Направление подготовки бакалавров
090301 «Информатика и вычислительная техника»

Электронная цифровая подпись

Караваева Ольга Владимировна

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Электронно-цифровая подпись (ЭЦП)

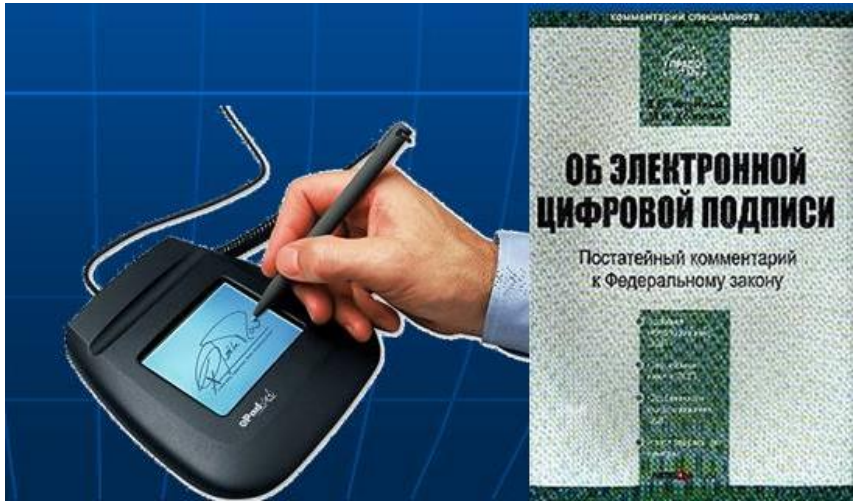
ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП

ЭЦП – это аналог обычной подписи, применяют, чтобы придать юридическую силу документации, находящейся на электронном носителе. которую

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП



Электронной цифровой подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста проверить авторство и подлинность сообщения.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП

Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП

Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП

ФЗ-63"Об электронной подписи"

Устанавливает принципы использования электронной подписи:

1. Пользователи могут использовать ЭП любого вида по своему усмотрению;
2. Пользователи могут использовать любую информационную технологию и (или) технические средства, удовлетворяющие требованиям ФЗ-63;
3. Разрешается автоматическое (не собственноручное) создание и проверка ЭП в ИС;
4. Разрешается подписание одной ЭП совокупности электронных документов;
5. Признается юридическая сила ЭП, созданных в соответствии с нормами иностранного права.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП

К ЭЦП предъявляются два основных требования:

- легкость проверки подлинности подписи
- высокая сложность подделки подписи

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП

Преимущества:

- упрощение и ускорение процесс обмена данными (особенно когда ведется сотрудничество с зарубежными компаниями);
- сокращение расходов, связанных с документооборотом;
- повышение уровня безопасности для информации, носящей коммерческий характер.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП

Определение подлинности информации реализуется путем установки факта, что полученные данные были отправлены подписавшим документ с помощью электронной цифровой подписи, и то что данные не были искажены. Недавно считалось, что электронный документ проще подделать, чем бумажный экземпляр.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП

Подпись под документом используется в качестве доказательства, что человек согласен с содержимым документа. Основные причины доверия к подписи:

- подлинность подписи можно проверить
- подпись, которая стоит под одним документом, не может быть использована под другим
- подпись нельзя подделать
- подписанный документ не может быть изменен
- подпись забрать назад нельзя, и поэтому поставив подпись нельзя потом сказать, что не подписывали или не были уведомлены с содержимым документа

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

Понятие электронной подписи появилось в середине 1970-х годов.

1975 год Уитфилдом Диффи и Мартином Хеллманом было впервые предложено понятие «электронная цифровая подпись» в работе «Новые направления в криптографии»

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

1977 год — Рональд Ривест, Ади Шамир и Леонард Адлеман разработали первый в мире криптографический алгоритм – RSA, который без дополнительных модификаций можно использовать для создания примитивных цифровых подписей.

Вскоре после RSA были разработаны другие ЭЦП, такие как алгоритмы цифровой подписи Рабина, Меркле.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

1981 год Разработан алгоритм DSA, который и сейчас используется как стандарт США для электронной подписи.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

1984 год — Создана криптосистема Схема Эль-Гамаля, которая лежит в основе стандартов ЭП в США и России.

