МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КубГУ»)
Факультет компьютерных технологий и прикладной математики
Кафедра анализа данных и искусственного интеллекта

КУРСОВАЯ РАБОТА

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ДВОИЧНОГО РЮКЗАКА

Работу выполнил_____В.В.Шмыгля

Направление подготовки 09.03.03 Прикладная информатика_____курс 3

Направленность (профиль) Прикладная информатика в экономике

Научный руководитель, проф.
д-р. физ.-мат. наук, доц._____В.О.Осипян
(подпись)

Нормоконтролер
канд. физ.-мат. наук, доц. _____ Г.В. Калайдина
(подпись)

Краснодар
2024

РЕФЕРАТ

Курсовая работа 27 с., 8 ч., 7 рис., 10 источ.

КРИПТОГРАФИЯ, АСИММЕТРИЧНОЕ ШИФРОВАНИЕ, КЛЮЧ, ШИФРОВАНИЕ, ЗАЩИТА ИНФОРМАЦИИ, ЗАДАЧА О РЮКЗАКЕ, АЛГОРИТМ МЕРКЛА – ХЕЛЛМАНА

Объектом исследования является криптографическая система защиты информации на основе двоичного рюкзака.

Цель работы – ознакомление с основами криптографии, описание принципов работы системы защиты информации на основе стандартного рюкзака.

В результате исследования были рассмотрены основные понятия в криптографии, а также описан алгоритм Меркла – Хеллмана. Предоставленные данные будут использованы для практической реализации. Нами был введен ряд основных понятий, списки достоинств и недостатков, классификация алгоритмов шифрования

Также мы ознакомились с историей криптографии, этапами ее развития и становления.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Целью данной курсовой работы является освоение основных аспектов работы криптосистем, построенных на основе стандартного рюкзака. В дальнейшем мы используем всю изложенную в данной курсовой работе матчасть для реализации собственной системы защиты информации, а именно защищенного мессенджера, который будет шифровать и дешифровать сообщения, используя асимметричное шифрование. Мы не будем углубляться в детали криптографических алгоритмов (за исключением взятого нами за основу), а сосредоточимся на создании теоретического базиса, который позволит понять основные принципы работы систем защиты информации и их применение в реальных условиях.

1 Основы криптографии

1.1 История криптографии

Криптография как способ сокрытия информации существует достаточно давно, как и большинство того, что мы используем в обычной повседневной жизни, изначально использовалось при ведении военных действий. Ведь никто из противоборствующих сторон, не заинтересован в том, что их планы станут известны противнику, это может стоить потерей ценнейшего ресурса, а именно солдат, времени, да и в целом жизни.

Существовало множество видов сокрытия информации от противника:

– Скрытое сообщение гонец мог проглотить сообщение или спрятать в каблуке либо просто запомнить;

– Тайный метод, например шифр Цезаря или другие, где сообщения шифровались с помощью перестановок и моно алфавитным подстановкам;

– Замаскированное сообщение;

– Невидимое сообщение, например микроточки или невидимые чернила, которые проявляются при нагревании или иных химических процессах.

В целом данные методы в наши дни можно назвать примитивными. Это по большей части обусловлено отсутствием технических возможностей. Предположительно еще в 700 году до н. э. в Древней Греции и Спарте, как средство шифрования использовалась скитала или сцитала Рисунок 1.

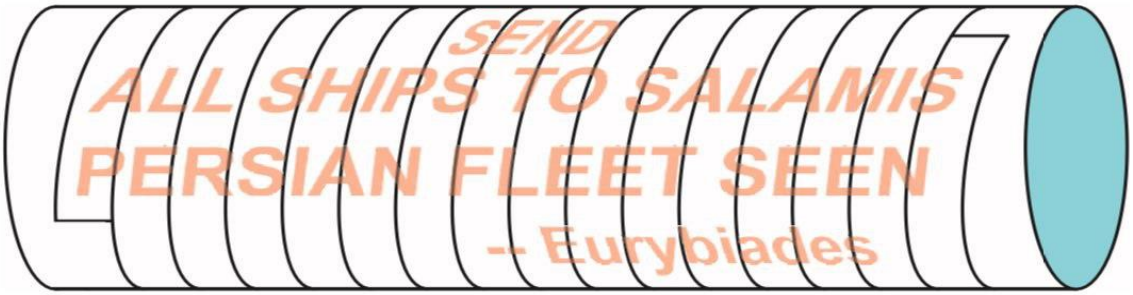

Рисунок 1 – Скитала

Она представляла собой цилиндр, обвитый по спирали узкой полоской кожи или пергамента таким образом чтобы края соседних витков без пробелов и перекрытий. Если же развернуть эту полоску будут видны только разрозненные части букв, иногда наносились дополнительные завитки что бы или раскраска что бы как украшение, что не давало врагу понять суть сообщения. Тот, кто передает сообщение, мог носить его как ремень, подпругу для лошади или все что угодно, а получателю нужна была всего лишь палка нужного диаметра.

