Министерство науки и высшего образования РФ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет автоматики и вычислительной техники

Кафедра радиоэлектронных средств

Отчет по лабораторному практикуму №8

**Составление обзора "Современные проблемы (задачи) избранной отрасли наук"**

дисциплина «Методология научных исследований»

|  |  |
| --- | --- |
| Выполнил: студент группы ИВТм-1301 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Седов М.Д. / |
|  |  |
| Проверил: профессор кафедры РЭС | \_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Частиков А.В. / |

Киров 2021

**Цель**: овладеть методикой составления обзора НТИ на заданную тему.

**Задачи**:

1. Подобрать публикации и патенты для обзора в отечественных и зарубежных источниках информации. Использовать для этого НТИ, найденную на занятии 7.
2. Полный текст публикации можно найти по DOI из ieeexplore (баз Scopus или WoS) на ресурсе  [https://sci-hub.tf/](https://sci-hub.im/). Выполнить устный перевод отобранных статей и патентов на русский язык. Привести в отчете их библиографическое описание и расширенные аннотации.
3. На основе подобранных публикаций, патентов и составленных аннотаций выполнить аналитический обзор НТИ в соответствии с общепринятыми правилами (название обзора, сведения об авторе, введение, разделы, заключение, список использованных источников информации по ГОСТ Р7.0.5-2008). В первом разделе должна быть классификация рассматриваемых методов (способов, технологий, схем, программного обеспечения и т.п.), которые в дальнейшем анализируются и описываются. В обзоре должны быть рисунки, таблицы, формулы, схемы (при наличии), фотографии (при необходимости).
4. Оформить обзор в электронной форме.
5. В отчете сделать обобщенные развернутые выводы.
6. В выводах по отчету на основании обзора публикаций указать одну-две публикации, наиболее близкие к теме исследований.
7. В выводах по отчету на основании обзора патентной информации отобрать один-два патента (наиболее близких к теме исследований) в качестве прототипов.

**1 Библиографические описания и расширенные аннотации**

**публикаций и патентов, подобранных для обзора**

Тема научного исследования «Разработка программы моделирования передачи сообщений с асимметричным и симметричным шифрованием данных ».

1.1 Коржик, В. И. Основы криптографии: монография / В. И. Коржик, В.А. Яковлев. – Санкт-Петербург: Интермедия, 2016 – 296 с. – Текст : непосредственный .

1.2 Krishna Chaitanya Nunna. Secure Data Transfer Through Internet Using Cryptography and Image Steganography / Krishna Chaitanya Nunna – Текст : непосредственный // IEEE. – 2017. – №.12 – 7 p.

Расширенная аннотация

Искусство сокрытия информации существует уже несколько веков. Улучшение и развитие всегда сопровождали информационную безопасность. Сокрытие информации должно гарантировать, что сообщение попадет к предполагаемому получателю без ошибок. На протяжении многих лет криптография и стеганография являются двумя основными методами защиты и передачи информации. Криптографические алгоритмы использовали информацию, чтобы зашифровать или скрыть исходное представление. На данный момент безопасность классифицируется методами надежной защиты информации и информационными системами, находящиеся на компьютере. Потенциальные угрозы включают разрушение компьютерного оборудования, программного обеспечения, кражу, несанкционированное использование или раскрытие данных. Компьютер и содержащаяся в нем информация часто считаются конфиденциальными системами, поскольку их использование обычно ограничивается ограниченным числом пользователей. Эта конфиденциальность может подвергаться опасности по-разному. Например, данные и информация могут быть раскрыты хакерами, вирусами. Следовательно, безопасность можно определить как степень сопротивления или защиту от повреждений. Криптография – это искусство и наука сокрытия сообщений для обеспечения секретности данных, а информационная безопасность известна как криптография. В данной статье рассматриваются способы защиты информации при помощи стеганографии и криптографии. Рассматриваются основные криптографические алгоритмы, такие как AES и RSA.

1.3 Смирнова, М. А. Асимметричное шифрование как способ проверки подлинности автора сообщения / М. А. Смирнова, И. А. Самойлова, Л. В. Устинова– Текст : непосредственный //Актуальные проблемы современности. – 2017. – № 2. – 5 с.

1.4 Xiaojuan Chen. Analysis of Cryptographic Protocol by Dynamic Epistemic Logic / Xiaojuan Chen, Huiwen Deng – Текст : непосредственный // IEEE. – 2019. – № 7. – 7 p.

Расширенная аннотация

Безопасность криптографических протоколов всегда была важна для обеспечения правильной реализации протокола. Для обеспечения безопасности протокола в литературе появился ряд работ по анализу и проверке криптографических протоколов. В данной статье предлагается модельный подход для анализа криптографических протоколов. Безопасность криптографических протоколов имеет большое значение при разработке протоколов, поскольку криптографические протоколы должны учитывать атаки злоумышленников. Если в криптографическом протоколе есть какой-либо недостаток безопасности, он может быть атакован злоумышленникам. Проверка безопасности криптографических протоколов особенно важна для проверки того, соответствует ли протокол целям безопасности. Для проверки безопасности криптографических протоколов существует множество методов. В этих методах важную роль играют методы, основанные на логике. Существует множество работ о применении логических методов для анализа и проверки криптографических протоколов. Самый ранний метод анализа логики основан на модели Долева-Яо. Модель действия построена для отображения элементов действия. Модель обновляется посредством выполнения обновления. Выполнение действий приводит к изменениям между моделями. Мы точно моделируем протокол. В некотором смысле логическое описание - это логический анализ криптографических протоколов. С помощью логического языка и модели действий проверяется конкретный пример. Протокол заключается в том, что секретное сообщение передается между двумя пользователями, у которых есть только собственный ключ. Цель протокола состоит в том, чтобы только два пользователя знали секретное сообщение, а внешний злоумышленник не мог узнать секретное сообщение после выполнения протокола. Путем анализа и доказательств мы показываем, что протокол соответствует предполагаемым требованиям и является безопасным.

1.5 Романьков, В. А. Алгебраическая криптография : монография / В. А. Романьков. – Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. – 136 c. – Текст : непосредственный.

1.6 Lee, J. A Theory of Secure Communication. Doctoral dissertation / J. Lee; Universitat Karlsruhe . – DE. – 2014. – 231 p. – Текст: непосредственный.

Расширенная аннотация

Криптографические схемы и протоколы - важные инструменты для защиты коммуникаций и ИТ-приложений. Одно из наиболее распространенных в настоящее время применений - защита связи по сетям электронных устройств, в первую очередь в Интернете, где криптографические протоколы используются в повседневных услугах, таких как онлайн-банкинг, а также для обеспечения конфиденциальности личных (электронных) сообщений. Поскольку безопасность криптографического протокола или схемы, в отличие от ее правильности, не может быть просто продемонстрирована, широко принятая в настоящее время парадигма состоит в том, что уверенность в криптографических протоколах повышается путем предоставления (математического) доказательства их безопасности. Первый вклад – это спецификация формальной структуры, которая воплощает концепции абстрактной и конструктивной криптографии (Maurer and Renner, ICS 2011) и в которой заявления безопасности о конкретных криптографических протоколах могут быть сформулированы и подтверждены. Второй вклад - это применение этой структуры в настройке безопасного обмена данными. Это включает в себя доказательство хорошо известных протоколов в отношении новых определений, сравнение с несколькими существующими понятиями безопасности из литературы и анализ нового протокола одностороннего установления ключа. Третий вклад представляет собой модульное доказательство «уровня записи» протокола безопасности транспортного уровня (TLS), наиболее широко применяемого в настоящее время криптографического протокола в Интернете.

1.7 Умрзоков, С. Криптографические протоколы / С. Умрзоков – Текст : непосредственный // Мировая наука. – 2029. – № 6. – 5 с.

1.8 Новиков, С. Н. Методология зашиты информации на основе технологий сетевого уровня мультисервисных сетей связи : специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : диссертация на соискание ученой степени доктора технических наук / Новиков Сергей Николаевич; Томский государственный университет систем управления и радиоэлектроники. – Томск, 2016. – 235с. – Текст: непосредственный.