В этом же году Шафи Гольдвассер, Сильвио Микали и Рональд Ривест первыми строго определили требования безопасности к алгоритмам цифровой подписи. Ими были описаны модели атак на алгоритмы ЭЦП, а также предложена схема GMR, отвечающая описанным требованиям.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

1991 год Опубликован стандарт на ЭП DSS (Digital Signature Standard), разработчиком которого явился Национальный институт стандартизации и технологий (NIST) США

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

1993 год — Метод RSA обнародован и принят в качестве стандарта, его рекомендовано применять для шифрования/расшифровки и для генерации/проверки электронной подписи.
В этом же году разработан российский закон об электронной подписи.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

1994 год Принят первый отечественный стандарт в области ЭП – ГОСТ Р34.10-94.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

1997 год Закон «Об электронной цифровой подписи» принят в Германии.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

1999 год Министерство РФ по связи и информатизации инициировало создание проекта федерального закона «Об электронной цифровой подписи». Данный закон создаёт правовые основы формирования надежной инфраструктуры, включая удостоверяющие центры.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

2001 год Законопроект «Об электронной цифровой подписи» одобряет Правительство РФ

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

2002 год Принят новый стандарт на электронную подпись: ГОСТ Р 34.10-2001.
В этом же году принят Федеральный закон «Об электронной цифровой подписи». Он стал основой для использования электронных документов и ЭП.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

2011 год Президент РФ Дмитрий Медведев подписал закон «Об электронной подписи» (ЭП), одобренный Госдумой и Советом Федерации в марте. Документ пришел на смену принятому в 2001 г. закону «Об электронно-цифровой подписи» (ЭЦП), который содержал слишком серьезные требования к ЭП и сильно ограничивал возможности по применению электронных документов.

Федеральный закон № 63-ФЗ «Об электронной подписи» от 06.04.2011 N 63-ФЗ

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

В соответствии с 63-ФЗ «Электронная подпись» - это информация в электронной форме, которая содержит уникальную последовательность символов (ключ) и присоединяется к цифровому документу, чтобы определить личность подписанта.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

Закон о цифровой подписи включает 20 статей, раскрывающих следующие нормы:

- основные термины и определения;
- принципы и правила использования;
- виды, особенности использования;
- процедура выдачи сертификата в удостоверяющем центре;
- обязанности человека, который использует ЭП; деятельность и обязанности Удостоверяющих центров, которые имеют право на выпуск.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Виды ЭП

Федеральный закон № 63-ФЗ от 06.04.2011 г. Определяет новые виды ЭЦП:

- простая – подтверждает, что электронное сообщение отправлено конкретным лицам. Сообщение приравнивается к бумажному документу, если стороны заранее об этом договорились, а также в предусмотренных законом случаях.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Виды ЭП

Федеральный закон № 63-ФЗ от 06.04.2011 г. Определяет новые виды ЭЦП:

- усиленная неквалифицированная позволяет идентифицировать отправителя и подтвердить, что документ никто не изменял. Сообщение приравнивается к бумажному документу, если стороны заранее об этом договорились, а также в предусмотренных законом случаях

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Виды ЭП

Федеральный закон № 63-ФЗ от 06.04.2011 г. Определяет новые виды ЭЦП:

- усиленная квалифицированная (дополнительно к «У не К») подтверждается сертификатом, выданным аккредитованным удостоверяющим центром. Сообщение с УК со всех случаях приравнивается к бумажному документу с собственноручной подписью

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Виды ЭП

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Виды ЭП

Сфера применения	*Простая*	*Неквалифицированная*	*Квалифицированная*
Внутренний документооборот	+	+	+
Внешний документооборот	+	+	+
Арбитражный суд	+	+	+
Сайт Госуслуг	+	-	+
Контролирующие органы	-	-	+
Электронные аукционы	-	-	+

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

2011 год Сенаторы разрешили государственным органам вносить документы в правительство в электронном виде при помощи ЭП.
Правительство России 30 августа 2012 года утвердило изменения в Регламент об электронном документообороте в органах государственной власти. Документация между органами государственной и исполнительной власти, а также аппаратом правительства передается в электронном виде с помощью электронной подписи.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

2013 год Одноименный ГОСТ Р 34.10-2001 заменён на ГОСТ Р 34.10-2012.