Однако научно-технический прогресс не стоял на месте, и в начале XX века уже использовалась более стойкие к ручному криптоанализу шифры. Обеспечение более высокой криптостойкости было ознаменовано появлением роторных криптосистем, позволявших автоматизировать процесс шифрования, одной из известнейших машин такого типа стала немецкая Enigma. Криптография все больше и больше закреплялась как наука имея под собой математический фундамент.

Начиная с 70-х готов XX века главным инструментом криптографов стала ЭВМ, которая позволила ускорить процесс шифрования и расшифровки при этом обеспечить высокую криптостойкость. Появились новые методы и способы, сокрытия данных, новый метод кодирования и передачи сообщений

– криптография с открытым ключом. Данный прогресс стал возможен благодаря значительному развитию технологий и распространению шифрования среди частных лиц. Наука о кодировании сообщений выделилась как отдельная область, сочетающая математику и информатику.

Криптография находит обширное применение: скрытие содержания передаваемых сообщений, защита банковских операций, охрана баз данных компаний и многое другое.

Вот так из способа утаить планы от противника в сугубо военных целях криптография стала неотъемлемой частью нашей повседневной жизни. Переводы денег, общению в мессенджерах и прочие блага цивилизации.

1.2 Основные понятия

Убедившись в необходимости, криптографии давайте же всё-таки введем понятия что бы расставить все по своим местам.

Криптография – наука, изучающая различные методы преобразования, шифрования или кодирования данных, таким образом что бы их мог принять и интерпретировать только тот, для кого они предназначены.

Под данными будем подразумевать ценную или не очень ценную информацию любого рода и вида.

Данные передаются по каналу связи в *зашифрованном* виде.

Существуют два способа передачи данных. Первый способ подразумевает сокрытие самого факта передачи (стеганогфический подход с засекречивания информации). Второй (криптографический подход) передача не скрывается, скрывается само сообщение с помощью специальных шифров, таким образом, чтобы информация, перехваченная аналитиком, без предварительной обработки не имела бы смысла. В рамках курсовой работы первый способ рассматриваться не будет.

Шифр – совокупность условных знаков, применяемых для сокрытия содержимого открытого текста, а также сами условные знаки.

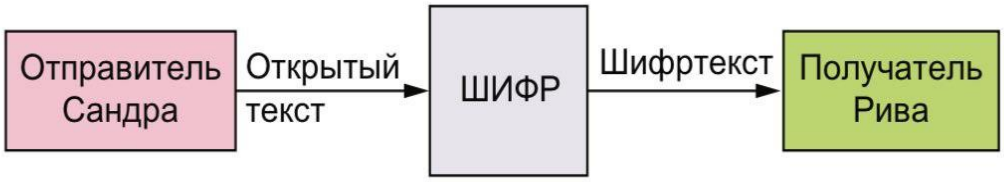

Рисунок 2 – Схема передачи информации

Криптоанализ – рассматривает всевозможные способы раскрытия шифров, или различные несанкционированные способы доступа и модификации самих данных.

Вскрытие (взламывание) шифра — процесс получения защищаемой информации из шифрованного сообщения без знания примененного шифра. Способность шифра противостоять всевозможным атакам на него называется стойкостью шифра.

Ключ – это элемент шифра, используемый для конкретного сообщения. Он представляет собой набор символов, который контролирует процесс шифрования и расшифрования. Безопасность защищаемой информации в значительной степени зависит именно от ключа.

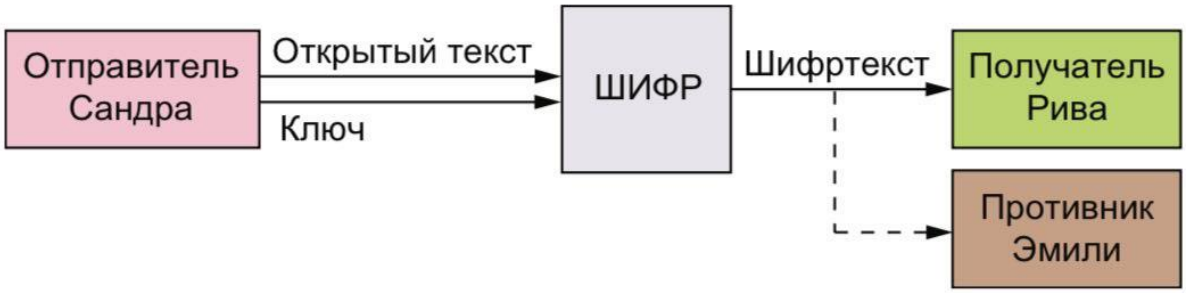

Рисунок 3 – Схема шифрования с ключом

Современные шифры с использованием ключа обычно делятся на три категории с секретным ключом (симметричное шифровании), открытым ключом (ассиметричное шифрование) и с персональным ключом (трехпроходный протокол).