1.9 Сизоненко, А. Б. Модели и алгоритмы синтеза логико-вычислительных подсистем защиты информации систем критического применения : специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : диссертация на соискание ученой степени доктора технических наук / Сизоненко Александр Борисович; Воронежский институт МВД РФ. – Воронеж, 2016. – 310 с. – Текст: непосредственный.

1.11 Патент № 2617972 Российская Федерация, МПК RU 2016617549 A (20.06.2016. Криптографическое шифрование: № 2016108116 : заявл. 18.05.2016 : опубл. 07.07.2016 / Насыров Ринат Ришатович, Сулейманов Игорь Рашидович, Чуркин Андрей Игоревич.; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (RU). – 2 с. : ил. – Текст : непосредственный.

1.12 United States Patent №: US US2005235342A1, IPC G06F21/00; H04L9/00; (IPC1-7): H04L9/00 . Cryptography correctness detection methods and apparatuses : Appl. No.: 15/371,117 : 16.01.2004 : Publication: 20.10.2005; Assignee: Microsoft Corp. (US). – 17 p. – Текст : непосредственный.

Расширенная аннотация

Представлены методы и устройства, которые могут формировать определенные процессы и/или даже пользователя об относительной силе или слабости криптографических протоколов. Способ дополнительно включает в себя выборочное обнаружение запроса по меньшей мере для одной службы криптографии и выборочное выполнение по меньшей мере одного действия по обнаружению корректности на основе запрошенной службы криптографии и порогового значения параметра службы криптографии. Раскрыты способы установления корректности криптографического протокола. Криптографический протокол включает в себя определение того, подходит ли криптографический ключ. Включает в себя проверку сравнение размера криптографического ключа. Также устанавливаются правила, при которых тот или иной криптографический протокол, установленный на компьютере, имеет неприемлемый алгоритм шифрования. Рассматриваются возможные способы идентификации криптографического протокола.

2 **Аналитический обзор**

**Модели передачи сообщений**

М.Д. Седов

Магистрант кафедры ЭВМ, ВятГУ, Киров, Россия,

[stud142503@vyatsu.ru](mailto:stud142503@vyatsu.ru)

Аннотация

Выполнен обзор существующих моделей передачи сообщений. Также рассмотрены возможные варианты атак на сообщения, их влияние, а также способ противодействия. Выполнено сравнение симметричного и асимметричного шифрования, выявлены достоинства и недостатки. Актуальность объясняется тем, что в современном мире безопасный способ передачи сообщений имеет большое значение, так как все большее число людей обменивается сообщениями через открытые каналы связи.

Ключевые слова: симметричное шифрование, асимметричное шифрование, дешифрование, блочный алгоритм, сеть Фейстеля, закрытый ключ, открытый ключ, защита информации.

Annotation

The review of message transfer models is carried out. Also considered are possible options for attacks on messages, their impact, as well as a method of countering. Comparison of symmetric and asymmetric encryption is performed, advantages and disadvantages are revealed. The relevance is explained by the fact that in the modern world a secure way of transmitting messages is of great importance, since an increasing number of people exchange through open communication channels.

Keywords: symmetric encryption, asymmetric encryption, decryption, block algorithm, Feistel network, private key, public key, information protection.

**Введение**

На сегодняшний день все большее число людей сталкивается с передачей информации по сети. Широкое распространение мобильных устройств с доступом в интернет заставило взглянуть по-новому на безопасность передачи сообщений. Большинство людей будет против, если их общение в социальных сетях, их банковские данные либо содержимое электронной почты попадет злоумышленникам или будет всеобще опубликовано. В связи с чем возникает потребность в защите передаваемых данных, которая может быть решена при помощи криптографии. Цель современной криптографии – защита передаваемых данных от доступа посторонних лиц или возможности подмены какой-то информации. Именно это обуславливает высокую актуальность криптографии как одного из важнейших направлений компьютерных технологий.

Вместе с тем важно отметить, что в настоящее время в области образования все больше производится автоматизация контроля знаний учащихся и освоения нового материала. Одним из способов автоматизации являются специальные программные модели, эмулирующие работу какой-либо системы. С их помощью студенты имеют возможность достаточно подробно изучить ее работу, принципы и особенности. В совокупности с теоретическим материалом это позволяет увеличить степень освоения новых знаний по данной дисциплине и повысить качество обучения в целом.

Поэтому целью данной обзорной работы является просмотр основных моделей передачи сообщений, их достоинства и недостатки.

**1 Модели передачи сообщений**

При рассмотрении моделей передачи сообщений можно выделить следующие группы:

1. передача сообщений без посторонних злоумышленников. Данный способ передачи предполагает, что сообщения передаются адресату без перехвата злоумышленниками. Отправитель шифрует сообщение и отправляет по открытому каналу. Адресат принимает сообщением с последующем расшифрованием. Отсутствие злоумышленников является наиболее благоприятной ситуацией;
2. передача сообщений с участием пассивного злоумышленника. При данном способе передачи информации между двумя субъектами существует злоумышленник, который может прочитывать информацию, передаваемую по каналу связи. Злоумышленник никак не изменяет данные, а только осуществляет «кражу»;
3. передача сообщений с участием активного злоумышленника. Данный способ предполагает, что существует активный злоумышленник, который пытается всячески изменить информацию;
4. передача сообщений через доверительного посредника. Данный способ предполагает наличие третьей стороны, которая помогает реализовать передачу данных между не доверяющими друг другу сторонами.

Схема моделей, рассмотренных выше, представлены на рисунках 1-4.

