Лабораторная работа № 14, 15
Особенности использования и использование схемы цифровой подписи RSA для защиты целостности информации

Цель работы:

1. Закрепление теоретического материала (раздел – системы защиты информации).
2. Изучение теоретического материала (методическое пособие, конспект).
3. Закрепление теоретического материала, ответы на вопросы преподавателя.

Пояснения к работе:

После установления соединения необходимо обеспечить защиту от фальсификации в процессе обмена сообщениями. Для этого требуется обеспечить выполнение следующих четырех условий:

1. получатель должен быть уверен в истинности источника данных;
2. получатель должен быть уверен в истинности представляемых данных;
3. отправитель должен быть уверен в доставке данных получателю;
4. отправитель должен быть уверен в истинности полученного подтверждения о приеме информации.

Подтверждение истинности источника данных и истинности передаваемых (доставленных) данных осуществляется с помощью цифровой подписи. Подтверждение приема сообщений обеспечивается организацией режима передачи квитанций. Квитанция представляет собой короткое сообщение, содержащее контрольную информацию о принятом сообщении и электронную подпись. В качестве контрольной информации могут использоваться зашифрованные данные о номере полученного сообщения и времени получения, а также цифровая подпись отправителя рабочего сообщения. Получив такую квитанцию, заверенную цифровой подписью, отправитель делает вывод об успешной передаче сообщения.

Цифровая подпись представляет собой контрольную двоичную последовательность. Она получается путем специальных преобразований хэш-функции от данных сообщения и секретного ключа отправителя сообщения. Таким образом цифровая подпись, с одной стороны, несет в себе контрольную характеристику(хэш-функцию) содержимого сообщения, а с другой – однозначно указывает на связь содержимого сообщения и владельца секретного ключа. использование хэш-функции позволяет зафиксировать подмену или модификацию данных сообщения. При удовлетворительных результатах проверки цифровой подписи получатель может быть уверен, что полученное сообщении пришло от субъекта, владеющего секретным ключом, и содержательная часть получается в соответствии с официальным государственным стандартом, то она имеет юридическую силу обычной подписи под документом.

Впервые идею цифровой подписи предложили в 1976 году американские специалисты У.Диффи и М.Хеллман. В настоящее время для получения цифровой подписи используются методы, применяемые в шифровании с несимметричным ключом.

Первым по времени изобретения алгоритмов цифровой подписи был разработанный в 1977 году алгоритма RSA. Предложенный в 1987 году алгоритм Т. Элт-Гамаля позволял повысить стойкость подписи при ключе в 64 байта примерно в 1000 раз, но длина самой цифровой подписи увеличивалась в два раза и оставляла 128 байт.

Алгоритм Эль-Гамаля послужил основой для разработки национального стандарта США DSA, введенного в 1991 году, и государственного стандарта РФ ГОСТ Р 31.10-94, введенного в действие с 1995 года. В алгоритме DSA удалось сократить длину цифровой подписи до 49 байт при сохранении ее стойкости на прежнем уровне. Дальнейшим развитием стандарта DSA стал стандарт США DSS.

Российский стандарт ГОСТ Р 34.10 схож со стандартом DSS, но предполагает более сложный алгоритм вычисления хэш-функции. Стандартом ГОСТ Р 31.10 определен следующий алгоритм вычисления цифровой подписи и аутентификации сообщения. Отправитель и получатель сообщения имеют в своем расположении некоторые открытые атрибуты создания и проверки цифровой подписи: начальный вектор хэширования H и параметры p, g и a. Параметры вычисляются в соответствии с процедурой ГОСТ. Отправитель выбирает свой секретный ключ x и вычисляет открытый ключ $y = a^x (\mathrm{mod}\ p)$. Открытый ключ y отсылается получателю.

Секретный ключ выбирается из интервала $0 < x < 2^{256}$. Число k генерируется в процессе получения подписи сообщения, является секретным и должно быть уничтожено после выработки подписи. Упрощенный алгоритм процедуры выработки подписи включает следующие шаги:

1. Вычисление хэш-функции h(M) от сообщения M.
2. Получение целого числа k, 0<k<g
3. Вычисление значений $r = a^k \pmod p$ и $r' = r \pmod g$. Если r'=0, перейти к шагу 2.
4. Вычисление значения $s = (xr' + kh(M)) \pmod g$. Если s=0, то переход к шагу 2, иначе конец работы алгоритма.

Цифровой подписью сообщения M является вектор $< r' >_{256} \| < s >_{256}$, который состоит из двоичных слов по 256 бит каждое, т.е. длина цифровой подписи составляет 521 бит.

Для проверки подписи (верификации сообщения) получатель сообщения выполняет следующие шаги.

1. Проверка условий: 0<s<g и 0<k<g. Если хотя бы одно условие не выполнено, то подпись считается недействительной.
2. Определяется хэш-функция $h(M_1)$ от полученного сообщения M_1.
3. Вычисление значения $v = (h(M_1))^{g-2} \pmod g$.
4. Вычисляются значения $z_1 = sv \pmod g, z_2 = (g - r')v \pmod g$.
5. Вычисление значения $u = a^{Z1} y^{X2} \pmod p) \pmod g$.
6. Проверка условия: r'=u. Если условие выполнено, то получатель считает, что полученное сообщение подписано отправителем, от которого был получен ключ y. Кроме того, получатель считает, что в процессе передачи целостность сообщения не нарушена. В противном случае подпись считается недействительной и сообщение отвергается.

Имея открытые атрибуты цифровой подписи и тексты открытых сообщений, определить секретный ключ x можно только путем полного перебора. Причем при длине цифровой подписи 40 байт стандарт DSA гарантирует число комбинаций ключа 10^{21}. Для получения ключа перебором потребуется 30 лет непрерывной работы 1000 компьютеров производительностью 1 млрд. операций в секунду.

Использование цифровой подписи для аутентификации коротких сообщений, подтверждающих прием информационных сообщений, существенно увеличивает длину служебного подтверждающего сообщения. Для подписи служебного сообщения может быть использована подпись полученного информационного сообщения, модифицированная по определенному алгоритму. Например, выбраны разряды по маске. Если в сети реализован режим передачи пакетов, то цифровая подпись передается в конце всего сообщения, а не с каждым пакетом. Иначе трафик в сети увеличится. Степень увеличения трафика будет зависеть от длины пакета. При длине информационной части пакета в 2048 бит использование цифровой подписи каждого пакета привело бы к возрастанию примерно на 25 %.

При организации электронной почты необходимо учитывать особенности подтверждения полученных сообщений. получатель в момент передачи сообщения может быть не активным. Поэтому следует организовать отложенную проверку подлинности сообщения и передачу подтверждения.

Контрольные вопросы:

1. Дайте понятие «цифровой подписи».
2. Порядок использования цифровой подписи в условиях установления соединения
3. Что собой представляют атрибуты цифровой подписи?