

Криптографические методы защиты информации

Основы информационной безопасности



Определение

- **Криптографическое преобразование** - это преобразование информации, основанное на некотором алгоритме, зависящем от изменяемого параметра (обычно называемого секретным ключом), и обладающее свойством невозможности восстановления исходной информации по преобразованной, без знания действующего ключа, с трудоемкостью меньше заранее заданной.
- Основным достоинством криптографических методов является то, что они обеспечивают **высокую гарантированную стойкость защиты**, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей).

Недостатки криптографического метода

- *К числу основных недостатков криптографических методов следует отнести:*
 - значительные затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации;
 - трудности совместного использования зашифрованной (подписанной) информации, связанные с управлением ключами (генерация, распределение и т.д.);
 - высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены.
- *Криптография делится на два класса: криптография с симметричными ключами и криптография с открытыми ключами.*

Криптография с симметричными ключами

- В *криптографии с симметричными ключами* (классическая криптография) абоненты используют один и тот же (общий) ключ (секретный элемент) как для шифрования, так и для расшифрования данных.
- *Следует выделить следующие преимущества криптографии с симметричными ключами:*
 - относительно высокая производительность алгоритмов;
 - высокая криптографическая стойкость алгоритмов на единицу длины ключа.
- *К недостаткам криптографии с симметричными ключами следует отнести:*
 - необходимость использования сложного механизма распределения ключей;
 - технологические трудности обеспечения неотказуемости.

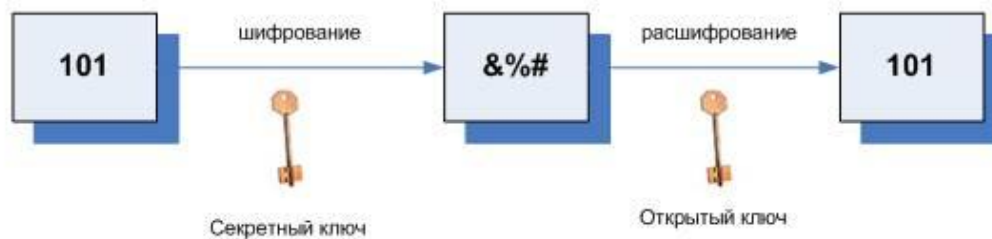
Криптография с открытыми ключами

- Для решения задач распределения ключей были использованы *идеи асимметричности преобразований* и *открытого распределения ключей* Диффи и Хеллмана.
- В результате была создана *криптография с открытыми ключами*, в которой используется не один секретный, а пара ключей: *открытый* (публичный) ключ и *секретный* (личный, индивидуальный) ключ, известный только одной взаимодействующей стороне.
- В отличие от секретного ключа, который должен сохраняться в тайне, открытый ключ может распространяться публично. На Рисунке представлены два свойства систем с открытыми ключами, позволяющие формировать зашифрованные и аутентифицированные сообщения.