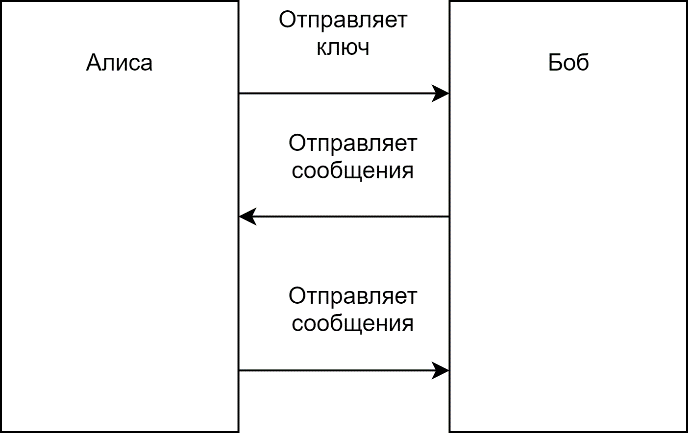


Рисунок 1 – Модель передачи сообщений без злоумышленников

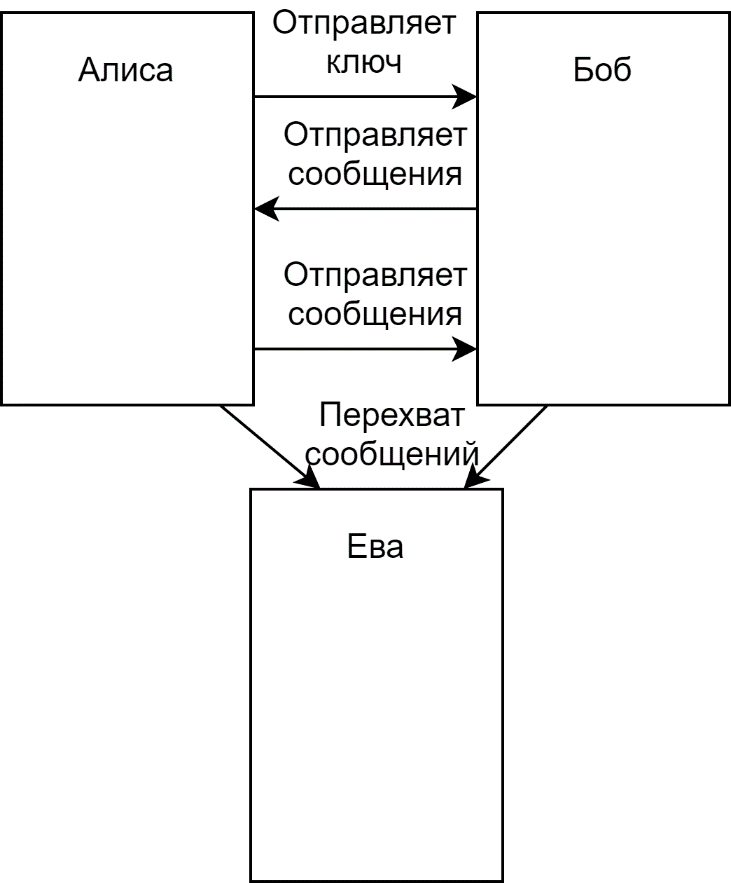


Рисунок 2 – Модель передачи сообщений с пассивным злоумышленником

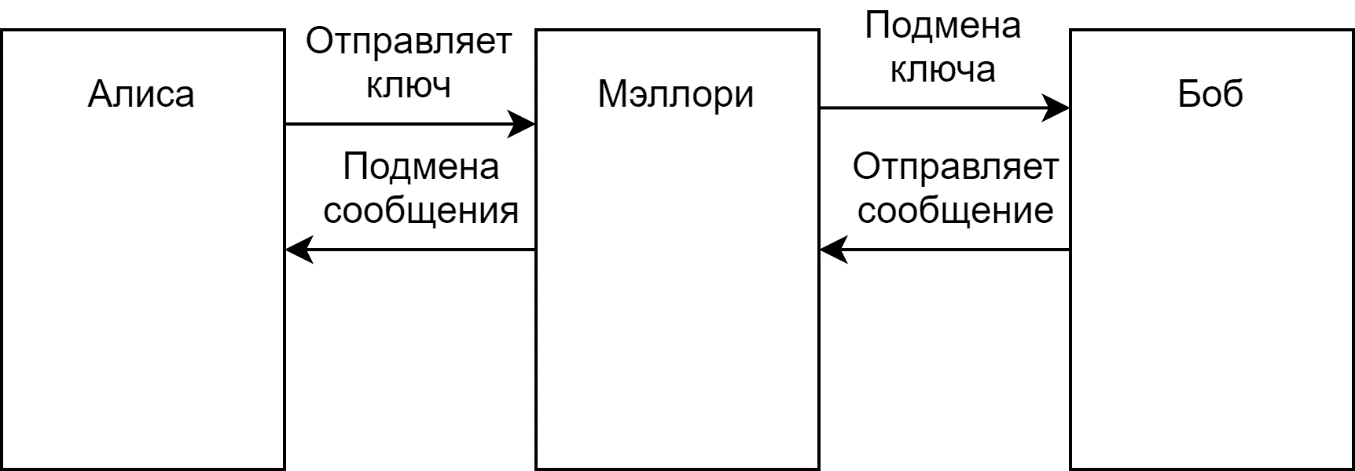


Рисунок 3 – Модель передачи сообщений с активным злоумышленником

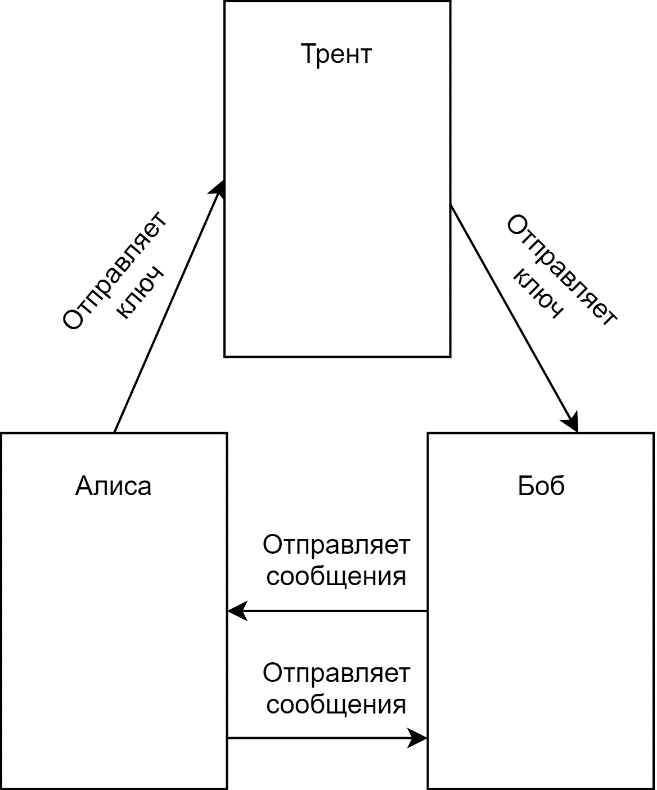


Рисунок 4 – Модель передачи сообщений с доверительным посредником

Описание последовательности действий пользователя при выполнении передачи сообщения без злоумышленников (алгоритм RSA):

1. сформировать запрос, который отправляет Боб Алисе для начала взаимодействия;
2. сгенерировать ключи на основе заданных простых чисел (пользователю необходимо вычислить все необходимые значения для получения пары открытого из закрытого ключей);
3. отправить сгенерированный открытый ключ Бобу для дальнейшего использования;
4. зашифровать сообщение полученным ключом (пользователю необходимо выбрать нужный порядок действий для шифрования). Так как работа нацелена на способы передачи сообщений, то операции по шифрованию опускаются (алгоритмы шифрования изучаются в другом лабораторной работе);
5. передать зашифрованное сообщение Алисе;
6. расшифровать полученное сообщение закрытым ключом (порядок действий схож с шифрованием сообщения).

Пример выполнения задания передачи сообщения с доверительным посредником похож на передачу сообщений, описанную выше. В данном способе добавляется третье лицо, которое находится между Алисой и Бобом – Трент. Трент участвует в процессе распределения ключа. Основная функция Трента – проверка подлинности двух сторон, участвующих в передачи сообщения. Пользователю также необходимо сгенерировать ключ и отправить, но уже Тренту.

Третий и четвертый способ передачи сообщений предполагает наличие злоумышленника. Пассивная атака может как выполняться самим пользователем, либо осуществляться наоборот на передаваемое сообщение пользователем. Атака осуществляется следующим образом:

1. установить прослушивание на канал связи (пользователю необходимо ввести адрес, на который будет осуществляться пассивная атака);
2. начать получать пакеты, которые передаются от Алисы к Бобу или обратно;

Так как рассматриваются модели передачи сообщений, то способом защиты от пассивных атак можно назвать процесс шифрования сообщения. Злоумышленник может получить сообщения, но они не будут представлены в явном виде. А для перевода их в осмысленный текст необходим ключ для расшифрования.

При активной атаке пользователь выполнят роль Мэллори, который осуществляет атаку «человек посередине». В данной атаки пользователь также устанавливает соединение на канал связи и пытается подменить открытый ключ Алисы своим собственным. После получения уже зашифрованного сообщения пользователь сможет расшифровать его своим закрытым ключом, тем самым получить исходное сообщение. Так как процесс генерации ключей занимает некоторое время, то задержка при передаче сообщения может потенциально обнаружить атаку. Для выявления потенциальной атаки необходимо проверить расхождение во времени ответа. Если обычно затрачивается одинаковое количество времени, но присутствуют моменты передачи с большим временем, то это свидетельствует о вмешательстве третьей стороны. Также возможным способом обнаружения будет являться проверка IP – адреса отправителя сообщения.

**2 Способы шифрования при передаче сообщений**

Сегодня все больше и больше людей общаются не лично, а используя компьютерную сеть. Большинство информации необходимо передавать так, чтобы ее смог получить только адресат. В качестве безопасной передачи данных можно использовать следующие способы:

1. создание надежного и недоступного для других канала связи (закрытый канал связи). При современном уровне развития науки сделать данный канал связи для многократной передачи данных является сложным;
2. использование общедоступного канала связи с сокрытием факта передачи информации. Скрытие факта передачи сообщения возможно при помощи стеганографии;
3. использование общедоступного канала связи с передачей данных в преобразованном виде, который восстановить может только адресат. Методами преобразования информации с целью ее защиты от злоумышленников занимается криптография.

Разработка модели будет выполняться на основе задачи, рассмотренной в книге «Прикладная криптография» Брюс Шнайер.

Криптографический протокол – протокол, который использует криптографию. Криптографический протокол включает в себя некоторый криптографический алгоритм.

