**3. Криптография и Защита Данных**

* Основы криптографии: симметричные и асимметричные шифры.

Симметричное и ассиметричное шифрование: просто о сложном

**Криптографическая защита данных** — важнейшая задача, которая сегодня актуальна, как никогда. Однако до сих пор некоторые спорят, что лучше — **симметричное или ассиметричное шифрование**? Что круче — AES или RSA? Однако все эти споры — бесполезное занятие и результат непонимания сути **криптографии**. Без упоминания конкретики (условий и задач использования) нельзя сказать, что однозначно лучше. В этой статье мы попробуем разобрать особенности ассиметричного и симметричного шифрования, увидим их разницу, приведём аргументы в пользу того либо иного подхода.

Мы расскажем базовый минимум, который должен знать каждый. Никаких математических обоснований и сложных формул не будет, поэтому готовьтесь к приятному и лёгкому чтению)).



**Симметричное шифрование**

Для работы применяется всего один пароль. Происходит всё следующим образом: 1. Существует некий математический алгоритм шифрования. 2. На его вход подаётся текст и пароль. 3. На выходе получаем зашифрованный текст. 4. Если хотим получить исходный текст, применяется тот же самый пароль, но с алгоритмом дешифрования.

Говоря простым языком, если кто-то узнает наш пароль, безопасность криптосистемы тут же нарушится. Именно поэтому, используя подходы симметричного шифрования, мы должны особое внимание уделять **вопросам создания и сохранения конфиденциальности пароля**. Он должен быть сложным, что исключит подбор программным перебором значений. И не должен передаваться кому-нибудь в открытом виде как в сети, так и на физических носителях информации. Очевидно, что листочек, прикреплённый к монитору — явно не лучший вариант)). Тем не менее если наша секретная комбинация используется командой, нужно обеспечить безопасность её распространения. Пригодится и система оповещения, которая сработает, если шифр узнают, произойдёт утечка данных.

Несмотря на свои ограничения и угрозу безопасности, подход до сих пор широко распространён в криптографии. Дело в том, что он очень прост в работе и понимании. И техническая нагрузка на железо невелика (как правило, всё работает очень быстро).

**Ассиметричное шифрование**

Здесь применяют 2 пароля — публичный (открытый) и секретный (закрытый). Первый отсылается всем людям, второй остаётся на стороне сервера. Эти названия достаточно условные, а зашифрованное одним из ключей сообщение можно расшифровать лишь с помощью другого. По сути и значимости они равноценны.

Данные **алгоритмы шифрования** дают возможность без проблем распространять пароли по сети, ведь не имея 2-го ключа, любое исходное сообщение останется для вас непонятным шифром. Кстати, на этом принципе работает и протокол SSL, позволяющий устанавливать безопасные соединения с пользователями, т. к. закрытый ключ есть только на стороне сервера.

Для **ассиметричного шифрования** хранение паролей проще, ведь секретный ключ не нужно передавать кому-либо. А в случае взлома сервер сменит пару ключей и разошлёт всем новые комбинации.

Считается, что ассиметричное шифрование «тяжелее» симметричного. Всё потому, что оно требует больше компьютерных ресурсов. Есть ограничения и на процесс генерации ключей.

Как правило, возможности ассиметричного шифрования используют для выполнения **идентификации пользователей** (например, при входе на сайт). Или с его помощью создают сессионный ключ для симметричного шифрования (речь идёт о временном пароле для обмена данными между сервером и пользователем). Или формируют зашифрованные цифровые подписи. В последнем случае проверить такую подпись может каждый, используя публичный ключ, находящийся в открытом доступе.