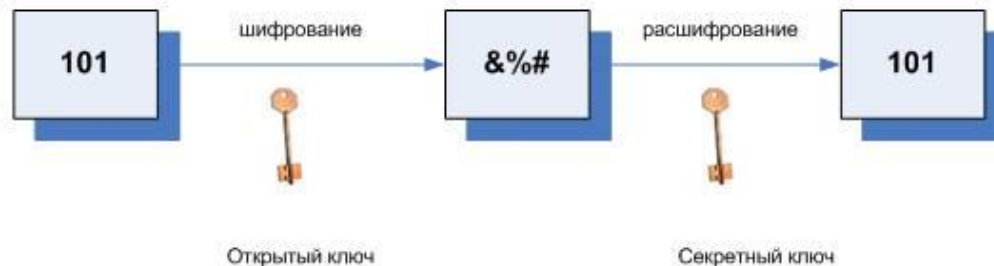
Криптография с открытыми ключами

- *Два важных свойства криптографии с открытыми ключами*

Обладание закрытым ключом
позволяет посылать
аутентифицированные
сообщения



Обладание открытым ключом
позволяет посылать
шифрованные сообщения



Криптография с открытыми ключами

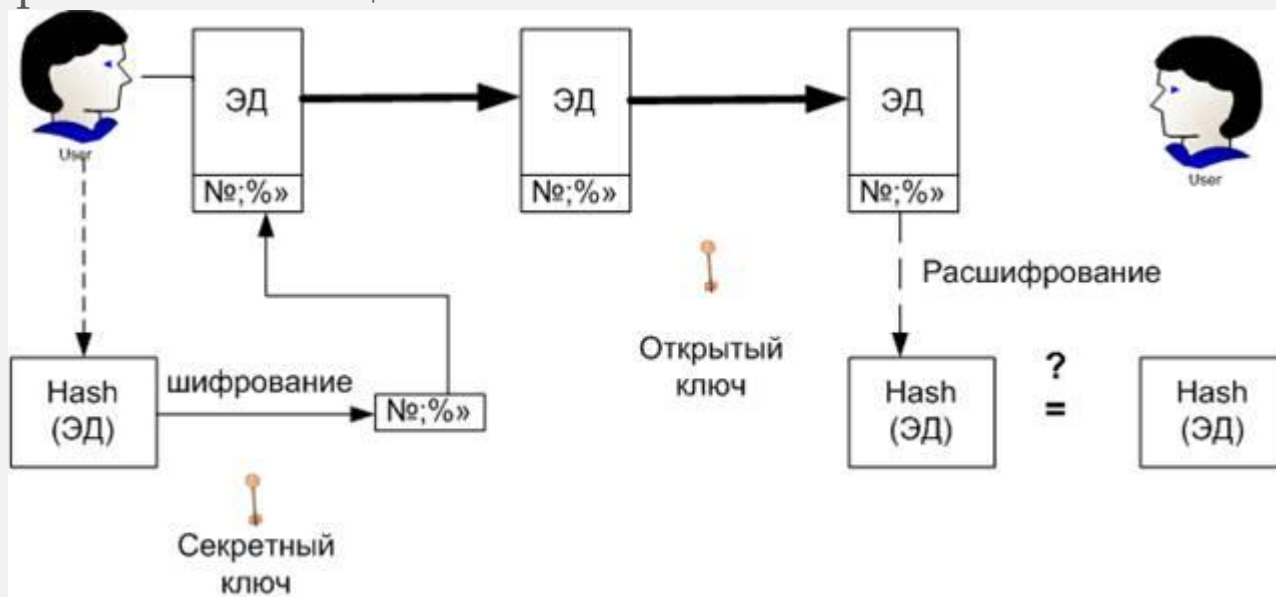
- Схема шифрования данных с использованием открытого ключа состоит из двух этапов.
- *На первом* из них производится обмен по несекретному каналу открытыми ключами. При этом необходимо обеспечить подлинность передачи ключевой информации.
- *На втором этапе*, собственно, реализуется шифрование сообщений, при котором отправитель зашифровывает сообщение открытым ключом получателя.
- Зашифрованный файл может быть прочитан только владельцем секретного ключа, т.е. получателем.
- Схема расшифрования, реализуемая получателем сообщения, использует для этого секретный ключ получателя.

Шифрование

- *Реализация схемы ЭЦП* (электронной цифровой подписи) связана с вычислением *хэш-функции* (дайджеста) данных, которая представляет собой уникальное число, полученное из исходных данных путем его сжатия (свертки) с помощью сложного, но известного алгоритма.
- *Хэш-функция* является однонаправленной функцией, т.е. по хэш-значению невозможно восстановить исходные данные.
- Хэш-функция чувствительна к всевозможным искажениям данных. Кроме того, очень трудно отыскать два набора данных, обладающих одним и тем же значением хэш-функции.