Для демонстрации работы протоколов используются следующие «игроки»:

1. Алиса и Боб. Они участвуют во всех протоколах. Обычно в качестве инициатора выступает Алиса, которая первая посылает сообщения, а Боб отвечает. При необходимости могут вступить Кэрол и Дейв как третья и четвертая сторона соответственно;
2. Ева. Пассивный злоумышленник, который может прослушивать передаваемые сообщения между Алисой и Бобом, но не может никак воздействовать на сообщения с целью их изменения;
3. Мэллори. Активный злоумышленник, который может не только читать сообщение, но и подменять их. В рамках протоколов его можно назвать взломщиком протоколов;
4. Трент. Доверительный посредник. Это доверенная третья сторона, которая завершает протокол. Посредник помогает реализовать работу протоколов взаимодействия между недоверяющими друг другу сторонами.

В рамках выпускной квалификационной работы будут рассмотрены модели передачи сообщений с симметричным и асимметричным шифрованием данных. Симметричное шифрование – это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации. До 1970-х годов, когда появились первые асимметричные шифры, оно было единственным криптографическим методом. В целом симметричным считается любой шифр, использующий один и тот же секретный ключ для шифрования и дешифрования.

Например, если алгоритм предполагает замену букв числами, то и у отправителя сообщения, и у его получателя должна быть одна и та же таблица соответствия букв и чисел: первый с ее помощью шифрует сообщения, а второй -дешифрует.

Однако такие простейшие шифры легко взломать - например, зная частотность разных букв в языке, можно соотносить самые часто встречающиеся буквы с самыми многочисленными числами или символами в коде, пока не удастся получить осмысленные слова. С использованием компьютерных технологий такая задача стала занимать настолько мало времени, что использование подобных алгоритмов утратило всякий смысл.

Симметричные алгоритмы требуют меньше ресурсов и демонстрируют большую скорость шифрования, чем асимметричные алгоритмы. Большинство симметричных шифров предположительно устойчиво к атакам с помощью квантовых компьютеров, которые в теории представляют угрозу для асимметричных алгоритмов.

Слабое место симметричного шифрования – обмен ключом. Поскольку для работы алгоритма ключ должен быть и у отправителя, и у получателя сообщения, его необходимо передать; однако при передаче по незащищенным каналам его могут перехватить и использовать посторонние. На практике во многих системах эта проблема решается шифрованием ключа с помощью асимметричного алгоритма шифрования.

Концепцию криптографии с открытым ключом была выдвинута Уитфилдом Диффи и Мартином Хеллманов, и независимо Ральфом Мерклом. Их вкладом в криптографию было убеждение, что ключи можно использовать парами – ключ шифрования и ключ дешифрования, и что может быть невозможно получить один ключ из другого. Некоторые из алгоритмов шифрования подходят только для распределения ключей. Другие – наоборот подходят только для цифровых подписей.

Алгоритмы, которые хорошо работают как для цифровых подписей, так и для шифрования:

1. RSA;
2. ElGamal;
3. Rabin.

Они шифруют и дешифруют данные намного медленнее, чем симметричные алгоритмы. Обычно их скорость недостаточна для шифрования больших объемов данных. Гибридные системы обычно позволяют ускорить процесс: для шифрования сообщения используется симметричный алгоритм, а алгоритм с открытым ключом применяется шифрования случайного сеансового ключа.

Алгоритмы криптографии с открытым ключом можно использовать:

1. как самостоятельное средство для защиты передаваемой и хранимой информации;
2. как средство распределения ключей;
3. как средство аутентификации пользователей.

Таким образом, протокол передачи сообщений выглядит следующим образом:

1. Алиса и Боб выбирают алгоритм шифрования;
2. Алиса и Боб выбирают ключи;
3. Алиса шифрует открытый текст своего сообщения с использованием алгоритма шифрования и ключа, получая шифрованное сообщение;
4. Алиса посылает зашифрованное сообщение Бобу;
5. Боб расшифровывает полученное сообщение с использованием алгоритма шифрования и ключа, получая открытый текст сообщения.

Ева, находясь между Алисой и Бобом, может прослушивать канал. Если она может подслушивать только передачу на этапе (4), ей придется дешифровать полученное сообщение. С другой стороны, Ева может подслушивать и этапы (1) и (2). Тогда ей станут известны алгоритм и ключ.

В хорошей криптосистеме безопасность полностью зависит от знания ключа, а не от знания алгоритма. Используя симметричный алгоритм, Алиса и Боб могут открыто выполнять этап (1), но этап (2) они должны хранить в тайне. Мэллори, активный злоумышленник, может попытаться нарушить линию связи на этапе (4), сделав так, что Алиса вообще не сможет передавать информацию Бобу. Мэллори также может перехватить сообщение Алисы и заменить его своим собственным. Если ему удалось узнать ключ, то он сможет зашифровать свое сообщение и отправить его Бобу вместо перехваченного. Таким образом Боб не сможет узнать, что сообщение отправлено Алисой. Если Мэллори не знает ключа, он сможет только создать сообщение, превращающееся после расшифрования в бессмыслицу. Боб, считая, что сообщение отправлено Алисой, может решить, что либо у Алисы, либо в сети возникли проблемы.

Обобщенная схема передачи сообщений с симметричным шифрованием показана на рисунке 1. Исходный текст передаваемого сообщения M зашифровывается алгоритмом и передается по незащищенному каналу связи.

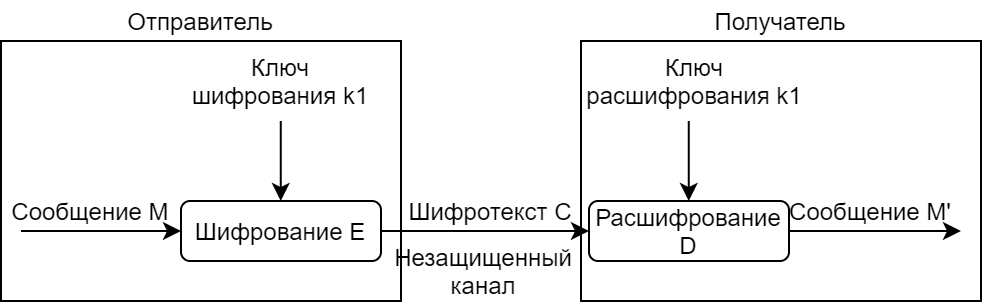


Рисунок 5 – Обобщенная схема передачи сообщений с симметричным шифрованием данных

При передаче сообщений симметричным шифрованием можно выделить следующие положительные моменты:

1. используются простые операции для шифрования и дешифрования;
2. длина ключа меньше по сравнению с ключом, необходимым для ассиметричного шифрования.

При передаче сообщений симметричным шифрованием можно выделить следующие недостатки:

1. распределение ключей должно производиться в секрете. Для распространенных систем шифрования задача распределения ключей является серьезной задачей;
2. если ключ скомпрометирован, то Ева сможет расшифровать все сообщения, зашифрованные этим ключом. Она также сможет выступить в качестве одно из сторон, создающей ложные сообщения;
3. в предположении, что каждая пара пользователей сети использует отдельный ключ, общее число ключей быстро возрастает с ростом числа пользователей. Сеть из n пользователей требует n\*(n-1)/2 ключей. Например, для 10 пользователей необходимо 45 различных ключей, а для 100 пользователей необходимо уже 4950 ключей.

Обобщенная схема передачи сообщений с асимметричным шифрованием показана на рисунке 2. Исходный текст передаваемого сообщения M зашифровывается алгоритмом и передается по незащищенному каналу связи.