**Что важно знать**

Давайте перечислим основные моменты и сравним оба вида шифрования: 1. **Симметричный алгоритм** прекрасно подходит при передаче больших объёмов зашифрованных данных. Ассиметричный в этом случае будет работать медленнее. Кроме того, при организации обмена информацией по ассиметричному алгоритму оба ключа должны быть известны обеим сторонам либо пар должно быть две (по одной на каждую сторону). 2. **Ассиметричное шифрование** позволяет дать старт безопасному соединению без каких-либо усилий со стороны пользователя. Если говорить о симметричном шифровании, то пользователю нужно знать пароль. Однако не стоит думать, что ассиметричный подход безопасен на 100 %. К примеру, он подвержен атакам «человек посередине». Это когда между сервером и вами размещается компьютер, который вам отсылает свой открытый ключ, а при передаче информации с вашей стороны, использует открытый ключ сервера. В итоге происходит перехват конфиденциальных данных. 3. **Продолжая тему взлома** и компрометации пароля, давайте ещё раз отметим, что в случае с симметричным шифрованием возникает проблема конфиденциально передать следующий пароль. В этом плане ассиметричный алгоритм «легче». Серверу достаточно сменить пару и разослать вновь созданный публичный ключ. Однако и тут есть своя Ахиллесова пята. Дело в том, что генерация ключей постоянно происходит по одному и тому же алгоритму, стало быть, если его узнают, безопасность окажется под угрозой. 4. **Симметричный шифр** обычно строится на основании ряда блоков с математическими функциями преобразования, ассиметричный — на математических задачах. Тот же RSA создан на задаче возведения в степень с последующим вычислением модуля. В результате алгоритмы симметричного шифрования модифицировать просто, а ассиметричного — практически невозможно. 5. Лучший эффект достигается **при комбинации** обоих видов шифрования. Происходит это так: — посредством ассиметричного алгоритма серверу отсылается сессионный ключ для симметричного шифрования; — происходит обмен информацией по симметричному алгоритму. Тут возможны варианты, но общий смысл обычно не меняется. 6. В симметричном шифровании **пароли генерируются** по специальным правилам с учётом цифр, букв, регистра и т. д., создаются комбинации повышенной сложности. В ассиметричном пароли не так безопасны, однако их секретность обеспечивается тем, что их знает только сервер. 7. Вне зависимости от выбранного вида шифрования **ни один из них** не является гарантом стопроцентной безопасности. Помните, что любой подход нужно комбинировать с другими средствами информационной защиты.

**Послесловие**

Как видим, области применения у обоих типов шифрования разные, поэтому при выборе нужно соотносить возможности алгоритмов с поставленными задачами. Может быть, использовать гибридные решения.

Следует учитывать и практическую целесообразность. Допустим, если ваша программа предназначена только для персонального пользования, вряд ли будет рациональным использовать ассиметричный подход. Лучший вариант здесь — мощный симметричный алгоритм.

Как бы там ни было, получить более глубокие знания вы всегда сможете на нашем курсе «[Криптографическая защита информации](https://otus.ru/lessons/cryptography/)». Вы подробно узнаете про симметричное и ассиметричное шифрование, блочные шифры, строение криптосистем, режимы шифрования, прикладные аспекты криптографии и многое другое.

Вы, возможно, помните, как в детстве с помощью символов писали одноклассникам закодированные сообщения, которые никто, кроме вас самих, не мог понять. Но если говорить серьёзнее, коды и шифры используются для **обеспечения информационной безопасности в компьютерных системах и сетях** для защиты конфиденциальной и коммерческой информации от несанкционированного доступа, когда она находится на хранении или при её передаче между адресатами. Сфера применения шифрования включает в себя все: от сохранения военных секретов до безопасной передачи финансовых данных через интернет.

Криптография - это важный инструмент компьютерной безопасности, который включает в себя методы **хранения и передачи информации таким образом, чтобы предотвратить несанкционированный доступ к ним или вмешательство в их целостность**.

**Как криптография обеспечивает секретность и безопасность связи**

Криптографический процесс преобразования текста из читаемой формы в неразборчивую - известную как шифрованный текст - называется шифрованием. Отправка секретных или частных сообщений в виде шифрованного текста является типичным применением криптографии. После получения зашифрованного текста он дешифруется уполномоченным получателем в читаемую форму. Дешифровка (или расшифровка) выполняется с использованием ключа шифрования, который служит для того, чтобы третьи лица не смогли прочитать пересылаемые сообщения.

Методы шифрования использовались многими цивилизациями на протяжении всей истории человечества для предотвращения понимания сообщений неуполномоченными лицами. Юлию Цезарю приписывают одну из самых ранних форм шифрования — так называемый шифр Цезаря — для передачи сообщений своим генералам. С развитием цивилизации и усложнением передаваемой информации к нашему дню криптография стала играть жизненно важную роль в обеспечении приватности, конфиденциальности данных, их целостности и аутентификации в компьютерных системах и сетях. В современном мире, где большинство наших личных и профессиональных коммуникаций и транзакций осуществляется в режиме онлайн, криптография важна как никогда.