Формирование ЭЦП с хэшированием

- Схема формирования подписи ЭД (электронного документа) его отправителем включает вычисление хэш-функции ЭД и шифрование этого значения посредством секретного ключа отправителя.
- Результатом шифрования является значение ЭЦП ЭД (реквизит ЭД), которое пересылается вместе с самим ЭД получателю. При этом получателю сообщения должен быть предварительно передан открытый ключ отправителя сообщения.



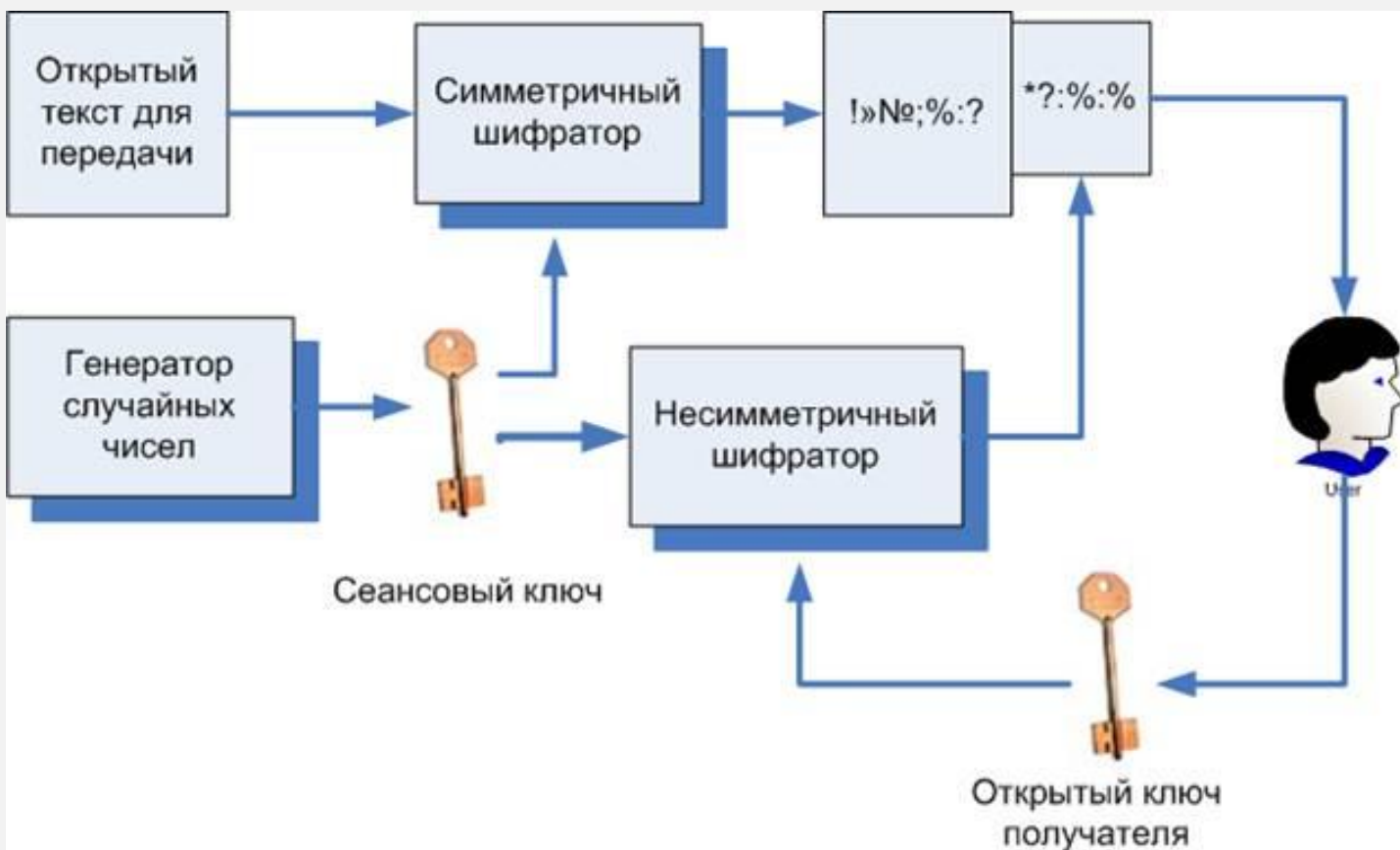
Формирование ЭЦП с хэшированием

- *Схема проверки* (верификации) ЭЦП, осуществляемая получателем сообщения, состоит из следующих этапов.
- *На первом* из них производится расшифрование блока ЭЦП посредством открытого ключа отправителя.
- Затем вычисляется хэш-функция ЭД. Результат вычисления сравнивается с результатом расшифрования блока ЭЦП. В случае совпадения, принимается решение о соответствии ЭЦП ЭД.
- *Несовпадение результата расшифрования с результатом вычисления хэш-функции ЭД может объясняться следующими причинами:*
 - в процессе передачи по каналу связи была потеряна целостность ЭД;
 - при формировании ЭЦП был использован не тот (поддельный) секретный ключ;
 - при проверке ЭЦП был использован не тот открытый ключ (в процессе передачи по каналу связи или при дальнейшем его хранении открытый ключ был модифицирован или подменен).

Формирование ЭЦП с хэшированием

- Реализация *криптографических алгоритмов с открытыми ключами* (по сравнению с симметричными алгоритмами) требует больших затрат процессорного времени. Поэтому *криптография с открытыми ключами обычно используется для решения задач распределения ключей и ЭЦП, а симметричная криптография для шифрования.*
- Широко известна схема комбинированного шифрования, сочетающая высокую безопасность криптосистем с открытым ключом с преимуществами высокой скорости работы симметричных криптосистем.
- В этой схеме для шифрования используется случайно вырабатываемый симметричный (сеансовый) ключ, который, в свою очередь, зашифровывается посредством открытой криптосистемы для его секретной передачи по каналу в начале сеанса связи.