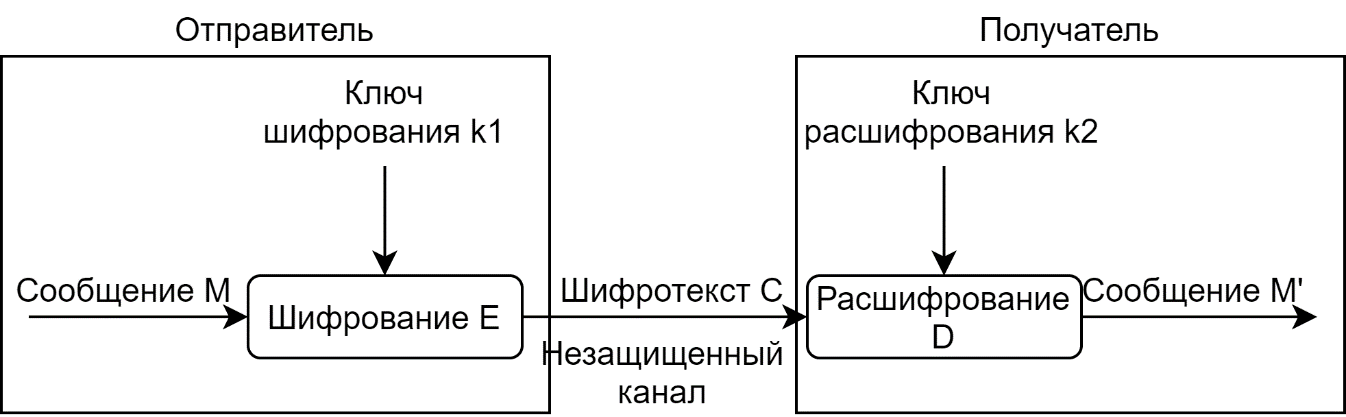


Рисунок 6 – Обобщенная схема передачи сообщений с асимметричным шифрованием данных

При передаче сообщений асимметричным шифрованием можно выделить следующие недостатки:

1. длина ключа, необходимая для безопасной передачи данных, заметно больше, чем при передаче данных с симметричным шифрованием;
2. низкая скорость выполнения операций шифрования и дешифрования, вследствие чего увеличивается время передачи сообщений.

При передаче сообщений асимметричным шифрованием можно выделить следующие положительные моменты:

1. имеется возможность передавать ключ по открытому каналу связи;
2. ассиметричное шифрование возможно использовать для создания цифровых подписей и сертификатов. Это позволяет проверить подлинность электронных документов, а также убедиться, что документ был отправлен именно владельцем сертификата.

При рассмотрении криптографии можно выделить следующие определения:

1. сообщение, которое передается адресату, называется открытым сообщением;
2. преобразованное криптографическими методами сообщение называется шифрованным сообщением;
3. процесс преобразования открытого сообщения в шифрованное называется шифрованием;
4. процесс преобразования шифрованного сообщения в открытое сообщение называется расшифрованием.

В современной криптографии существуют следующие цели:

1. конфиденциальность. Традиционной задачей криптографии является проблема обеспечения конфиденциальности информации при передаче сообщений по открытому каналу связи. Владелец информации, называемый обычно отправителем, осуществляет преобразование открытой информации в шифрованные сообщения с целью защиты от противника. Под противником понимается любой субъект, который не имеет прав ознакомления с содержанием информации. Противник пытается овладеть защищаемой информацией (такие действия обычно называют атаками). Атаки могут быть как пассивными, так и активными;
2. целостность. Наряду с конфиденциальностью не менее важной задачей является обеспечение целостности информации. Решение этой задачи предполагает разработку средств, позволяющих обнаруживать изменения противником в информации. Без знания секретного ключа вероятность успешного навязывания противником искаженной информации мала. Такая вероятность служит мерой имитостойскости шифра, то есть способности самого шифра противостоять активным атакам со стороны противника;
3. аутентификация. В общем случае этот термин может относиться ко всем аспектам информационного взаимодействия: сеансу связи, сторонам, передаваемым сообщениям. Установление подлинности всех аспектов информационного взаимодействия является важной составной частью проблемы обеспечения достоверности получаемой информации.

Электронная цифровая подпись (ЭЦП) – особый реквизит документа, который позволяет установить отсутствие искажения информации в электронном документе с момента формирования ЭП и подтвердить принадлежность ЭП владельцу. Значение реквизита получается в результате криптографического преобразования информации.

ЭЦП может быть получена путем криптографического преобразования информации при помощи закрытого ключа. ЭЦП может быть проверена на отсутствие искажений информации при помощи открытого ключа, который может свободно передавать пользователям.

Существует несколько схем для создания ЭЦП:

1. на основе алгоритмов симметричного шифрования. В данной схеме предусматривается роль третьего лица (арбитра), которые должен пользоваться доверием обеих сторон. Документ зашифровывается закрытым ключом и отправляется арбитру;
2. на основе алгоритмов ассиметричного шифрование. Данная схема на сегодняшний момент является наиболее популярной в силу простоты использования.

Проверить сформированную подпись может любое лицо, так как ключ проверки подписи является открытым. При положительном результате проверки подписи делается заключение о подлинности и целостности полученного сообщения, то есть о том, что это сообщение действительно отправлено тем или иным отправителем и не было модифицировано при передаче по сети. Однако если пользователя интересует, не является ли полученное сообщение повторением ранее отправленного или не было ли оно задержано на пути следования, то он должен проверить дату и время его отправки, а при наличии — порядковый номер.

После этого злоумышленник n может посылать документы абоненту B, подписанные своим секретным ключом kn. При проверке подписи этих документов абонент B будет считать, что документы подписаны абонентом A и их ЭЦП верна, то есть они не были модифицированы кем-либо. До выяснения отношений непосредственно с абонентом А у абонента В может не появиться сомнений в подлинности полученных документов. Открытые ключи ЭЦП можно защитить от подмены с помощью соответствующих цифровых сертификатов. Пример защиты открытых ключей с помощью удостоверяющего центра показан на рисунке 3.

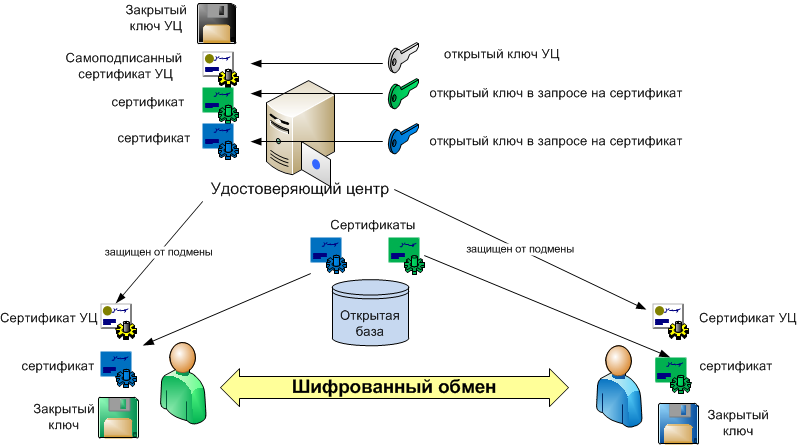


Рисунок 7 – Защита открытых ключей с помощью удостоверяющего центра

Алгоритм DSA показывает пример использования цифровой подписи. DSA включает в себя два алгоритма (S, V): для создания подписи сообщения (S) и для ее проверки (V).

Оба алгоритма вначале вычисляют хэш сообщения, используя криптографическую хэш-функцию. Алгоритм S использует хэш и секретный ключ для создания подписи, алгоритм V использует хэш сообщения, подпись и открытый ключ для проверки подписи.

Стоит подчеркнуть, что фактически подписывается не сообщение (произвольной длины), а его хэш (160 — 256 бит), поэтому неизбежны коллизии и одна подпись, вообще говоря, действительна для нескольких сообщений с одинаковым хэшем. Поэтому выбор достаточно «хорошей» хэш-функции очень важен для всей системы в целом. В первой версии стандарта использовалась хэш-функция SHA-1 (англ. Secure Hash Algorithm — безопасный алгоритм хэширования), в последней версии также можно использовать любой алгоритм семейства SHA-2. В августе 2015 был опубликован FIPS-202, описывающий новую хэш-функцию SHA-3. Но на сегодняшний день она не включена в стандарт DSS.

Для работы системы требуется база соответствия между реальными реквизитами автора (это может быть, как частное лицо, так и организация) и открытыми ключами, а также всеми необходимыми параметрами схемы цифровой подписи (хеш-функция, простые числа). Например, подобной базой может служить центр сертификации.

На рисунке 4 показана работа алгоритма DSA.