В этом же году была упрощена электронная подпись, подписью президента в начале 2013 года постановление №33, описывающее порядок использования «простой электронной подписи» при оказании государственных и муниципальных услуг.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. История

2013 год

Согласно тексту постановления, ключ ЭЦП - это сочетание идентификатора и пароля, причем идентификатор - это страховой номер лицевого счета физического лица либо руководителя юридического лица.

Одновременно граждане, получившие простую подпись, будут избавлены от необходимости использовать при обращениях к Порталу государственных услуг электронный ключ на флеш-накопителе, который необходим при использовании усиленной подписи.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Терминология

С понятием ЭЦП тесно связаны два других:

ключ и *сертификат электронной подписи*.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Терминология

Сертификат является электронным (и/или бумажным) документом:

- выдаётся на ФИО конкретного человека (должностного лица) - содержит персональные данные;
- подписывается ЭП Удостоверяющего центра, который тем самым подтверждает его действительность;
- сертификат в себе содержит открытый ключ Пользователя (поэтому открытый ключ называют сертификатом).

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Терминология

Сертификат подтверждает, что ЭП принадлежит конкретному лицу. Он бывает усиленным и обычным. Усиленный сертификат выдается либо удостоверяющим центром, либо ФСБ.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Терминология

- Ключ – это символы, находящиеся в последовательности. Обычно они используются парой. Первый – это сама подпись, другой подтверждает, что она подлинная. Для подписи каждого вновь создаваемого документа, формируется новый ключ.
- Информация, которую получают в УЦ – это не ЭЦП, это средство, чтобы создать ее.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Терминология

Ключевая пара состоит из двух частей: открытой и закрытой. Оба этих ключа выдаются и создаются удостоверяющими центрами с помощью специальной программы шифрования (например, «Крипто-про»).

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Терминология

Закрытый ключ – или «Ключ электронной подписи» по 63-ФЗ – уникальная последовательность символов, предназначенная для создания ЭП и для расшифровки сообщений. Это частная, приватная информация, которая известна только ее владельцу.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Терминология

Закрытый ключ генерируется на рабочем месте пользователя с помощью средства криптографической защиты информации (СКЗИ) и сохраняется (только у пользователя) на съемный носитель (флешка, токен, смарт-карта) или в реестр Windows. Такой закрытый ключ необходимо хранить в секретном месте со всеми мерами предосторожностей.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Терминология

На основе закрытого ключа создается открытый ключ (стоит сказать, что обратный процесс здесь невозможен, так как подобрать закрытый ключ по открытому ключу нельзя).

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Терминология

Открытый ключ – он же «Ключ проверки электронной подписи» по 63-ФЗ – уникальная последовательность символов, предназначенная для проверки подлинности ЭП. Это открытая, общеизвестная информация доступна любому пользователю системы электронного документооборота (ЭДО).