Защита информации – совокупность мероприятий, методов и средств (программных, программно-аппаратных или других), обеспечивающих как исключение несанкционированного доступа к самой информации, так; и ее безопасность в самом широком смысле.

Система, позволяющая защитить информацию на этапах ее обработки и передачи (хранение информации есть ее передача во времени), называется системой защиты информации(криптосистема) или СЗИ.

У СЗИ существуют четыре цели:

– Конфиденциальность – защита информации от лиц, не имеющих права доступа к ней;

– Целостность – гарантирование того, что информация дошла до пункта назначения нетронутой;

– Аутентикация – методика проверки подлинности отправителя и получателя, а также самой информации;

– Невозможность отказа от авторства (или невозможность приписывания авторства) – предотвращение попыток получателя или отправителя отказа от некоторых действий, которые они совершили по отношению к пересылаемой информации.

Для достижения этих целей криптосистемы должны обладать следующим функционалом:

– Шифрование и дешифрование данных;

– Идентификация;

– Аутентикация;

– Создание цифровых подписей;

– Организация системы ключей: хранение, генерация обмен ключей;
– Установка безопасного канала;
– Защита от атак.

Схематически СЗИ можно представить в виде Рисунок 4.

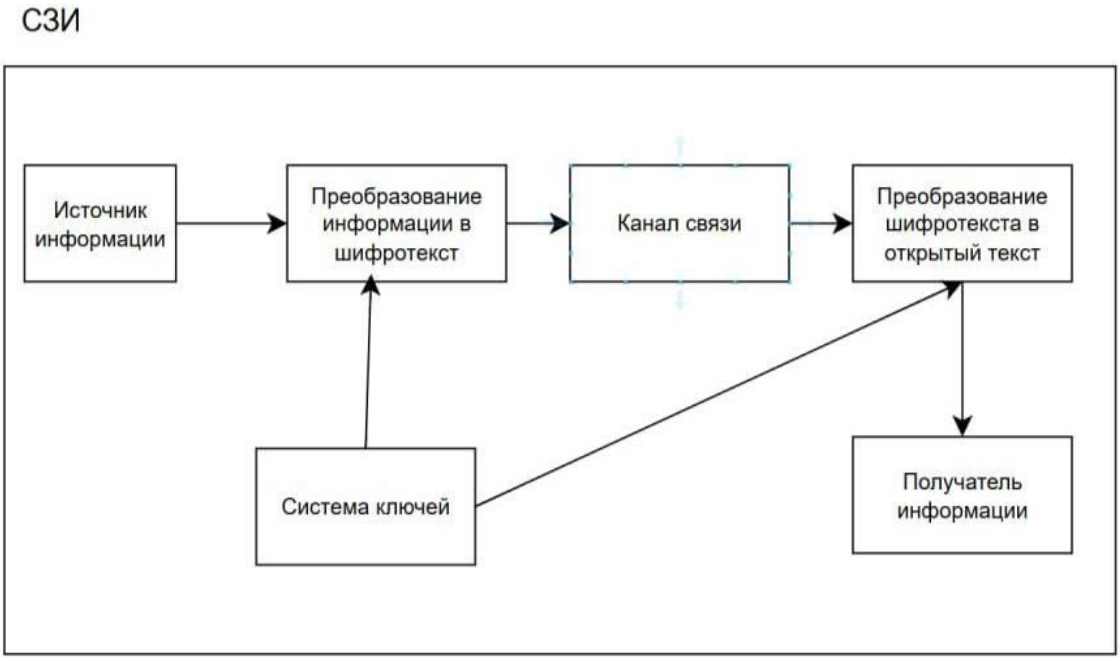

Рисунок 4 - СЗИ

1.3 Целостность информации

Как уже говорилось ранее информация это то, что мы передаем, и основная задача СЗИ обеспечить защиту. Предположим, что наша система справилась со всеми совершаемыми на нее атаками и наши оппоненты так и не смогли разгадать наше послание. Но дошло ли наше сообщение в том виде, в котором мы его посылали? Тут встает вопрос о целостности информации.

Дадим определение, целостность информации – подразумевает под собой что данные не были изменены при выполнении какой-либо операции над ними будь то передача или хранение. К сожалению, процедура шифрования не гарантирует никакой целостности, а лишь дает нам гарантию того, что заинтересованное лицо, не являющее получателем, не сможет получить

информацию. Но не оберегает нас от помех в канале связи или внедрении мусора от того самого заинтересованного лица.

Под нарушением целостности информации понимают:

– Инверсию битов;

– Добавление новых битов (т. е. совершенно новых данных);

– Удаление битов;

– Изменение порядка следования битов.