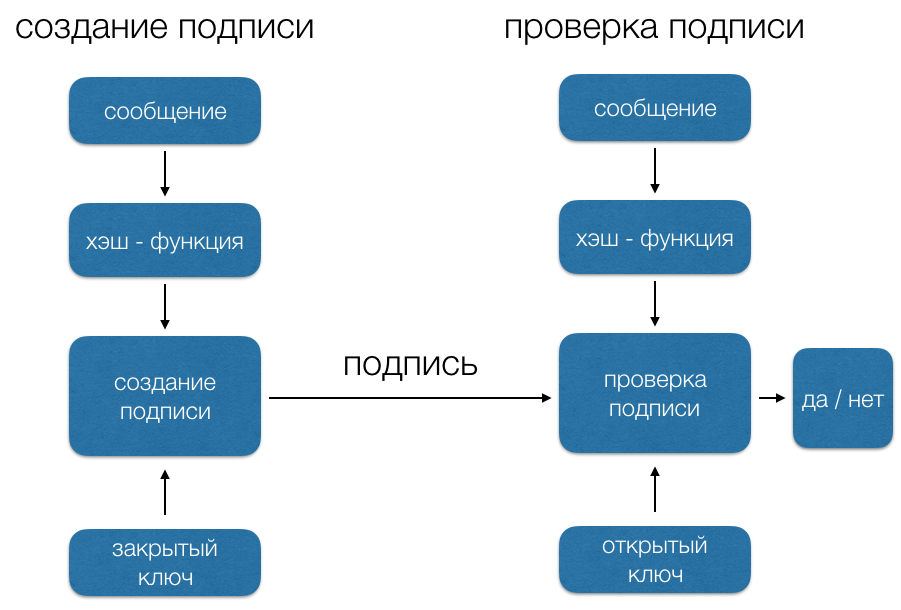


Рисунок 8 – Пример работы алгоритмы DSA

Генерация ключей DSA:

1. отправитель выбирает случайное целое число x, 1 < x < q. Число x является секретным ключом отправителя для формирования электронной цифровой подписи;
2. затем отправитель вычисляет значение y=gx mod p. Число y является открытым ключом для проверки подписи отправителя. Число y передается всем получателям документов;

Генерация подписи DSA:

1. выбирается случайное целое k в интервале [1, q – 1];
2. вычисляется r = (gk mod p) mod q;
3. вычисляется s = [k–1{h(M) + xr}] mod q, где h есть алгоритм хэширования SHA-1;
4. если s = 0, тогда перейти к шагу 1;
5. подпись для сообщения М есть пара целых чисел (r, s).

Проверка подписи DSA:

1. получение подлинной копии открытого ключа y участника А;
2. вычисляет w = s–1 mod q и хэш-значение h(М);
3. вычисляет значения u1 = [h(М)w] mod q и u2 = (rw) mod q;
4. используя открытый ключ y, вычисляется значение v = ((gu1yu2)mod p) mod q;
5. признается подпись (r, s) под документом M подлинной, если v = r.

Поскольку r и s являются целыми числами, причем каждое меньше q, подписи DSA имеют длину 320 бит. Безопасность алгоритма цифровой подписи DSA базируется на трудностях задачи дискретного логарифмирования.

ГОСТ Р 34.10-2012 (полное название: «ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи») — российский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи. Принят и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 года № 215-ст вместо ГОСТ Р 34.10-2001. До ГОСТ Р 34.10-2001 действовал стандарт ГОСТ Р 34.10-94.

Цифровая подпись позволяет:

1. аутентифицировать лицо, подписавшее сообщение;
2. контролировать целостность сообщения;
3. защищать сообщение от подделок;
4. доказать авторство лица, подписавшего сообщение.

Данный алгоритм разработан главным управлением безопасности связи Федерального агентства правительственной связи и информации при Президенте Российской Федерации при участии Всероссийского научно-исследовательского института стандартизации. Разрабатывался взамен ГОСТ Р 34.10-94 для обеспечения большей стойкости алгоритма.

ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001 основаны на эллиптических кривых. Стойкость этих алгоритмов основывается на сложности вычисления дискретного логарифма в группе точек эллиптической кривой, а также на стойкости хэш-функции. Для ГОСТ Р 34.10-2012 используется хэш-функция по ГОСТ Р 34.11-2012. Для ГОСТ Р 34.10-2001 — ГОСТ Р 34.11-94.

Эллиптическая кривые описываются уравнением вида

Определение эллиптической кривой также требует, чтобы кривая не имела особых точек. Геометрически это значит, что график не должен иметь каспов и самопересечений. Алгебраически, достаточно проверить, что дискриминант не равен нулю. На рисунках 5-6 представлены различные формы эллиптических кривых

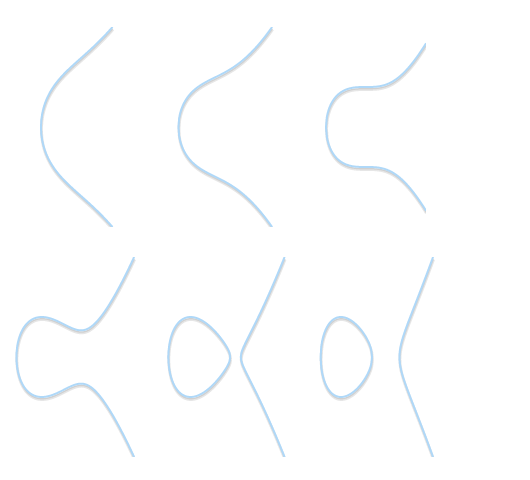


Рисунок 9 – Формы эллиптических кривых (b=1, a изменяется от 2 до -3)



Рисунок 10 – Виды особенностей эллиптических кривых

Установленная в настоящем стандарте схема цифровой подписи должна быть реализована с использованием операций группы точек эллиптической кривой, определенной над конечным простым полем, а также хэш-функции. Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции.

Простая электронная подпись чаще всего применяется при банковских операциях, а также для аутентификации в информационных системах, для получения госуслуг, для заверения документов внутри корпоративного электронного документооборота (далее — ЭДО). Простую электронную подпись нельзя использовать при подписании электронных документов или в информационной системе, которые содержат гостайну. Простая подпись приравнивается к собственноручной, если это регламентирует отдельный нормативно-правовой акт или между участниками ЭДО заключено соглашение, где прописаны:

1. правила, по которым подписанта определяют по его простой электронной подписи;
2. обязанность пользователя соблюдать конфиденциальность закрытой части ключа ПЭП (например, пароля в паре “логин-пароль” или СМС-кода, присланного на телефон).

Во многих информационных системах пользователь должен сначала подтвердить свою личность во время визита к оператору систему, чтобы его ПЭП в будущем имела юридическую силу. Например, для получения подтвержденной учетной записи на портале Госуслуг, нужно лично прийти в один из центров регистрации с документом, удостоверяющим личность.

Усиленная неквалифицированная электронная подпись (далее — НЭП) создается с помощью программ криптошифрования с использованием закрытого ключа электронной подписи. НЭП идентифицирует личность владельца, а также позволяет проверить, вносили ли в файл изменения после его отправки. Человек получает в удостоверяющем центре два ключа электронной подписи: закрытый и открытый. Закрытый ключ хранится на специальном ключевом носителе с пин-кодом или в компьютере пользователя. С помощью закрытого ключа владелец генерирует электронные подписи, которыми подписывает документы. Открытый ключ электронной подписи связан с закрытым ключом ЭП и предназначен для проверки подлинности ЭП. Открытый ключ доступен всем, с кем его обладатель ведет ЭДО. Соответствие открытого ключа владельцу закрытого ключа прописывается в сертификате электронной подписи, который также выдается удостоверяющим центром. Требования к структуре неквалифицированного сертификата не установлены в федеральном законе № 63-ФЗ “Об электронной подписи”. При использовании НЭП сертификат можно не создавать.

НЭП используется в электронных госзакупках по 44-ФЗ в качестве поставщика на шести федеральных электронных торговых площадках госзакупок. Этот же вид подписи можно использовать для внутреннего и внешнего ЭДО, если стороны предварительно договорились об этом.