**Типы криптографических систем**

Криптография относится к техникам и алгоритмам, которые используются в настоящее время для безопасной связи и хранения данных, и включает в себя математику, информатику, электронику и цифровую обработку сигналов. В широком смысле, существует четыре типа криптографических систем:

* **Криптография с симметричным ключом (или "секретным ключом"):**В данном типе системы и отправитель, и получатель имеют один и тот же ключ, который используется для шифрования и дешифрования сообщения.
* **Криптография с асимметричным ключом (или "открытым ключом"):**В данном типе криптографической системы существует два ключа - открытый и закрытый; они образуют пару и связаны между собой математически. Для применения асимметричной криптографии отправитель использует открытый ключ предполагаемого получателя для кодирования сообщения, а затем отправляет его в путь. Когда сообщение приходит, только закрытый ключ получателя может быть использован для его декодирования, что означает, что украденное сообщение не может быть полезным для вора без соответствующего закрытого ключа. Механизмы шифрования находятся в центре внимания [ISO/IEC 18033](https://www.iso.org/ru/standard/76156.html), набора международных стандартов, который определяет ряд асимметричных шифров. Многокомпонентная серия включает шифры, основанные на идентификации, блочные шифры, потоковые шифры и гомоморфное шифрование.
* **Управление криптографическими ключами:**Данный тип системы имеет решающее значение для защиты ключей, используемых как в симметричной, так и в асимметричной криптографии. Она включает в себя набор процессов, охватывающих весь "жизненный цикл" ключа, включая его генерацию, обмен и распространение, хранение, использование, безопасное уничтожение и замену. Если управление ключами слабое, то и защита зашифрованных данных не может быть сильной. Существует ряд международных стандартов, касающихся управления ключами (например, [ISO/IEC 11770](https://www.iso.org/ru/standard/53456.html)) и генерации ключей (например, [ISO/IEC 18031](https://www.iso.org/ru/standard/54945.html) и [ISO/IEC 18032](https://www.iso.org/ru/standard/72009.html)).
* **Криптографическая хэш-функция:** Это метод, который преобразует строку данных любой длины в хэшированный результат (хэш-сумма входных данных) фиксированной длины. Хэш-функции имеют множество применений, например, в цифровых подписях, MAC (кодах аутентификации сообщений) и контрольных суммах (для проверки повреждения данных). Международные стандарты, определяющие хэш-функции, включают [ISO/IEC 9797-2](https://www.iso.org/ru/standard/75296.html), [ISO/IEC 9797-3](https://www.iso.org/ru/standard/51619.html) и [ISO/IEC 10118](https://www.iso.org/ru/standard/64213.html).

**Принципы информационной безопасности и использование криптографии**

Ключевыми принципами информационной безопасности являются конфиденциальность, целостность и доступность. Криптография является важным инструментом, который помогает сохранить два из этих принципов:

* **Конфиденциальность данных** гарантирует, что данные не будут раскрыты неавторизованным лицам. Криптографические методы, такие как шифрование, могут использоваться для защиты конфиденциальности данных, делая их абсолютно нечитаемыми для тех, у кого нет соответствующего ключа для их расшифровки.
* **Целостность данных**гарантирует, что данные не были изменены или повреждены. Одним из примеров международных стандартов по целостности данных является ISO/IEC 9797, который определяет алгоритмы вычисления кодов аутентификации сообщений.

В дополнение к вышеописанным ключевым целям информационной безопасности криптография используется для достижения таких целей, как:

**Аутентификация субъекта**

Путем проверки знания определенного секрета, аутентификация субъекта проверяет личность отправителя. Для этого могут использоваться различные криптографические механизмы и протоколы, такие как симметричные системы, цифровые подписи, методы нулевого знания и контрольные суммы. ISO/IEC 9798 - это серия стандартов, определяющих протоколы и методы аутентификации субъектов.

**Цифровые подписи**

Используемые для проверки подлинности данных, цифровые подписи подтверждают, что данные исходят именно от подписанта и не были изменены. Они используются, например, в сообщениях электронной почты, электронных документах и онлайн-платежах. Международные стандарты, определяющие схемы цифровой подписи, включают ISO/IEC 9796, ISO/IEC 14888, ISO/IEC 18370 и ISO/IEC 20008.