Задача состоит в том, чтобы обнаружить не столько случайные изменения информации (спонтанные искажения), но целенаправленную обработку сообщения криптоаналитиком. В этом может помочь, например хеш-функции.

Хэш-функция — это математическая функция, которая принимает входные данные произвольной длины и преобразует их в строку фиксированной длины, называемую хэшем. Хэш-функции обладают несколькими важными свойствами:

– Уникальность: для разных входных данных хэш-функция должна давать разные хэши;

– Даже небольшое изменение во входных данных должно приводить к значительно изменившемуся хэшу;

– Невозможно восстановить исходные данные по хэшу.

После передачи сравнивая хеш-значения сообщений, вычисленные до и после передачи, можно определить, были ли внесены какие-либо изменения в сообщение или файл. Если хэши совпадают, это означает, что данные не были изменены. Если произойдет любое изменение в данных (например, из-за ошибки или атаки), новый хэш будет отличаться от исходного, что сигнализирует о том, что данные были компрометированы. Хэш-функции часто используются в сочетании с цифровыми подписями, где создается хэш сообщения, который затем подписывается закрытым ключом. Это гарантирует,

что подпись относится именно к этому сообщению и изменять её без изменения самого сообщения невозможно.

Если же возникла проблема при передаче данных в самом канале, то для устранения «канальных ошибок» используют помехоустойчивые коды, исходя из характеристик канала связи и типов канальных ошибок

1.4 Подлинность

С развитием интернета установить является тот или иной человек, тем за кого он себя выдает достаточно сложно, если раньше подлинность теоретически можно было определить, например по подчерку, или иным косвенным признаком, то всемирная паутина лишает нас это возможности.

Поэтому очень важно, чтобы в нашей СЗИ была возможность могло установить подлинность того или иного лица.

Для этого используют 4 процедуры проверки:

1) Идентификация;
2) Аутентикация;
3) Верификация;
4) Авторизация.

Идентификация – процесс определения, кто именно пытается получить доступ к системе. Это может быть просто имя пользователя или email-адрес. Например, когда вы вводите свой логин в форму входа, система идентифицирует вас по этому идентификатору.

Аутентикация подтверждает подлинность предоставленного идентификатора путем проверки доказательств: пароля, отпечатка пальца или голосового образца. Например, после указания логина вы вводите пароль, который система сравнивает с сохраненным хешем этого пароля.

Верификацию часто путают с аутентикацией. На самом деле это процесс подтверждения, что система или компонент соответствует определенным

требованиям или стандартам. В контексте безопасности это может включать такие процессы, как двухфакторная аутентикация (например, после ввода пароля требуется ввести код, полученный по SMS).

Авторизация определяет, какие действия или ресурсы доступны пользователю после его идентификации и аутентикации. Например, может быть доступ к чтению файлов, но не к их изменению.

1.5 Ключи

Как ранее было сказано ранее ключи это неотъемлемая часть процесса шифрования и самая важная часть любой криптосистемы.

Ключи чаще всего имеют следующую классификацию:

– Секретный ключ(симметричный) – ключ известный только своему владельцу, с помощью его происходит как зашифровка, так и расшифровка сообщения;

– Ассиметричные ключи или ключ пара – используются в ассиметричных алгоритмах и состоят из двух ключей (закрытый и открытый).

Это не совсем точно, ключи по своему назначению делятся на ключи для шифрования ключей и ключи для шифрования данных. *По* времени жизни делятся на долговременные и кратковременные, но в рамках курсовой этот вопрос затрагиваться не будет.

Количество информации в ключе, как правило, измеряется в битах.

Для современных симметричных алгоритмов (AES, CAST5, Twofish) основной характеристикой криптостойкости является длина ключа. Чтобы получить максимальную надежность, сегодня обычно используются крипто ключи длиной в 256 бит и более. Для того чтобы расшифровать их, нужно использовать суперкомпьютеры — сверхмощные аппаратно-программные комплексы, доступ к которым имеют лишь единицы.

Для асимметричных алгоритмов, основанных на проблемах теории чисел (проблема факторизации —RSA, проблема дискретного

логарифма — Elgamal) в силу их особенностей минимальная надёжная длина ключа в настоящее время — 1024 бит.

В любой криптосистеме должна быть реализованная система управления ключами в понятие управление ключами входит совокупность методов решения следующих задач:

- генерация ключей;
- распределение ключей;
- хранение ключей;
- замена ключей;
- депонирование ключей;
- уничтожение ключей.

Правильное решение всех перечисленных задач имеет огромное *значение*, так как в большинстве случаев противнику гораздо проще провести атаку на ключевую подсистему или на конкретную реализацию криптоалгоритма, а не на сам этот *алгоритм* криптографической защиты. Использование стойкого алгоритма шифрования является необходимым, но далеко не достаточным условием построения надежной системы криптографической защиты информации. Используемые в процессе информационного обмена ключи нуждаются в не менее надежной защите на всех стадиях своего жизненного *цикла*.