Комбинированный метод



Доверие у открытому ключу

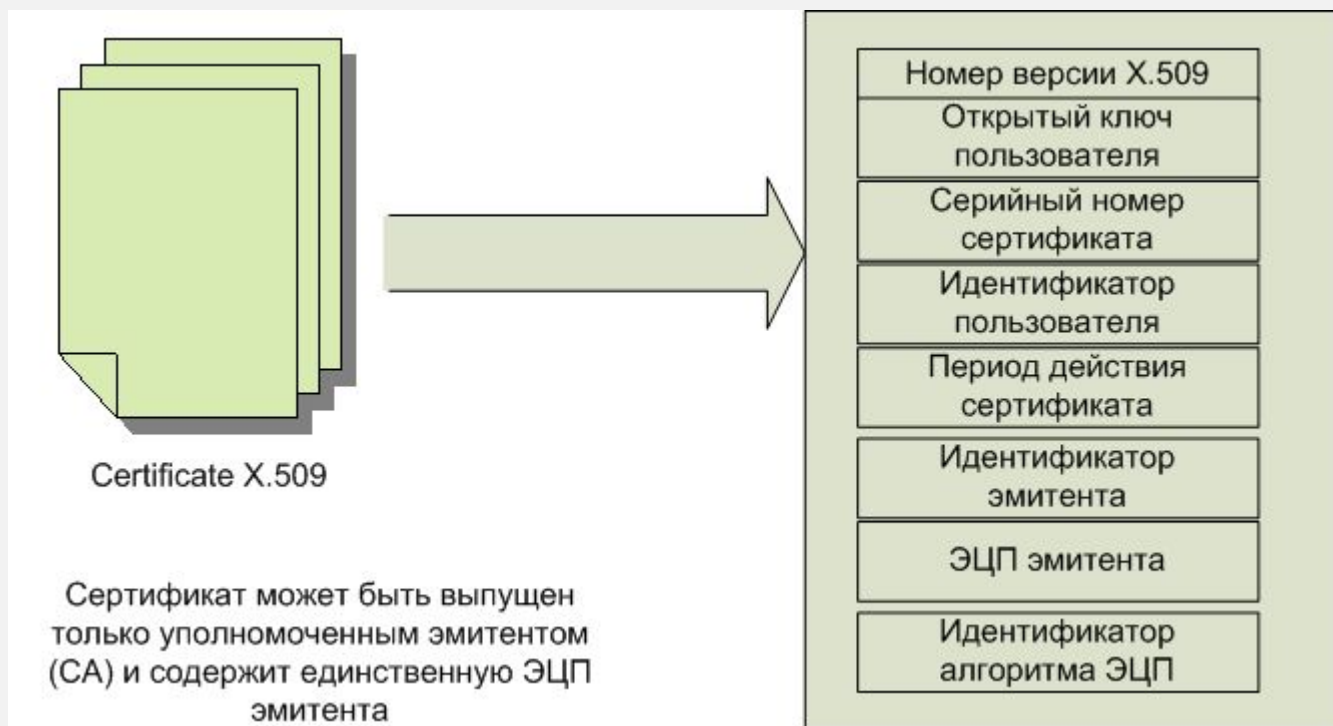
- Центральным вопросом схемы открытого распределения ключей является *вопрос доверия к полученному открытому ключу партнера*, который в процессе передачи или хранения может быть модифицирован или подменен.
- Для широкого класса практических систем (системы электронного документооборота, системы Клиент-Банк, межбанковские системы электронных расчетов), в которых возможна личная встреча партнеров до начала обмена ЭД, эта задача имеет относительно простое решение - *взаимная сертификация открытых ключей*.

Доверие у открытому ключу

- Эта процедура заключается в том, что каждая сторона при личной встрече удостоверяет подписью уполномоченного лица и печатью бумажный документ - *распечатку содержимого открытого ключа другой стороны*.
- Этот бумажный сертификат является, во-первых, *обязательством стороны использовать для проверки подписи под входящими сообщениями данный ключ*, и, во-вторых, *обеспечивает юридическую значимость взаимодействия*.
- Действительно, рассмотренные бумажные сертификаты позволяют однозначно идентифицировать мошенника среди двух партнеров, если один из них захочет подменить ключи.
- Таким образом, для реализации юридически значимого электронного взаимодействия двух сторон необходимо заключить договор, предусматривающий обмен сертификатами.
