МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА

ЛЕКЦИОННЫЕ МАТЕРИАЛЫ

Методы обеспечения целостности информации

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень	бакалавриат
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление(-я) подготовки	09.03.02 «Информационные системы и технологии»
	(код(-ы) и наименование(-я))
Институт	кибербезопасности и цифровых технологий (ИКБ)
	(полное и краткое наименование)
Кафедра	Разработка программных решений и системное программирование
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))
Лектор	К.т.н. Ермакова Алла Юрьевна
	(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2023/24

(учебный год цифрами)

Проверено и согласовано «____» _____2023_г.

(подпись директора Института/Филиала с расшифровкой)

Москва 2023 г.

Лекция 4. Защита целостности при транспортировке информации (вторая часть)

Классические схемы ЭЦП

Изложим основные идеи, на которых основан механизм цифровой подписи.

Пусть имеется пара преобразований *E* и *D*, преобразование *D* сложно обратить, т. е., зная *D* и *x,* трудно найти *y* такое, что *D(y) = x* [3].

Для того чтобы наладить обмен подписанными электронными сообщениями, необходимо передать получателю сообщений ключ расшифрования, а ключ зашифрования держать в секрете.

Для того чтобы подтвердить подлинность сообщения *x*, отправитель *A* (рис.1) должен отправить вместе с ним значение *E*1(*x*), полученное в результате шифрования сообщения на своем секретном ключе. Это значение и является цифровой подписью *x.* Получатель *B*, получив пару *x, E*1(*x*), применяет преобразование *D*1 и убеждается в том, что *D*1(*E*1(*x*)) = *x.* Если *A* держит преобразование *E*1 в секрете, то никто кроме него не сможет подобрать такое *y,* чтобы *D*1*(y)* совпадало с *x.*

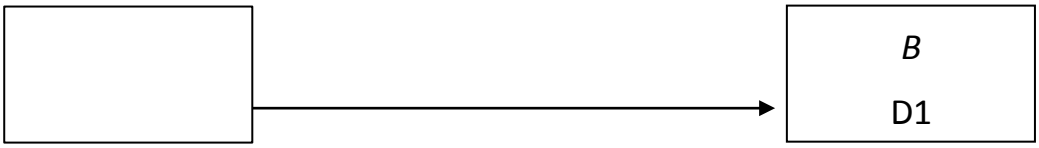

Рис.1. Обмен ключами в режиме цифровой подписи

Таким образом, при создании ЭЦП по классической схеме отправитель:

1) применяет к исходному тексту хэш-функцию;

2) дополняет при необходимости хэш-образ сообщения до длины, требуемой в алгоритме создания подписи;

3) вычисляет цифровую подпись по дополненному хэш-образу сообщения с использованием секретного ключа создания подписи.

Получатель, получив подписанное сообщение, отделяет цифровую подпись от основного текста и выполняет проверку подписи, а именно:

1) применяет к тексту полученного сообщения хэш-функцию;

2) дополняет при необходимости хэш-образ сообщения до длины, требуемой в алгоритме проверки подписи;

3) проверяет соответствие дополненного хэш-образа сообщения полученной цифровой подписи с использованием открытого ключа проверки подписи [4].

Дополнение хэш-образа нужно лишь в том случае, если необходимая длина не обеспечивается алгоритмом хэш-функции. На практике, как правило (например, в стандартах DSS и ГОСТ Р34.10–94), такое дополнение не требуется.

ЭЦП не является полным аналогом обычной подписи. Так, например, возможность постановки подписи авторучкой принадлежит конкретному физическому лицу и не может быть передана или утеряна. Что касается ЭЦП, то секретный ключ, позволяющий подписывать электронные документы, может быть передан другому лицу, а также потерян или украден. Поэтому необходимо разрабатывать специальные процедуры, позволяющие дезавуировать ЭЦП.

Еще одна особенность ЭЦП заключается в том, что она не связана с единственным экземпляром документа. Уничтожив подписанный экземпляр бумажного документа, можно быть уверенным, что второго точно такого больше нет. Что касается уничтожения электронного документа с ЭЦП, то это ни о чем не говорит, т. к. может существовать неограниченное количество ничем не отличающихся копий этого документа.

Если имеется необходимость в обеспечении и целостности, и секретности сообщения, то целесообразно сначала подписать сообщение, а затем уже зашифровать его вместе с подписью. При такой последовательности действий удастся избежать подписывания зашифрованного сообщения. Кроме того, будет скрыта ЭЦП, по которой можно установить автора сообщения. В этом случае необходимо иметь две пары ключей: одну использовать для генерации цифровой подписи, а другую для расшифровки сообщений.