**Неотказуемость**

Криптографические методы, такие как цифровые подписи, могут использоваться для обеспечения неотказуемости, гарантируя, что отправитель и получатель сообщения не смогут отрицать, что они, соответственно, отправили или получили это сообщение. В стандарте ISO/IEC 13888 описаны методы (симметричные и асимметричные) для предоставления услуг по обеспечению неотказуемости.

**Облегченная криптография**

Облегченная криптография используется в приложениях и технологиях, которые ограничены по сложности вычислений: ограничивающими факторами могут быть память, мощность и вычислительные ресурсы. Потребность в облегченной криптографии растет в нашем современном цифровом мире. Ограниченные устройства - например, датчики IoT (Интернет вещей) или исполнительные механизмы, например, включающие электроприборы в так называемом умном доме - используют облегченную симметричную криптографию. ISO/IEC 29192 - это стандарт из восьми частей, который определяет различные криптографические методы для легких приложений.

**Управление цифровыми правами**

Управление цифровыми правами (УЦП) защищает авторские права на ваш цифровой контент. УЦП использует криптографическое программное обеспечение для гарантии того, что только авторизованные пользователи смогут иметь доступ к материалу, изменять или распространять его.

**Электронная коммерция и интернет-магазины**

Безопасная электронная коммерция становится возможной благодаря использованию шифрования с асимметричным ключом. Криптография играет важную роль в онлайн-покупках, поскольку она защищает информацию о кредитных картах и связанных с ними личными данными, а также историю покупок и транзакций клиентов.

**Криптовалюты и блокчейн**

Криптовалюта - это цифровая валюта, использующая криптографические методы для обеспечения безопасности транзакций. Каждая монета криптовалюты подтверждается с помощью технологий распределенного реестра (например, блокчейн). В данном случае реестр представляет собой постоянно растущий список записей - известных как блоки - которые связаны между собой с помощью криптографии.

**Что такое криптографические алгоритмы?**

Криптографический алгоритм - это математический процесс кодирования текста, делающий его нечитаемым. Криптографические алгоритмы используются для обеспечения конфиденциальности данных, целостности данных и их аутентификации, а также для цифровых подписей и других целей сферы обеспечения безопасности.

DES (Data Encryption Standard) и AES (Advanced Encryption Standard) являются популярными примерами алгоритмов с симметричным ключом, в то время как известные алгоритмы с асимметричным ключом включают RSA (Rivest-Shamir-Adleman) и КЭК (криптография эллиптических кривых).

***Криптография эллиптической кривой (КЭК)***

КЭК - это техника асимметричных ключей, основанная на использовании эллиптических кривых, которая находит применение, например, в шифровании и цифровой подписи. Технология КЭК может быть использована для создания более быстрых, компактных и эффективных криптографических ключей. Технологии эллиптических кривых рассматриваются в многокомпонентном стандарте ISO/IEC 15946.

**Стандарты для криптографии**

Криптография была предметом интенсивных усилий по стандартизации, в результате чего был разработан ряд международных стандартов, в которых отражены знания и передовой опыт ведущих экспертов в данной области. Согласованные на международном уровне методы работы делают технологию более безопасной и операционно-совместимой с другими технологиями. Используя стандарты для сферы криптографии, разработчики могут полагаться на общие определения, а также на проверенные методы и технологии.

**Защита криптографии в будущем**

Сегодня мы находимся на пороге квантовой революции. Появление квантовых вычислений в ближайшие годы обеспечит человечество вычислительными мощностями такого масштаба, с которыми традиционные компьютеры никогда не смогут сравниться. Хотя это открывает бесчисленные возможности для решения сложных проблем, но также несет в себе соответствующие угрозы безопасности. Именно эта мощь может подорвать большую часть сегодняшней кибербезопасности, включая устоявшиеся криптографические методы.

Квантовая криптография - это метод шифрования, который использует принципы квантовой механики для обеспечения безопасной связи. Она использует квантовую запутанность для генерации секретного ключа для шифрования сообщения в двух отдельных местах, что делает (почти) невозможным для подслушивающего перехват сообщения без изменения его содержания. Рассматриваемая как следующая большая революция в системах безопасной связи, квантовая криптография может стать настоящим прорывом для данных, которые должны оставаться конфиденциальными далеко в будущем.