2 Шифрование

2.1 Шифр

С понятием шифра мы ознакомились в части 1.2 Основные понятия.

Введем понятие шифрование. Шифрование — это процесс преобразования исходной информации в шифротекст, используя определенные алгоритмы, методы. Шифрование с использованием ключа, изменением порядка цифр или заменной их на другие.

В зависимости от вида шифрования, результирующий шифротекст должен обладать некоторыми свойствами:

– устойчивостью к дешифровке сторонними лицами;

– способностью быть расшифрованным тем, для кого он предназначен.

В современных реалиях чаще всего используют два вида шифрования симметричное и ассиметричное, подробнее о которых мы поговорим в следующей главе.

2.2 Виды шифрования

В этом разделе будут рассмотрены два вида шифрования:

– симметричное шифрование;

– асимметричное шифрование.

Примечание: в рамках курсовой работы мы рассмотрим виды лишь в общих чертах, более подробно мы рассмотрим способ реализации алгоритм Меркла - Хеллмана.

2.2.1 Симметричное шифрование

Симметричное шифрование или шифрование с одним ключом. Один из самых простых и надежных способов шифрования.

В настоящее время симметричные шифры — это:

– блочные шифры. Обрабатывают информацию блоками определённой длины, применяя к блоку ключ в установленном порядке, как правило, несколькими циклами перемешивания и подстановки;

– поточные шифры, в которых шифрование проводится над каждым битом либо байтом исходного (открытого) текста с использованием гаммирования. Поточный шифр может быть легко создан на основе блочного (например, ГОСТ 28147-89 в режиме гаммирования), запущенного в специальном режиме.

Суть подхода заключается в том, что зашифровка и расшифровка исходных данных происходит с помощью одного ключа, который есть только у отправителя и получателя Рисунок 5.

Рисунок 5 – Схема работы симметричного шифрования

Симметричное шифрование в общих чертах работает так:

1) субъект А и субъект Б согласовывают общий секретный ключ;

2) этот ключ должен оставаться в тайне и передаваться по защищенным каналам связи;

3) субъект Б шифрует пакет данных с использованием общего секретного ключа, после чего передает зашифрованные данные субъекту А;

4) субъект А расшифровывает данные, используя тот же самый общий секретный ключ;

5) ключ должен быть защищен от несанкционированного доступа, иначе безопасность шифрования будет скомпрометирована.

Большинство симметричных шифров используют сложную комбинацию большого количества подстановок и перестановок. Многие такие шифры исполняются в несколько (иногда до 80) проходов, используя на каждом проходе «ключ прохода». Множество «ключей прохода» для всех проходов называется «расписанием ключей» (key schedule). Как правило, оно создаётся из ключа выполнением над ним неких операций, в том числе перестановок и подстановок.

Преимущества:

1) Высокая скорость. Симметричное шифрование является относительно быстрым, что делает его подходящим для приложений, требующих высокой производительности;

2) Простота. Симметричное шифрование является относительно простым в реализации, что делает его доступным для широкого круга пользователей;

3) Безопасность. При использовании достаточно длинных ключей симметричное шифрование может обеспечить высокий уровень безопасности.

Недостатки:

1) Проблема передачи ключей. Ключи симметричного шифрования должны быть переданы всем участникам процесса шифрования в безопасном режиме. Это может быть затруднительно, особенно в случае большого количества участников;

2) Управление ключами. Сложность управления ключами в большой сети.

2.2.2 Ассиметричное шифрование

Криптографическая система с открытым ключом (или асимметричное шифрование, асимметричный шифр) — система шифрования, при которой открытый ключ передаётся по открытому каналу и используется для шифрования сообщения. Для расшифровки сообщения используется секретный ключ. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах и стандартах цифровой подписи.

Принцип обмена данными между двумя субъектами с использованием открытого ключа будет выглядеть так:

1) субъект А генерирует пару ключей – открытый и закрытый;

2) открытый ключ передается субъекту Б. Этот процесс может производиться при помощи незащищенных каналов связи;

3) субъект Б шифрует пакет данных за счет полученного открытого ключа, после чего передает его элементу А. Передача тоже может происходить по незащищенным каналам;

4) субъект А расшифровывает при помощи закрытого ключа полученные от субъекта Б сведения.

Предложенная схема делает перехват данных, передаваемых по незащищенным каналам, бесполезным. Связано это с тем, что восстановление исходной информации возможно только через закрытый ключ, который известен исключительно получателю. Он не требует никакой передачи, поэтому вычислить его практически невозможно.

Рисунок 6 – Схема ассиметричного шифрования

Асимметричное шифрование используется для решения проблемы симметричного метода, в котором для кодирования и восстановления информации используется один и тот же ключ. Если его передавать по незащищенным каналам связи, его могут перехватить злоумышленники или посторонние лица, чтобы получить доступ к зашифрованной информации.