Классические схемы подписи можно разделить по типу применяемых алгоритмов. Наиболее известные – задача разложения составного числа на простые (схема RSA) и задача дискретного логарифмирования (схема Эль-Гамаля, ГОСТ Р34.10–94). К задаче разложения близка (но не эквивалентна) схема цифровой подписи Рабина, со схемой Эль-Гамаля близок протокол Шнорра. При выборе конкретного протокола следует иметь в виду различия в скорости работы, в криптостойкости и удобстве использования.

Специальные схемы подписи

В некоторых ситуациях могут потребоваться дополнительные специальные свойства подписи. В последние годы было разработано множество специальных схем ЭЦП, удовлетворяющих требованиям различных приложений, в том числе:

• схема подписи «вслепую», когда отправитель не знает содержания подписанного им сообщения;

• схема «неоспоримой» (undeniable) подписи, решающая проблему отказа нечестного отправителя от правильной подписи;

• схема «групповой» подписи, в которой получатель может проверить, что подписанное сообщение пришло от некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано;

• схема «разовой» подписи, позволяющая использовать данный секретный (и открытый) ключ для подписи только одного сообщения;

• схема подписи, в которой проверка осуществляется с привлечением третьей стороны (designated confirmer) и др.

Угрозы безопасности при работе с ЭЦП

Нападения на ЭЦП можно классифицировать следующим образом:

• по видам (простейшие – подделка, переделка, повтор и более сложные – подбор сообщения, подаваемого на подпись отправителю, нападение на открытый каталог проверяющего);

• по последствиям (нападение на одно сообщение, на все сообщения данного абонента, на все сообщения всех абонентов в сети);

• по возможностям нарушителя (возможность иметь доступ к каналу связи отправитель–получатель, к компьютеру получателя, к компьютеру отправителя или участвовать в разработке системы подписи);

• по ресурсам, необходимым нарушителю (по временным ресурсам – подписанная информация передается в режиме реального времени и устаревает мгновенно или она хранится долгие годы и практически не устаревает).

Для осуществления своих планов злоумышленник может:

располагать образцами подписанных документов;

• готовить на подпись документы и использовать поставленные под ними настоящие подписи в своих целях;

• получить доступ к компьютеру отправителя, подпись которого он хочет подделать;

• получить доступ к компьютеру проверяющего с тем, чтобы изменить программу проверки подлинности подписи в своих целях;

• оказаться разработчиком программного комплекса (в систему заложены потенциальные слабости).

Большинство нападений имеет смысл только в том случае, когда злоумышленнику известны алгоритмы вычислений и проверки подписи, а также алгоритм вычисления хэш-функции. Как правило, в коммерческих программных продуктах эти алгоритмы не афишируются, говорится лишь о методе цифровой подписи (RSA, Эль-Гамаль и др.).

Меры безопасности при работе с ЭЦП

1. Обеспечение достоверности передаваемых открытых ключей.

Представим себе, что некий злоумышленник *C* подменил открытый ключ абонента *A* во время его передачи абоненту *B* на свой открытый ключ. В этом случае он сможет расшифровывать все сообщения абонента *B*, предназначенные для *A*. Аналогичная атака на цифровую подпись приведет к тому, что сообщения, подписанные злоумышленником, будут считаться подлинными, а настоящие сообщения – ложными.

2. Хранение секретных ключей.

В случае программной реализации секретный ключ подписывающего хранится на его личной дискете, защищенной от копирования, которая может быть утеряна или похищена.

3. Парольная защита.

Паролем могут закрываться не только функции постановки ЭЦП и генерации ключей, но и функции, изменяющие содержимое каталога открытых ключей абонентов сети, и др.

4. Проверка на «криптовирусы».

Наиболее вероятно наличие криптовирусов в нелицензионном программном обеспечении. Для выявления наличия криптовирусов целесообразно использовать антивирусные программы, контролирующие

обращение к определенным областям памяти и обнаружения характерных для криптовирусов команд.

Если пользователь ведет себя грамотно с точки зрения соблюдения норм секретности (хранение секретных ключей подписи, работа с «чистым» программным продуктом, осуществляющим функции подписи) и тем самым исключает возможность похищения ключей или несанкционированного изменения данных и программ, то стойкость системы подписи определяется исключительно криптографическими качествами.