- *Сертификат* представляет собой документ, связывающий личностные данные владельца и его открытый ключ. В бумажном виде он должен содержать рукописные подписи уполномоченных лиц и печати.

Взаимодействие клиентов с ЦС

- На предварительном этапе каждый из партнеров лично посещает **Центр Сертификации** (ЦС) и получает **личный сертификат** - своеобразный электронный аналог гражданского паспорта.



Взаимодействие клиентов с ЦС

- После посещения ЦС каждый из партнеров становится обладателем *открытого ключа ЦС*.
- Открытый ключ ЦС позволяет его обладателю проверить подлинность открытого ключа партнера путем проверки подлинности ЭЦП удостоверяющего центра под сертификатом открытого ключа партнера.
- *В соответствии с законом "Об ЭЦП" цифровой сертификат содержит следующие сведения:*
 - Наименование и реквизиты центра сертификации ключей (центрального удостоверяющего органа, удостоверяющего центра);
 - Свидетельство, что сертификат выдан в Украине;
 - Уникальный регистрационный номер сертификата ключа;
 - Основные данные (реквизиты) подписчика – собственника приватного (открытого) ключа;
 - Дата и время начала и окончания срока действия сертификата;
 - Открытый ключ;
 - Наименование криптографического алгоритма, используемого владельцем открытого ключа;
 - Информацию об ограничении использования подписи;
 - Усиленный сертификат ключа, кроме обязательных данных, которые содержатся в сертификате ключа, должен иметь признак усиленного сертификата;
 - Другие данные могут вноситься в усиленный сертификат ключа по требованию его владельца.