Рассматриваемая концепция более безопасная, но медленнее симметричных шифров. Основная масса криптосистем предусматривает одновременное применение обоих методов шифрования.

Можно выделить следующие виды ассиметричных алгоритмов:

1) RSA (Rivest, Shamir, Adelman). Это алгоритм, в основе которой заложена вычислительная сложность факторизации (разложения на множители) больших чисел. Концепция встречается в защищенных протоколах TLS и SSL, а также в различных стандартах шифрования – S/MIME, PNG. RSA широко используется при шифровании информации и создании цифровых подписей;

2) DSA (Digital Signature Algorithm) – алгоритм, которые базируется на сложности вычисления дискретных логарифмов. Метод подойдет для

генерирования цифровых подписей. Это часть стандарта DSS (Digital Signature Standard);

3) Схема Эль-Гамаля – алгоритм, опирающийся на сложность вычисления дискретных логарифмов. Заложен в основу DSA и устаревшего российского стандарта ГОСТ 34.10-94. Может применяться и для формирования цифровых подписей, и для непосредственного шифрования данных;

4) ECDSA (Elliptic Curve Digital Signature Algorithm) – концепция, опирающаяся на сложность вычисления дискретного логарифма в группе точек эллиптической кривой. Используется преимущественно для создания цифровых подписей. Может быть задействована для подтверждения транзакций в криптовалюте под названием Ripple;

Все эти разновидности алгоритмов активно применяются в криптовалютах и шифровании информации.

Преимущества ассиметричного шифрования:

1) Безопасность передачи ключей. Ассиметричное шифрование использует пару ключей (публичный и приватный), что позволяет безопасно передавать публичный ключ всем участникам, не опасаясь компрометации приватного ключа;

2) Упрощенное управление ключами. В отличие от симметричного шифрования, где каждому участнику требуется отдельный секретный ключ, в ассиметричном шифровании достаточно иметь публичный ключ для шифрования и один приватный ключ для расшифровки, что упрощает управление ключами.

3) Аутентикация**.** Ассиметричное шифрование позволяет использовать цифровые подписи, что обеспечивает возможность аутентификации отправителя и целостности данных;

4) Гибкость. Публичные ключи могут быть легко распределены и обновлены, что делает систему более гибкой в условиях изменения участников.

Недостатки ассиметричного шифрования:

1) Низкая скорость. Ассиметричное шифрование значительно медленнее, чем симметричное, что может быть проблемой для приложений, требующих высокой производительности и быстрого обмена данными;

2) Сложность реализации. Ассиметричное шифрование требует более сложных математических алгоритмов и может быть труднее в реализации, что может привести к ошибкам и уязвимостям;

3) Зависимость от инфраструктуры. Эффективность ассиметричного шифрования часто зависит от наличия надежной инфраструктуры управления ключами (PKI), что может быть сложно и дорого в реализации;

4) Уязвимость к атакам. Хотя ассиметричное шифрование считается безопасным, оно может быть подвержено определенным типам атак, таким как атаки на основе квантовых вычислений, что требует постоянного обновления алгоритмов и ключей.

Разобравшись со всеми основными составляющими СЗИ, мы перейдем к описанию СЗИ, основанную на задаче о рюкзаке, системы данного типа носят название «рюкзачная» система защиты информации или РСЗИ.

3 Алгоритм Меркла Хеллмана

Первый алгоритм для шифрования на основе задачи о рюкзаке был разработан Мерклом и Хеллманом в 1978 году и получил название «Алгоритм Меркла-Хеллмана».

Алгоритм Меркла – Хеллмана является одним из алгоритмов, реализующих взаимно однозначную связь между закрытым ключом и открытым ключом. В алгоритме Меркла – Хеллмана закрытым ключом является последовательность весов из задачи «сверх возрастающего рюкзака». Открытый ключ – это последовательность весов из задачи «нормального рюкзака» с тем же решением. Меркл и Хеллман, используя модульную арифметику, разработали способ преобразования проблемы сверх возрастающего рюкзака в проблему нормального рюкзака.

Постановка задачи. Имеется число $p > 0$ и упорядоченный набор чисел $A = (a_1, \ldots, a_n)$, где $n > 3$, A - называют рюкзаком или рюкзачным вектором. Требуется указать такой бинарный вектор $(x_1, x_2 \ldots, x_n)$, для которого выполняется равенство

$$p = \mathbf{x_1} * \mathbf{a_1} + \mathbf{x_1} * \mathbf{a_1} + \cdots + \mathbf{x_n} * \mathbf{a_n}$$

В общем случае для данной задачи нет эффективного алгоритма решения и приходится применять полный перебор для нахождения требуемого вектора или доказательства отсутствия решения. Кроме того, в общей постановке задача о рюкзаке может иметь несколько различных решений. Но если рюкзак является сверхрастущим, то решение в случае его существования единственно и существует эффективный алгоритм его нахождения.