Усиленная квалифицированная электронная подпись — самый регламентированный государством вид подписи. Так же, как и НЭП, она создается с помощью криптографических алгоритмов и базируется на инфраструктуре открытых ключей, но отличается от НЭП в следующем:

1. обязательно имеет квалифицированный сертификат в бумажном или электронном виде, структура которого определена приказом ФСБ России № 795 от 27.12.2011;
2. программное обеспечение для работы с КЭП сертифицировано ФСБ России;
3. выдавать КЭП может только удостоверяющий центр, который аккредитован Минкомсвязи России;

Усиленная квалифицированная электронная подпись нужна, чтобы сдавать отчетность в контролирующие органы, участвовать в качестве поставщика и заказчика в электронных торгах, работать с государственными информационными системами, обмениваться формализованными документами с ФНС, вести электронный документооборот внутри компании или с ее внешними контрагентами.

**3 Криптографические протоколы**

Каждый криптографический протокол предназначен для решения определенной задачи и имеет следующие свойства:

1. при выполнении протокола важен порядок действий;
2. каждое действие должно выполняться в свою очередь и только по окончании предыдущего;
3. протокол должен быть непротиворечивым;
4. протокол должен быть полным, то есть для каждой возможной ситуации должно быть предусмотрено соответствующее действие.

Свойства протокола напоминают известные свойства алгоритма. В криптографических протоколах используются стандарты шифрования, представленные на (рис. 11)

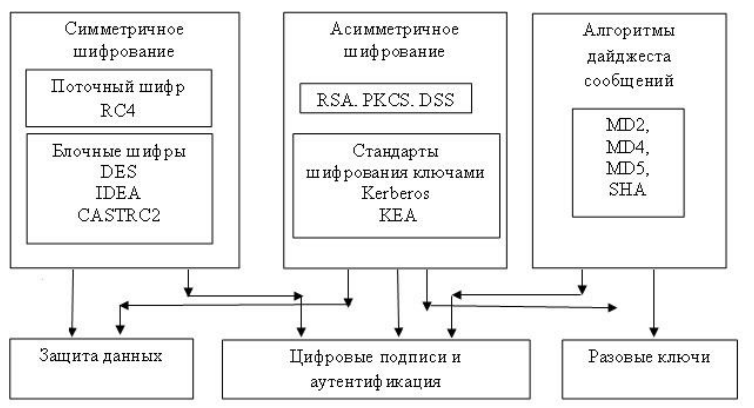


Рисунок 11 – Криптографические методы

Назначение некоторых видом протоколов:

1. протоколы конфиденциальной передачи сообщений;
2. протоколы аутентификации и идентификации;
3. протоколы распределения ключей;
4. протоколы электронной цифровой подписи;
5. протоколы обеспечения неотслеживаемости.

Протоколы конфиденциальной передачи сообщений. Задача конфиденциальной передачи сообщений состоит в следующем. Имеются два участника протокола, которые являются абонентами сети связи. Участники соединены некоторой линией связи, по которой можно пересылать сообщения в обе стороны. Линию связи может контролировать противник. У одного из абонентов имеется конфиденциальное сообщение m, и задача состоит в том, чтобы это сообщение конфиденциальным же образом передать второму абоненту. Протоколы этого типа, наверно, появились раньше других криптографических протоколов, так как задача конфиденциальной передачи сообщений – исторически первая задача, которая решалась криптографией.

Протоколы аутентификации и идентификации. Они предназначены для предотвращения доступа к некоторой информации лиц, не являющихся ее пользователями, а также предотвращения доступа пользователей к тем ресурсам, на которые у них нет полномочий. Типичная сфера применения – организация доступа пользователей к ресурсам некоторой большой информационной системы.

Протоколы распределения ключей необходимы для обеспечения секретными ключами участников обмена зашифрованными сообщениями.

Протоколы электронной цифровой подписи позволяют ставить под электронными документами подпись, аналогичную обыкновенной подписи на бумажных документах. В результате выполнения протокола электронной цифровой подписи к передаваемой информации добавляется уникальное числовое дополнение, позволяющее проверить ее авторство.

Протоколы обеспечения неотслеживаемости ("Электронные деньги"). Под электронными деньгами в криптографии понимают электронные платежные средства, обеспечивающие неотслеживаемость, то есть невозможность проследить источник пересылки информации.

Для современных криптографических систем защиты информации сформулированы следующие требования:

1. зашифрованное сообщение должно поддаваться чтению только при наличии ключа;
2. знание алгоритма шифрования не должно влиять на надежность защиты;
3. любой ключ из множества возможных должен обеспечивать надежную защиту информации;
4. алгоритм шифрования должен допускать как программную, так и аппаратную реализацию.

Примером криптографического протокола распределения ключей может быть протокол Диффи – Хеллмана. Для его выполнения стороны должны договориться о значениях большого простого числа p и образующего элемента α мультипликативной группы. Для выработки общего ключа k они должны сгенерировать случайные числа x, 1<=x<=p-2, и y, 1<=y<=p-2, соответственно. Затем они должны обменяться сообщениями.

Искомый общий ключ теперь вычисляется по формуле

Слабость: отсутствие аутентификации сторон.

Примером атаки на данный криптографический протокол может быть атака «человек посередине»:

1. выбираются числа x∗ и y∗;
2. подменяются ax и ay на ax\* и ay\* соответственно;
3. вычисляются ключи kAC= axy\* mod p и kCB= ayx\* mod p

В результате чего злоумышленник полностью контролирует обмен сообщениями между участниками.

Протокол, предложенный Т. Мацумото, И. Такашима и Х. Имаи в 1986г, является подходом к защите протокола DH от атаки «человек посередине». Была предложена серия протоколов предполагающих наличие у абонентов открытых ключей и использующих различные модификации процедуры выработки общего ключа.

Предположим, что участники A и B имеют секретные ключи a, 1<=a<=p-2, и b, 1<=b<=p-2, соответственно и публикуют свои открытые ключи βA = αa mod p и βB = αb mod p. Для выработки общего секретного ключа k они должны сгенерировать случайные числа x, 1<=x<=p-2, и y, 1<=y<=p-2, соответственно, после чего происходит обмен сообщениями. После чего участники вычисляют общий ключ k=axb+ya mod p.

Любая подмена сообщений приводит к тому, что все стороны получают различные значения ключа, в результате чего становится невозможным чтение всей передаваемой информации. Тем самым свойство аутентификации ключа протокола при атаке «противник в середине» не нарушено. Вместе с тем этот протокол не обеспечивает аутентификации сторон и подтверждения правильности получения ключа. Данный протокол хотя и обеспечивает аутентификацию ключа для участника A, в то же время не обеспечивает аутентификации сторон, а также аутентификации ключа для участника B.

Другим примером протокола может являться протокол STS(station-to-station), созданный У.Диффи, П. Ван Ооршотом и М.Вайнером. Вставка во второе и третье сообщения протокола значений цифровых подписей позволяет гарантировать достоверность получения сообщения именно от того пользователя, от которого это сообщение получено. Шифрование значений подписей пользователей с помощью симметричного алгоритма E введено для того, чтобы обеспечить взаимное подтверждение правильности вычисления значения ключа, так как при неверно вычисленном ключе невозможно получить верные значения цифровых подписей. Примером атаки на данный протокол может служить атака с неизвестным общим ключом. Нарушитель C, используя свой законный обмен с участником B, может применить против участника A атаку, в результате которой он может убедить A в том, что он выступает от имени B. Нарушитель C использует свой законный обмен с участником B и убеждает A в том, что он выступает от имени B. Сеанс с участником B остается незавершенным, так как C, не зная секретного ключа участника A, не сможет подобрать правильный ответ для B. Поэтому любое его сообщение на третьем шаге будет участником B отвергнуто. Данная атака не представляет реальной опасности, так как при этом нарушитель небудет знать секретного ключа k = αxy mod p и поэтому не сможет читать передаваемые сообщения, передаваемые от A к B. Однако в результате участник A не будет ничего подозревать и примет участника C за B. Таким образом, протокол не обеспечивает: аутентификации сторон, аутентификации ключа для участника B, так как последний будет полагать, что сформировал общий ключ с участником C, а на самом деле — с участником A.

