ЛАБОРАТОРНАЯ РАБОТА 5

РЕАЛИЗАЦИЯ ЭЛЕМЕНТОВ ЭЦП RSA

Цель работы: формирование умений подписи электронных документов электронной цифровой подписью с помощью алгоритма RSA.

Теоретические сведения

Электронная подпись (ЭП) – реквизит электронного документа, предназначенный для удостоверения источника данных и защиты данного электронного документа от подделки.

Общая схема

Схема электронной подписи обычно включает в себя:

алгоритм генерации ключевых пар пользователя;

функцию вычисления подписи;

функцию проверки подписи.

Функция вычисления подписи на основе документа и секретного ключа пользователя вычисляет собственно подпись. В зависимости от алгоритма функция вычисления подписи может быть детерминированной или вероятностной. Детерминированные функции всегда вычисляют одинаковую подпись по одинаковым входным данным. Вероятностные функции вносят в подпись элемент случайности, что усиливает криптостойкость алгоритмов ЭП. Однако для вероятностных схем необходим надежный источник случайности (либо аппаратный генератор шума, либо криптографически надежный генератор псевдослучайных бит), что усложняет реализацию.

В настоящее время детерминированные схемы практически не используются.

Функция проверки подписи проверяет, соответствует ли данная подпись данному документу и открытому ключу пользователя. Открытый ключ пользователя доступен всем, так что любой может проверить подпись под данным документом.

Поскольку подписываемые документы переменной (и достаточно большой) длины, в схемах ЭП зачастую подпись ставится не на сам документ, а на его хэш. Для вычисления хэша используются криптографические хэш-функции, что гарантирует выявление изменений документа при проверке подписи. Хэш-функции не являются частью алгоритма ЭП, поэтому в схеме может быть использована любая надежная хэш-функция.

Защищенность

Цифровая подпись обеспечивает:

удостоверение источника документа. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесенные изменения», «метка времени» и т. д.;

защиту документа от изменений. При любом случайном или преднамеренном изменении документа (или подписи) изменится хэш, следовательно, подпись станет недействительной;

невозможность отказа от авторства, так как создать корректную подпись можно лишь, зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом.

Возможны следующие угрозы цифровой подписи:

злоумышленник может попытаться подделать подпись для выбранного им документа;

злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила

При использовании надежной хэш-функции, вычислительно сложно создать поддельный документ с таким же хэшем, как у подлинного. Однако эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов хэширования, подписи или ошибок в их реализациях.

Тем не менее, возможны еще следующие угрозы системам цифровой подписи:

злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа;

злоумышленник может обманом заставить владельца подписать какой-либо документ, например, используя протокол слепой подписи;

злоумышленник может подменить открытый ключ владельца на свой собственный, выдавая себя за него.

Реализацию алгоритма смотрите в лабораторной работе № 2, разница лишь в том, что открытый и секретный ключи меняются местами.

Содержание заданий

Реализуйте программу, которая будет подписывать документ MS Word, посмотрите, как будет изменяться подпись при незначительных и больших изменениях в исходном тексте.

Контрольные вопросы

1. Что такое хэш-функция?
2. Для чего применяется хэш-функция?
3. Особенности применения ЭП?

Отчетность по лабораторной работе

Подготовьте отчет с кодом программы с подробными его комментариями и результатами выполнения программы.

ЛАБОРАТОРНАЯ РАБОТА 6

РЕАЛИЗАЦИЯ ЭЛЕМЕНТОВ ЭЦП ГОСТ Р 34.10–94

Цель работы: формирование умений подписи электронных документов электронной цифровой подписью с помощью алгоритма ГОСТ Р 34.10–94.

Теоретические сведения

Первый российский стандарт цифровой подписи обозначается как ГОСТ Р 34.10–94. Алгоритм цифровой подписи, определяемый этим стандартом, концептуально близок к алгоритму DSA. В нем используются следующие параметры:

p – большое простое число длиной от 509 до 512 бит либо от 1020 до1024 бит;

q – простой сомножитель числа $(p - 1)$, имеющий длину 254–256 бит;

a – любое число, меньшее $(p - 1)$, причем такое, что $a^q \bmod p = 1$;

x – некоторое число, меньшее q;

$y = a^x \bmod p$.

Кроме того, этот алгоритм использует однонаправленную хэш-функцию $H(x)$.

Стандарт ГОСТ Р 34.10–94 определяет хэш-функцию, основанную на использовании стандартного симметричного алгоритма ГОСТ 28147–89.

Первые три параметра – p, q и a – являются открытыми и могут быть общими для всех пользователей сети. Число x является секретным ключом. Число y является открытым ключом.

Чтобы подписать некоторое сообщение m, а затем проверить подпись, выполняются следующие шаги:

1. Пользователь A генерирует случайное число k, причем $k < q$.

2. Пользователь A вычисляет значения:

$r = (a^k \bmod p) \bmod q$,

$s = (xr + k(H(m))) \bmod q$.

Если $H(m) \bmod q = 0$, то значение $H(m) \bmod q$ принимают равным единице.

Если $r = 0$, то выбирают другое значение k и начинают снова. Цифровая подпись представляет собой два числа: r и s.

Пользователь A отправляет эти числа пользователю B.

3. Пользователь B проверяет полученную подпись, вычисляя:

$v = H(m)^{q-2} \bmod q$;

$1z = (sv) \mathbf{mod}\ q$;

$2z = ((q - r)v) \mathbf{mod}\ q$;

$u = ((a^{z1} y^{z2}) \mathbf{mod}\ p) \mathbf{mod}\ q$.

Если $u = r$, то подпись считается верной.

Различие между этим алгоритмом и алгоритмом DSA заключается в том, что в DSA

$s = (k(xr + (H(m)))) \mathbf{mod}\ q$, что приводит к другому уравнению верификации.

Следует также отметить, что в российском стандарте ЭП параметр q имеет длину 256 бит. Современных криптографов вполне устраивает q длиной примерно 160 бит. Различие в значениях параметра q является отражением стремления разработчиков российского стандарта к получению более безопасной подписи. Этот стандарт вступил в действие с начала 1995 г.

Содержание заданий

Реализуйте программу, которая будет подписывать документ MS Word, посмотрите, как будет изменяться подпись при незначительных и больших изменениях в исходном тексте.

Контрольные вопросы

1. Что такое хэш-функция?
2. Для чего применяется хэш-функция?
3. Особенности применения ЭЦП?

Отчетность по лабораторной работе

Подготовить отчет с кодом программы с подробными его комментариями и результатами выполнения программы.