Определение. Рюкзак с положительными элементами $(a_1, \ldots, a_n)$ называется сверхрастущим, если $a_2 > a_1, a_3 > a_2 + a_1, a_n > a_1 + a_2 + \ldots + a_{n-1}$

На основе задачи о рюкзаке разработан ряд криптографических систем. Первой из них была система Меркла — Хеллмана, описание которой приведено ниже.

Генерация ключей:

1) Выбирается некоторый сверхрастущий рюкзак $A = (a_1, \ldots, a_n)$;

2) Выбирается число простое число k такое что $k > (a_1 + a_2 + \ldots + a_n)$;

3) Выбирается число c взаимно простое с k, такое что $c < k, k \in N$;

4) Формируется вектор $B = (b_1, \ldots, b_n)$, $b_i = (c * a_i, mod\ k)$, $i = 1, \ldots, n$, где($c * a_i\ mod\ k) = c * a_i - \left[\frac{c*a_i}{k}\right] k$, означает наименьший неотрицательный остаток от деления $c * a_i$ на k а запись $[c * a_i]$ – целая часть от $c * a_i$. Вектор B является открытым ключом;

5) Вектор $A = (a_1, \ldots, a_n)$, c и k являются закрытым ключом.

Алгоритм шифрования:

1) Открытый текст представляется в виде двоичной последовательности T;

2) Последовательность разбивается на блоки $T_i = W$ длины n. Так что $W = (w_1, \ldots, w_n)$, $w_j \in \{0,1\}$;

3) Вычислим число C_i, которое является частью шифртекста по следующей формуле $C_i = \sum_{j=1}^{n} w_j b_j$;

4) Полученная последовательность C является шифротекстом.

Алгоритм дешифрования:

1) Имеется последовательность C длины m, которая является шифротекстом зашифрованным с помощью открытого ключа B;

2) Вычисляется число s мультипликативно обратное множителю c по модулю k, такое, что $(s * c, \mathrm{mod}\ k) = 1$;

3) Вычисляется $R_i = (C_i * s, \mathrm{mod}\ k)$, $\mathbf{i = 1, \ldots, m}$;

4) Имеем $R_i = \sum_{j=1}^{n} w_j a_j$ что является простой задачей рюкзака;

5) Решаем задачу о рюкзаке: если $a_j > R_i$: $w_j = 0$; если $a_j \leq R_i$: $w_j = 1$; вычитаем из R_i произведение $w_j a_j$, повторяя шаги до тех пор, пока не вычислим $W_i = T_i$;

6) Полученная последовательность T переводиться из двоичной последовательности в изначальную.

Рассмотрим, на простом примере как работает алгоритм.

Итак, у нас имеется закрытый ключ

$A = (2, 3, 6, 13, 27, 52)$ и числа $k = 105$ и $c = 31$

Сгенерируем открытый ключ следующим образом:

$$b_1 = (31 * 2, mod\ 105) = 62$$
$$b_2 = (31 * 3, mod\ 105) = 93$$
$$b_3 = (31 * 6, mod\ 105) = 81$$
$$b_4 = (31 * 13, mod\ 105) = 88$$
$$b_5 = (31 * 27, mod\ 105) = 102$$
$$b_6 = (31 * 52, mod\ 105) = 37$$

Таким образом получаем ключ:

$$B = (62, 93, 81, 88, 102, 37)$$

Теперь перейдем к процессу шифрования

Шаг 1:

Пусть сообщение T (три блока в двоичном представлении по шесть элементов, т. е. битов, в каждом блоке) равно:

$$T = (011000, 110101, 101110).$$

Шаг 2:

Первый блок 011000 имеет значения «1» на 2-й и 3-й позициях, что соответствует шифру: 93 + 81 = 174. 3. Второй блок 110101: 62 + 93 + 88 + 37 = 280. 4. Третий блок 101110: 62 + 81 + 88 + 102 = 333. Таким образом, шифротекстом будет последовательность:

$$\mathrm{C} = (174, 280, 333)$$

Далее, законный получатель данного сообщения, знает свой закрытый ключ – оригинальную сверхвозрастающую последовательность, а также значения c и k, использованные для превращения ее в нормальную последовательность рюкзака.

Для расшифрования сообщения Алиса выполняет следующие действия:
Шаг 1:

Определяем значение $s = c^{-1} mod\ k = 61$

Шаг 2:

Каждое значение шифртекста C умножаем на 61, а затем разделим с помощью закрытого ключа $A = (2, 3, 6, 13, 27, 52)$, чтобы получить значения открытого текста. Получим далее:

$$174 \cdot 61 \ (\mathrm{mod}\ 105) = 9 = 6 + 3 \rightarrow 011000;$$
$$280 \cdot 61 \ (\mathrm{mod}\ 105) = 70 = 52 + 13 + 3 + 2 \rightarrow 110101;$$
$$333 \cdot 61 \ (\mathrm{mod}\ 105) = 48 = 27 + 13 + 6 + 2 \rightarrow 101110;$$

Таким образом мы вернулись к исходному тексту T, что доказывает корректность расшифровки.

