи дискретного логарифмирования, то есть вопрос о существовании решений уравнения, требует отдельного рассмотрения.

Пример. Рассмотрим задачу дискретного логарифмирования в кольце вычетов по модулю простого числа. Пусть задано сравнение $3^x \equiv 13\ (mod\ 17)$.

Будем решать задачу методом перебора. Выпишем таблицу всех степеней числа 3. Каждый раз мы вычисляем остаток от деления на 17 (например, $33 \equiv 27$ – остаток от деления на 17 равен 10).

$$31 \equiv 3, 32 \equiv 9, 33 \equiv 10, 34 \equiv 13, 35 \equiv 5, 36 \equiv 15, 37 \equiv$$
$$\equiv 11, 38 \equiv 16, 39 \equiv 14, 310 \equiv 8, 311 \equiv 7, 312 \equiv 4, 313 \equiv$$
$$\equiv 12, 314 \equiv 2, 315 \equiv 6, 316 \equiv 1.$$

Теперь легко увидеть, что решением рассматриваемого сравнения является x=4, поскольку 34≡13.

На практике модуль обычно является достаточно большим числом, и метод перебора является слишком медленным, поэтому возникает потребность в более быстрых алгоритмах.

В произвольной мультипликативной группе.

В алгоритме используется таблица, состоящая из $O(\sqrt{|(g)|}$ пар элементов и выполняется $O(\sqrt{|(g)|}$ умножений. Данный алгоритм медленный и не пригоден для практического использования. Для конкретных групп существуют свои, более эффективные, алгоритмы.

В кольце вычетов по простому модулю.

Рассмотрим сравнение

$a^x \equiv b(\mathrm{mod}\ p)$, где p – простое, b не делится на p без остатка. Если a является образующим элементом группы Z/pZ, то уравнение имеет решение при любых b. Такие числа a называются ещё первообразными корнями, и их количество равно $\phi(p-1)$, где ϕ – функция Эйлера. Решение уравнения можно находить по формуле:

$$x \equiv \sum_{i=1}^{p-2} \left(\frac{\left(1 - a^i\right)}{1} \right) * b^i\ (mod\ p).$$

Однако, сложность вычисления по этой формуле хуже, чем сложность перебора.

Следующий алгоритм имеет сложность $O\ (\sqrt{p} * logp)$.

Существует также множество других алгоритмов для решения задачи дискретного логарифмирования в поле вычетов. Их принято разделять на экспоненциальные и субэкспоненциальные. Полиномиального алгоритма для решения этой задачи пока не существует.

Алгоритмы с экспоненциальной сложностью:

1) алгоритм Шенкса (алгоритм больших и малых шагов, baby-step giant-step);

2) алгоритм Полига-Хеллмана – работает, если известно разложение числа $p - 1$ на простые множители;

3) ρ-метод Полларда имеет эвристическую оценку сложности.

В качестве алгоритма для проверки криптостойкости был взят Алгоритм Шенкса. Была реализована программа, проводящая расчеты для матричного протокола и для обычного. В случае с матричным протоколом, время для расчетов по алгоритму Шенкса больше, чем с обычным протоколом Диффи-Хеллмана, использующим числа для генерации ключа. Это говорит о том, что криптостойкость модифицированного протокола выше, чем у стандартного.

4.1.1 Код программы алгоритма Шенкса для матричного протокола

```
q:=12673;
M:=[[0,1],[1651,3514]];
m1:=250;
m2:=260;
n1:=[];
n2:=[];
K:=M^1000 mod q;
for i in [1..m1] do
n1[i]:=K*M^i mod q;
```

```
od;
B:=M^m1 mod q;
for j in [1..m2] do
n2[j]:=B^j mod q;
od;
for i in [1..m1] do
for j in [1..m2] do
if n1[i]=n2[j] then
b:=i;
c:=j;
fi;
od;
od;
M1:=M^(m1*c);
M2:=M^-b;
K:=M1*M2;
```

4.1.2 Код программы алгоритма Шенкса для стандартного протокола

```
q:=12673;
M:=60000;
m1:=250;
m2:=260;
n1:=[];
n2:=[];
K:=M^1000 mod q;
for i in [1..m1] do
n1[i]:=K*M^i mod q;
od;
B:=M^m1 mod q;
for j in [1..m2] do
```

```
n2[j]:=B^j mod q;
od;
for i in [1..m1] do
for j in [1..m2] do
if n1[i]=n2[j] then
b:=i;
c:=j;
fi;
od;
od;
M1:=M^(m1*c);
M2:=M^-b;
K:=M1*M2;
```

4.2 Вывод по четвертой главе

Для расчёта криптографической стойкости был выбран алгоритм Шенкса. Проведены расчеты для стандартного и модифицированного протоколов Диффи-Хеллмана. Данные расчеты показывают, что криптографическая стойкость модифицированного протокола выше, чем у стандартного, о чем говорит время выполнения алгоритма.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы был проведен анализ классического алгоритма Диффи-Хеллмана.

В ходе выполнения работы был разработан алгоритм генерации матриц большого порядка над кольцом вычетов, который необходима для дальнейшей модификации протокола, разработана модификация классического протокола Диффи-Хеллмана на основе алгоритма генерации матриц большого порядка. Разработана программа, выполняющая модифицированный алгоритм. Проведен анализ криптографической стойкости протокола и написаны программы для проверки и сравнения сложности выполнения задачи обратного логарифмирования.

Таким образом была выполнена цель работы – модификация протокола Диффи-Хеллмана и оценка ее криптостойкости.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Рябко, Б.Я. Основы современной криптографии для специалистов в информационных технологиях / Б.Я. Рябко, А.Н. Фионов. – М.: Научный мир, 2004. – 173 с.

2 Саломаа, А. Криптография с открытым ключом / А. Саломаа. – М.: Мир, 1995. – 318 с.

3 ГОСТ Р 34.10-94 Информационная технология (ИТ). Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма (принят в качестве межгосударственного стандарта ГОСТ 34.310-95).

4 Алфёров, А.П. Основы криптографии / А.П. Алфёров, А.Ю. Зубов, А.С. Кузьмин, А.В. Черёмушкин. – Изд.-во: Гелиос-АРВ, 2002. – 450 с.

5 Чмора, А.Л. Современная прикладная криптография / А.Л. Чмора. – М. Гелиос АРВ, 2001. – 256 с.

6 Фергюсон, Н. Практическая криптография / Н. Фергюсон, Б. Шнайер. – М.: Издательский дом «Вильямс», 2005. – С. 235–236.

7 Болотов, А.А., Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.: КомКнига, 2006. – 376 с.

8 Shannon, C.E. Communication Theory of Secrecy Systems / C.E. Shannon // Bell Systems Technical Journal 1949. – V. 28, №4. – P. 656–715.

9 Шнайер Б., Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: Триумф, 2012. – 815 с.

10 Черемушкин, А.В. Лекции по арифметическим алгоритмам в криптографии / А.В. Черемушкин. - М.: МЦНМО, 2002. – 77 с.

11 Литвинская, О.С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. – М.: КноРус, 2015. – 168 с.

12 Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии / Баричев С.Г., Гончаров В.В., Серов Р.Е. – М.: Горячая линия – Телеком, 2001. – 40 с.

13 Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов – СПб.: Лань, 2000. – 224 с.

14 Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография: скоростные шифры / А.А. Молдовян, Н.А. Молдовян, Н.Д. Гуц, Б.В. Изотов – СПб.: БХВ, 2002. – 489 с.