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Терминология

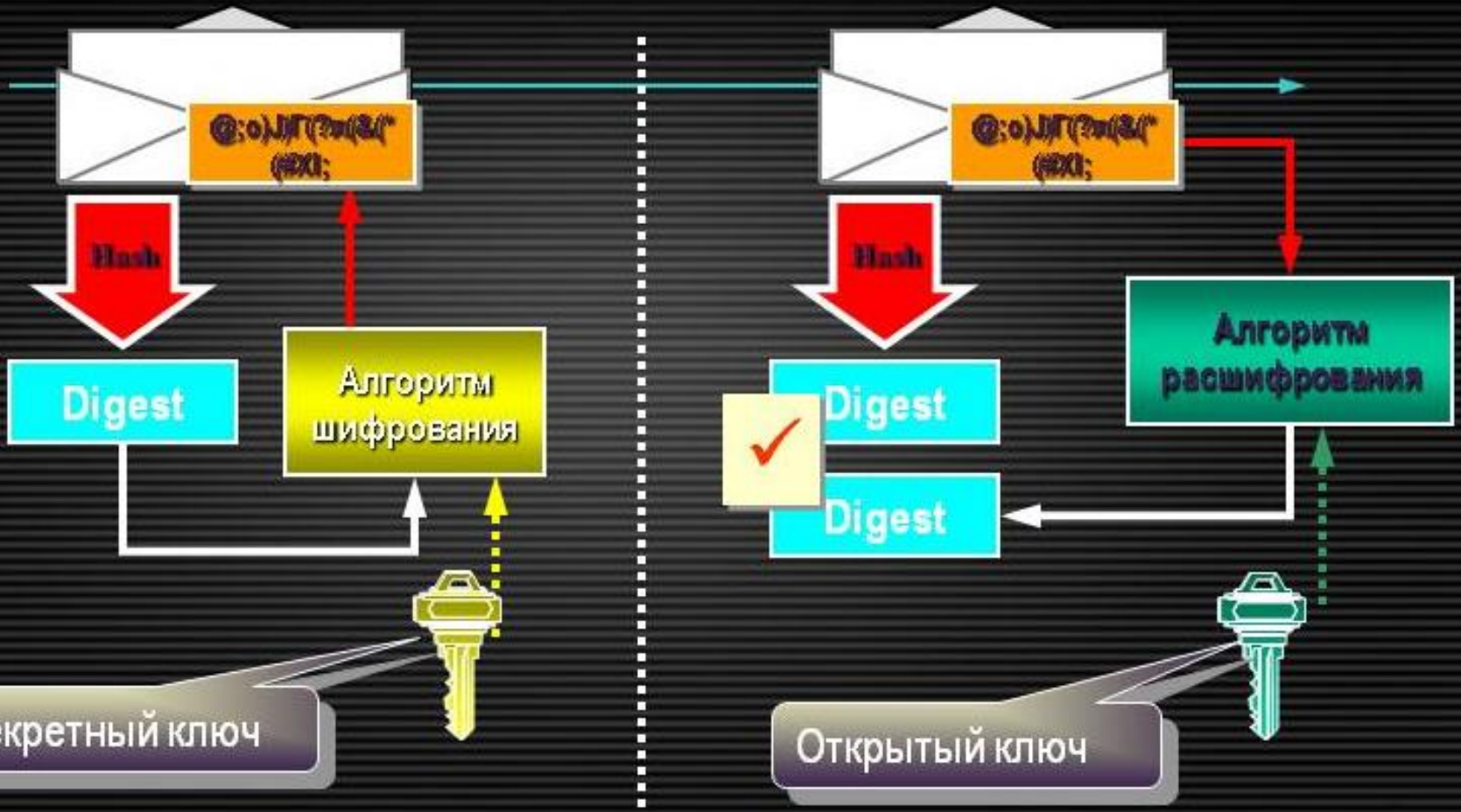
Открытый ключ вычисляется из закрытого ключа и отправляется в Удостоверяющий центр в виде запроса на сертификат.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