Достоинства:

– Первая система, основанная на асимметричном шифровании;
– Система проста для понимания;

– Попадание самой системы (алгоритма) в руки криптоаналитика не повредит надежности шифра;

– На основе данной системы был создан ряд других криптосистем, некоторые из них очень трудно взломать даже сейчас (напр. ECDSA).

Недостатки:

– Уязвимость к LLL – алгоритму;

– Лазейка внутри открытого ключа: в докладе израильского криптоаналитика Адди Шамира было доказано, что из открытого ключа можно восстановить значения c и k, необязательно совпадающие с оригинальными, с помощью которых можно получить сверхвозрастающую последовательность, также необязательно совпадающую с оригинальной, которую можно было использовать для расшифровки сообщения;

– Медленная скорость работы в сравнении с симметричными шифрами.

На сегодняшний день основное внимание криптографов сфокусировано на криптосистемах, базирующихся на целочисленной факторизации, дискретном логарифме и эллиптических кривых. Однако исследования рюкзачных систем продолжается. Если будет создан алгоритм, полностью использующий всю трудность задачи о ранце (NP-полноту), с высокой плотностью и с трудными для открытия секретными лазейками, то это будет система *лучше,* чем системы на основе целочисленной факторизации и дискретного логарифмирования (их NP полнота не доказана). Кроме того, данная система будет быстрой, а значит сможет соперничать в скорости с классическими системами на открытых ключа

ЗАКЛЮЧЕНИЕ

В рамках курсовой работы нами были рассмотрены ключевые аспекты систем защиты информации. Нами был описан алгоритм Меркла – Хеллмана, на основе которого мы в дальнейшем построим собственную РСЗИ, которая будет представлена в виде мессенджера с возможностью регистрации, авторизации и обмена защищёнными сообщениями.

Таким образом, реализация данного мессенджера позволит не только обеспечить высокий уровень безопасности передаваемой информации, но и продемонстрировать практическое применение теоретических знаний о криптографических алгоритмах. В дальнейшем мы планируем провести тестирование разработанного приложения, чтобы оценить его эффективность и устойчивость к потенциальным угрозам.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1) Баричев, С. Г. История криптографии // Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е Серов. — Москва.: Горячая линия — Телеком, 2002. — 175 с. – ISBN 978-59973-4489-4

2) Shannon, C. A Mathematical Theory of Communication / C. Shannon // The Bell System Technical Journal — 1948. – URL: http://affect-reason-utility.com/1301/4/shannon1948.pdf. (Дата обращения: 16.11.2024).

3) Баричев, С. Г. 2.4.2. Стандарт AES. Алгоритм Rijdael // Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е Серов. — 3-е изд. — Москва.: Диалог-МИФИ, 2011. — С. 30–35. — 176 с. – ISBN 978-59973-4489-4

4) Килин, С. Я. Квантовая криптография: идеи и практика [Текст] / С.Я. Килин, Д. Б. Хорошко, А. П. Низовцев. — Белорусская наука. — 2007. — 391 с. – ISBN 978-59973-4489-4

5) Валиев, К. А. Квантовые компьютеры: надежды и реальность / К. А. Валиев, А. А. Кокин — Ижевск: РХД, 2004. — 320 с. – ISBN 978-59973-4489-4

6) Осипян, В.О. Криптография в упражнениях и задачах [Текст] / В. О. Осипян, К. В. Осипян — М.: Гелиос АРВ, 2004. — 144 с. – ISBN 978-59973-4489-4

7) Kahn, David (1996), The Codebreakers: the story of secret writing (Abriged version) [Электронный ресурс]/ — 1996. —URL: http://mindguruindia.com/wp-content/uploads/2014/06/MP069_The-CodeBreakers.pdf. (дата обращения: 12.11.2017)

8) Shannon, C. A Mathematical Theory of Cryptography [Электронный ресурс] / C. Shannon — 1945. — 1 September. –URL:

https://www.iacr.org/museum/shannon/shannon45.pdf. (Дата обращения: 16.11.2024).

9) Осипян, В.О. Математическая модель системы защиты информации на основе диофантова множества / В.О. Осипян, А.В. Мирзаян, Ю.А. Карпенко, А.С. Жук, А.Х. Арутюнян // Чебышевский сборник. — 2014. —Т. 15. —№ 1. — С. 146-154. – ISBN 978-59973-4489-4

10) Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] / Б. Шнайер — М.: Триумф, 2002. — 816 с. – ISBN 978-59973-4489-4