Имеется большое число типов атак, которые зависят от конкретной реализации протокола. Например, для криптографических протоколов на основе симметричных шифрсистем можно использовать особенности работы самих шифрсистем и, в частности, реализованных способов и режимов шифрования, синхронизации и т. п. Чтобы защититься от подобных атак, необходимо провести анализ архитектуры протокола и структуры передаваемых сообщений с целью определения возможных уязвимостей, позволяющих, например, осуществить навязывание сообщений с известными или одинаковыми значениями определенных полей, либо с помощью подмены типа некоторых полей.

Для криптографических протоколов, построенных на основе асимметричных шифрсистем, основной уязвимостью является возможность осуществления подмены открытого ключа одного из участников на другой открытый ключ с известной противнику секретной половиной этого ключа. В частности, это позволяет противнику узнавать содержание зашифрованных сообщений, отправляемых данному участнику. В данном случае нарушается свойство связанности открытого ключа и идентификатора участника. Поэтому атаку данного типа называют атакой на основе связывания (binding attack). Для защиты от подобных атак вместо открытых ключей используют их сертификаты, создавая специальную инфраструктуру (PKI) для выдачи, отзыва и проведения проверки их правильности.

**Заключение**

В ходе аналитического обзора были рассмотрены основные модели передачи сообщений. Рассмотренные модели можно поделить на две группы:

1. модели передачи без злоумышленников;
2. модели передачи с злоумышленником.

Первая группа моделей имеет более простую реализацию, так как не проводятся проверки на наличие изменение в передаваемом сообщении. Но данная группа имеет недостаток, так как в определенных случая злоумышленник может либо получить информацию, либо может изменить ее содержание, что может привести к серьезным последствиям.

Вторая группа моделей рассматривает передачу сообщений, в которой может принимать участие третья сторона. В таких случаях необходимо осуществить защиту передаваемого сообщения соответствующими криптографическими протоколами.

Криптографические протоколы – это порядок действий, осуществляемый при передачи информации. Протоколы могут осуществлять конфиденциальную передачу сообщений, аутентификацию и идентификацию, распределение ключей, создание электронной цифровой подписи, обеспечение неотслеживаемости.

Каждый из криптографических протоколов использует один из двух методов шифрования:

1. ассиметричное;
2. симметрично.

Шифрование сообщений необходимо для защиты сообщения. Симметричное шифрование работает быстрее, но имеет недостаток в способе распространения закрытого ключа. Асимметричное шифрование позволяет передавать открытый ключ по незащищенному каналу связи.

Таким образом, в результате обзора была рассмотрены:

1. четыре модели передачи сообщений;
2. симметричное и асимметричное шифрование, их достоинства и недостатки;
3. примеры криптографических протоколов, использующиеся при передаче сообщений;
4. примеры возможных видов атак на протоколы.

**Список использованных источников информации**

1. Коржик, В. И. Основы криптографии: монография / В. И. Коржик, В.А. Яковлев. – Санкт-Петербург: Интермедия, 2016 – 296 с. – Текст : непосредственный .

2. Krishna Chaitanya Nunna. Secure Data Transfer Through Internet Using Cryptography and Image Steganography / Krishna Chaitanya Nunna – Текст : непосредственный // IEEE. – 2017. – №.12 – 7 p.

3. Смирнова, М. А. Асимметричное шифрование как способ проверки подлинности автора сообщения / М. А. Смирнова, И. А. Самойлова, Л. В. Устинова– Текст : непосредственный //Актуальные проблемы современности. – 2017. – № 2. – 5 с.

4. Xiaojuan Chen. Analysis of Cryptographic Protocol by Dynamic Epistemic Logic / Xiaojuan Chen, Huiwen Deng – Текст : непосредственный // IEEE. – 2019. – № 7. – 7 p.

5. Романьков, В. А. Алгебраическая криптография : монография / В. А. Романьков. – Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. – 136 c. – Текст : непосредственный.

6. Lee, J. A Theory of Secure Communication. Doctoral dissertation / J. Lee; Universitat Karlsruhe . – DE. – 2014. – 231 p. – Текст: непосредственный.

7. Умрзоков, С. Криптографические протоколы / С. Умрзоков – Текст : непосредственный // Мировая наука. – 2029. – № 6. – 5 с.

8. Новиков, С. Н. Методология зашиты информации на основе технологий сетевого уровня мультисервисных сетей связи : специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : диссертация на соискание ученой степени доктора технических наук / Новиков Сергей Николаевич; Томский государственный университет систем управления и радиоэлектроники. – Томск, 2016. – 235с. – Текст: непосредственный.

9. Сизоненко, А. Б. Модели и алгоритмы синтеза логико-вычислительных подсистем защиты информации систем критического применения : специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность» : диссертация на соискание ученой степени доктора технических наук / Сизоненко Александр Борисович; Воронежский институт МВД РФ. – Воронеж, 2016. – 310 с. – Текст: непосредственный.

10. Патент № 2617972 Российская Федерация, МПК RU 2016617549 A (20.06.2016. Криптографическое шифрование: № 2016108116 : заявл. 18.05.2016 : опубл. 07.07.2016 / Насыров Ринат Ришатович, Сулейманов Игорь Рашидович, Чуркин Андрей Игоревич.; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (RU). – 2 с. : ил. – Текст : непосредственный.

11. United States Patent №: US US2005235342A1, IPC G06F21/00; H04L9/00; (IPC1-7): H04L9/00 . Cryptography correctness detection methods and apparatuses : Appl. No.: 15/371,117 : 16.01.2004 : Publication: 20.10.2005; Assignee: Microsoft Corp. (US). – 17 p. – Текст : непосредственный.

**Выводы по отчету**

1. Выполнено описание используемых в обзоре источников информации и составлены расширенные аннотации:

– отечественных монографий: 1;

– зарубежных монографий: 1;

– отечественных статей: 3;

– зарубежных статей: 2;

– отечественных диссертаций: 1;

– зарубежных диссертаций: 1;

– депонированных рукописей: 1;

– отечественных публикаций в материалах НТК: 1;

– зарубежных публикаций в материалах НТК: 1;

– отчетов о НИР: 1;

–патентов РФ: 1;

– зарубежных патентов (США): 1.

2. Выполнен аналитический обзор научно-технической информации по теме исследований “Разработка программной системы для 3D-моделирования эвакуации людей при чрезвычайных ситуациях”:

– объем: 20 страниц;

– разделов: 3;

– рисунков: 10;

– таблиц: 0;

– формул: 1;

– количество источников информации: 11.

3. Наиболее близкими статьями (трудами, публикациями, тезисами и т.п.) к теме проводимых исследований “ Разработка программы моделирования передачи сообщений с асимметричным и симметричным шифрованием данных :

3.1 Коржик, В. И. Основы криптографии: монография / В. И. Коржик, В.А. Яковлев. – Санкт-Петербург: Интермедия, 2016 – 296 с. – Текст : непосредственный.

3.2 Смирнова, М. А. Асимметричное шифрование как способ проверки подлинности автора сообщения / М. А. Смирнова, И. А. Самойлова, Л. В. Устинова– Текст : непосредственный //Актуальные проблемы современности. – 2017. – № 2. – 5 с.

4. Наиболее близкими патентами к теме проводимых исследований “Разработка программной системы для 3D-моделирования эвакуации людей при чрезвычайных ситуациях” являются:

4.1 Патент № 2617972 Российская Федерация, МПК RU 2016617549 A (20.06.2016. Криптографическое шифрование: № 2016108116 : заявл. 18.05.2016 : опубл. 07.07.2016 / Насыров Ринат Ришатович, Сулейманов Игорь Рашидович, Чуркин Андрей Игоревич.; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова» (RU). – 2 с. : ил. – Текст : непосредственный.

4.2 United States Patent №: US US2005235342A1, IPC G06F21/00; H04L9/00; (IPC1-7): H04L9/00 . Cryptography correctness detection methods and apparatuses : Appl. No.: 15/371,117 : 16.01.2004 : Publication: 20.10.2005; Assignee: Microsoft Corp. (US). – 17 p. – Текст : непосредственный.