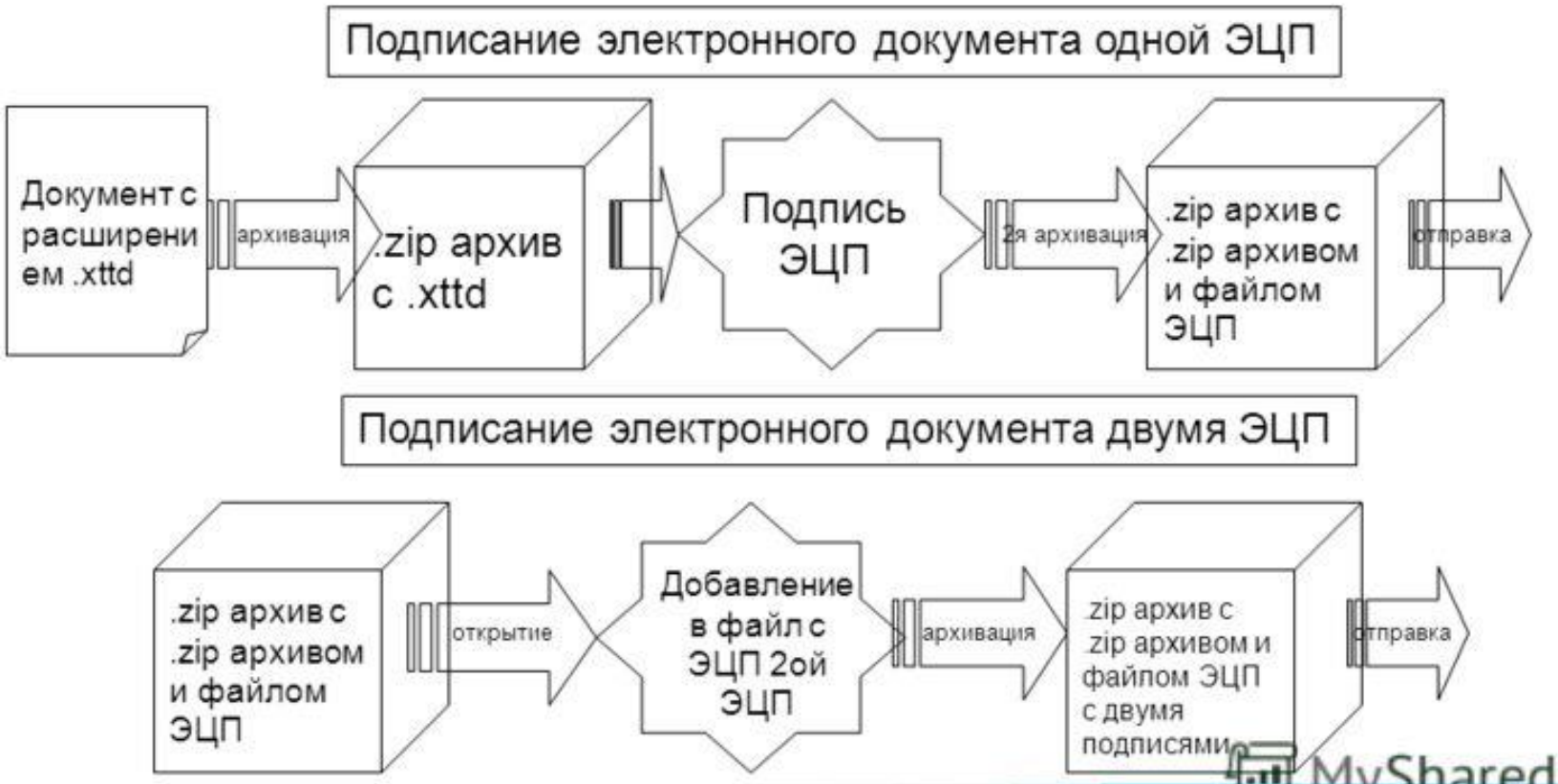
ЭЦП. Терминология

- При генерации пары ключей в алгоритмах ЭЦП, как и в асимметричных системах шифрования, реализованы разные математические схемы, которые основаны на однонаправленных функциях. Эти функции можно разделить на две группы:
- задача факторизации(разложение) больших целых чисел
- задача дискретного логарифмирования

Электронно-цифровая подпись



Электронно - цифровая подпись. Последовательность действий для подписания электронного документа ЭЦП



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Процедура получения ЭП

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Виды ЭП

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Первая и самая встречаемая система ЭЦП на основе RSA.

Сначала нужно вычислить пару ключей.

Отправитель (автор) электронных документов вычисляет два больших простых числа P и Q, затем находит произведение и значение функции:

- $N = P * Q;\ \phi(N) = (P-1)(Q-1)$.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

- Затем отправитель вычисляет число E из условий:

$$E \pounds \phi(N), \text{НОД}(E, \phi(N)) = 1$$

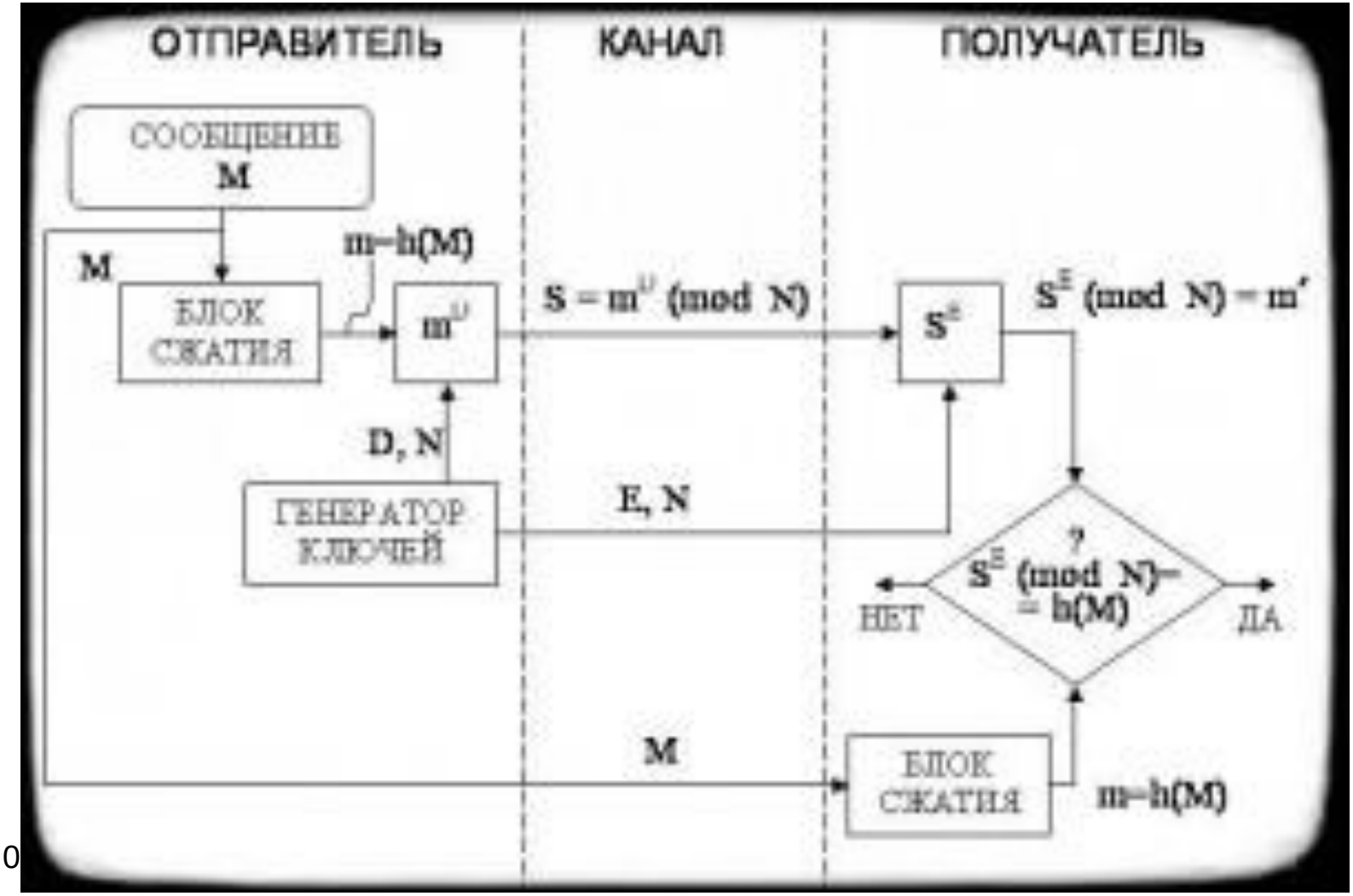
и число D:

$$D < N, E*D \text{ º } 1 (\text{mod } j(N)).$$

- Пара чисел (E, N) является открытым ключом. Такую пару автор передает партнерам по переписке для проверки его цифровых подписей. Число D сохраняется автором как секретный ключ для подписания.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы



ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Недостатки цифровой подписи на основе алгоритма RSA:

- При вычислении модуля N, ключей E, D для цифровой подписи нужно проверять множество дополнительных условий, что на практике трудно. Невыполнение любого из условий делает возможным фальсификации ЭЦП.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Недостатки цифровой подписи на основе алгоритма RSA:

- Для достижения криптостойкости подписи RSA к фальсификации по отношению к алгоритмы DES 10^{18}, нужно использовать целые числа не менее 2^{215}, что требует больших вычислительных затрат, а это на 20.. 30% больше чем другие алгоритмы цифровой подписи при той же криптостойкости.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Алгоритм цифровой подписи Эль Гамаля (EGSA)

- Основная идея обоснована на практической невозможности фальсификации цифровой подписи. Для этого нужна более сложная вычислительная задача, чем разложение на множители большого целого числа. Также Эль Гамалю удалось избежать слабости алгоритма ЭЦП RSA, связанной с подделкой ЭЦП без определения секретного ключа.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Чтобы генерировать пару ключей, нужно выбрать простое целое число P и G, причем G < P. Получатель и отправитель подписанного документа используют одинаковые большие числа

P (~10^{308} = ~2^{1024}) и G (~10^{154} = ~1^{512})

которые не секретные.