Взаимодействие клиентов с ЦС

- Этот цифровой сертификат подписан на секретном ключе ЦС, поэтому любой обладатель открытого ключа ЦС может проверить его подлинность.
- Таким образом, использование цифрового сертификата предполагает следующую схему электронного взаимодействия партнеров. Один из партнеров посылает другому собственный сертификат, полученный из ЦС, и сообщение, подписанное ЭЦП.
- *Получатель сообщения осуществляет проверку подлинности сертификата партнера, которая включает:*
 - проверку доверия эмитенту сертификата и срока его действия;
 - проверку ЭЦП эмитента под сертификатом;
 - проверку аннулирования сертификата.

Взаимодействие клиентов с ЦС

- В случае если сертификат партнера не утратил свою силу, а ЭЦП используется в отношениях, в которых она имеет юридическое значение, открытый ключ партнера извлекается из сертификата. На основании этого открытого ключа может быть проверена ЭЦП партнера под электронным документом (ЭД).
- Важно отметить, что в соответствии с законом "Об ЭЦП" подтверждением подлинности ЭЦП в ЭД является положительный результат проверки соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа подписи.

Взаимодействие клиентов с ЦС

- *ЦС, обеспечивая безопасность взаимодействия партнеров, выполняет следующие функции:*
- регистрирует ключи ЭЦП;
- создает, по обращению пользователей, закрытые и открытые ключи ЭЦП;
- приостанавливает и возобновляет действие сертификатов ключей подписей, а также аннулирует их;
- ведет реестр сертификатов ключей подписей, обеспечивает актуальность реестра и возможность свободного доступа пользователей к реестру;
- выдает сертификаты ключей подписей на бумажных носителях и в виде электронных документов с информацией об их действительности;
- проводит, по обращениям пользователей, подтверждение подлинности (действительности) подписи в ЭД в отношении зарегистрированных им ЭЦП.

Взаимодействие клиентов с ЦС

- В ЦС создаются условия безопасного хранения секретных ключей на дорогом и хорошо защищенном оборудовании, а также условия администрирования доступа к секретным ключам.
- *Регистрация каждой ЭЦП* осуществляется на основе заявления, содержащего сведения, необходимые для выдачи сертификата, а также сведения, необходимые для идентификации ЭЦП обладателя и передачи ему сообщений.
- Заявление подписывается собственноручной подписью обладателя ЭЦП, содержащиеся в нем сведения подтверждаются предъявлением соответствующих документов. При регистрации проверяется уникальность открытых ключей ЭЦП в реестре и архиве ЦС.

Взаимодействие клиентов с ЦС

- При регистрации в ЦС на бумажных носителях оформляются два экземпляра сертификата ключа подписи, которые заверяются собственноручными подписями обладателя ЭЦП и уполномоченного лица удостоверяющего центра (УЦ) и печатью удостоверяющего центра. Один экземпляр выдается обладателю ЭЦП, второй остается в УЦ.
- В реальных системах каждым партнером может использоваться несколько сертификатов, выданных различными ЦС.
- Различные ЦС могут быть объединены *инфраструктурой открытых ключей* или **PKI** (PKI - Public Key Infrastructure).
- ЦС в рамках PKI обеспечивает не только хранение сертификатов, но и управление ими (выпуск, отзыв, проверку доверия). Наиболее распространенная модель PKI - *иерархическая*.
- Фундаментальное преимущество этой модели состоит в том, что проверка сертификатов требует доверия только относительно малому числу корневых ЦС. В то же время эта модель позволяет иметь различное число ЦС, выдающих сертификаты.