Отправитель выбирает случайное целое число X,

1 < X £ (P — 1) и вычисляет: Y = G^X mod P;

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Число Y является открытым ключом, который используется для проверки подписи отправителя. Число X является секретным ключом отправителя для подписи документов.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Чтобы подписать сообщение M, сначала нужно чтобы отправитель захэшировал его с помощью хэш-функции h в целое число m:

$$m = h(M),\ 1 < m < (P - 1)$$

и сгенерировал случайное целое число K

$$1 < K < (P - 1),$$

такое, что K и (P — 1) будут взаимно простыми.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Потом отправитель вычисляет целое число a:

$$a = G^K \bmod P,$$

используя расширенный алгоритм Евклида, вычисляет с помощью секретного ключа X целое число b:

$$m = X * a + K * b \pmod{(P - 1)};$$

Пара чисел (a, b) образуют цифровую подпись S:

$$S = (a, b);$$

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Тройка чисел (M, a, b) транспортируется получателю, в то время как пара чисел (X, K) держится в секрете. Получатель получив сообщение (M, a, b), должен вычислить число m:

$$m = h(M),$$

затем получатель вычисляет:

$$A = Y^a a^b \bmod (P)$$

и признает сообщение M подлинным, если —

$$A = G^m \bmod (P).$$

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Можно строго математически доказать, что последнее равенство будет равно тогда, когда подпись S под документом M получена с помощью именно секретного ключа X, из которого был получен открытый ключ Y.

ВАЖНО! Процедура каждой подписи требует нового значения K и выбирается случайным образом.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Схема Эль Гамаля является типичным примером, который разрешает пересылку сообщений M в открытой форме вместе с аутентификатором (a, b). Такая схема имеет преимущества перед схемой ЭЦП RSA:

Для одинакового уровня стойкости, алгоритм Эль Гамаля использует целые числа короче на 25%, что уменьшает сложность вычислений почти в 2 раза.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

- Выбор модуль P прост, нужно убедится что число простое, и что у числа (P — 1) есть большой простой множитель.
- Схема создания подписи по алгоритму Эль Гамаля не разрешает вычислять ЭЦП под новыми сообщениями без знания секретного ключа.

К недостаткам можно отнести то, что подпись получается в 1,5 раза больше, чем RSA.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Алгоритм цифровой подписи DSA

DSA — Digital Signature Algorithm — это развитие алгоритмов цифровой подписи Эль Гамаля и К.Шнорра.

Получатель и отправитель электронного документа реализуют при вычислении большие целые числа G и P — простые числа L бит каждое (512 £ L £ 1024),

q — простое число длинной 160 бит

(делитель числа (P — 1)).

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Числа P, G, q открытые и могут быть общими для пользователей.

Отправитель берет случайное целое число X

$$1 < X < q.$$

Число X — секретный ключ отправителя для создания ЭЦП.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Отправитель вычисляет:

$$Y = G^X \bmod P.$$

число Y — открытый ключ.

Чтобы подписать документ M, отправитель хэширует его в целое хэш-значение m:

$$m = h(M),\ 1 < m < q,$$

потом генерирует случайное целое число K, $1 < K < q$, и вычисляет:

$$r = (G^K \bmod P) \bmod q.$$

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Также нужно вычислить:

$$s = ((m + r * X)/ K) \bmod q;$$

Пара чисел S = (r, s) образуют цифровую подпись.
Получатель проверяет выполнение условий:

$$0 < r < q,\ 0 < s < q.$$

Если хоть одно условие не выполнено,

то подпись нужно отвергнуть.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Если же выполнены все условия, то получатель вычисляет:

$$w = (l/s) \bmod q,$$

хэш значения

$$m = h(M)$$

и числа

$$u_1 = (m * w) \bmod q,$$

$$u_2 = (r * w) \bmod q.$$

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Затем получатель с помощью открытого ключа Y вычисляет:

$$v = ((G^{u}_{1} * Y^{u}_{2}) \bmod P) \bmod q;$$

Если условие v = r выполняется, тогда подпись S под документом подлинная.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Можно математически доказать, что последнее равенство будет выполнятся тогда, когда подпись S под документом получена с помощью секретного ключа X, из которого был получен открытый ключ Y.

ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ЭЦП. Алгоритмы

Алгоритм DSA имеет преимущества над ЭЦП Эль Гамаля:

- При одинаковом уровне стойкости, длина подписи явно меньше у DSA
- Также меньше время вычисления подписи

- https://zakon.ru/blog/2014/3/11/elektronnaya_cifrovaya_podpis_istoriya_poyavleniya_i_razvitiya