ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 681.3

УПРАВЛЕНИЕ КЛЮЧАМИ В КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ

И.А. Фомина

Нижегородский госуниверсистет им. Н.И. Лобачевского

fomis54@mail.ru

Поступила в редакцию 23.03.2010

Рассматриваются некоторые вопросы, связанные с управлением ключами шифрования. Описаны требования, предъявляемые к протоколам распределения ключей. Предлагается подход к распределению ключей в группах участников с постоянным составом на основе эллиптических кривых. Приводятся доказательства свойств данного протокола.

Ключевые слова: криптография, криптосистемы, шифрование, секретность, аутентичность, протоколы распределения ключей, эллиптические кривые.

Обеспечение информационной безопасности является одним из приоритетных направлений развития информационных технологий. Круг задач, решаемых в этой области, постоянно расширяется как в количественном, так и в качественном отношении. Одним из основных средств, используемых для защиты информации в компьютерных системах, являются криптографические преобразования. Проблематика криптографии включает решение многочисленных задач, не связанных непосредственно с обеспечением секретности. Современная криптография включает в себя четыре крупных раздела: симметричные криптосистемы, криптосистемы с открытым ключом, системы электронной подписи, управление ключами.

Современные криптосистемы – криптосистемы, построенные на основе использования ключей. И, как правило, управление ключами – это наиболее слабое место в криптографических приложениях. Использовать криптографические технологии просто, однако безопасно хранить, использовать ключи и обмениваться ключами гораздо сложнее. Очень часто плохое управление ключами портит даже исключительно хорошие системы, так как безопасность алгоритма сосредоточена в ключе. Управление ключами включает процедуры генерации, накопления и распределения ключей.

В общем случае все методы генерации ключей можно разделить на аппаратные и программные. Основным требованием при этом является равномерность распределения по всему пространству возможных ключей. При генерации ключей аппаратным способом используются генераторы шума – электронные устройства, в которых протекает случайный физический процесс; при программной реализации – генераторы псевдослучайных последовательностей. Существуют определенные критерии при выборе генератора псевдослучайных чисел [1].

Организация накопления ключей связана с процедурами их хранения, учета и удаления. В достаточно сложной информационной системе один пользователь может работать с большим объемом ключевой информации, вследствие чего иногда возникает необходимость организации мини-баз данных по ключевой информации. Такие базы данных отвечают за принятие, хранение, учет и удаление используемых ключей. Информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие ключевую информацию, называются мастер-ключами и, как правило, не хранятся в компьютерной системе, или для их преобразования используются криптографические алгоритмы. Количество используемых ключей зависит от числа абонентов, объема передаваемой информации и особенностей алгоритма шифрования. Сеансовые ключи должны уничтожаться.

Вопрос обновления ключей непосредственно связан с третьей проблемой управления ключами – распределением ключей. Распределение ключей – одна из фундаментальных задач криптографии. Чтобы понять масштабность проблемы, отметим, что при обслуживании n пользователей, обменивающихся закрытой информа-

цией друг с другом, необходимо $n(n\text{-}1)/2$ разных секретных ключей. С ростом n возникает проблема управления огромным числом ключей. Существует несколько путей решения этой проблемы. Определение наиболее подходящего из них выбирается в зависимости от сложившейся ситуации [2]:

• Физическое распределение. С помощью доверенных курьеров или вооруженной охраны ключи могут рассылаться традиционным физическим путем. Эта процедура используется как в симметричных, так и в асимметричных криптосистемах. Предполагается, что создатель ключей будет передавать асимметричный секретный ключ пользователю (и/или асимметричный открытый ключ) физически безопасным способом.

• Выдача общего ключа участникам взаимодействия центром выдачи ключей – схема «абонентского шифрования». В такой системе центр изготовления и рассылки ключей выступает как гарант подлинности и аутентичности передаваемых сообщений, так как он не только снабжает пользователей ключами, но и несет ответственность за их секретность при изготовлении и доставке. Если центр скомпрометирован, то обеспечение безопасности последующих запросов на выдачу ключей проблематично, а безопасность ранее выданных ключей зависит от криптосистемы.

• Предоставление центром сертификации ключей доступа к открытым ключам пользователей и выдача секретных ключей пользователя. Может использоваться как симметричными, так и асимметричными криптосистемами. Так как при данном способе каждый пользователь должен каким-то образом безопасно взаимодействовать с центром выдачи ключей в самом начале работы, то это просто еще один случай, когда начальный обмен ключами является проблемой. Если долговременные секретные ключи распределены между пользователями и неким центром, который обычно называют центром распределения ключей, то используют специальные криптографические протоколы. Этот способ распределения предусматривает, что пользователи и центр работают в режиме «онлайн».

• Сеть доверия. Используется в асимметричных криптосистемах. Пользователи сами распространяют свои ключи и следят за ключами других пользователей; доверие заключатся в неформальном способе обмена ключами. Одно из решений заключается в том, что за каждым пользователем закрепляется единственный ключ, используя который он может связываться с центром доверия. В этом случае система с n пользователями требует только n ключей. Когда двое пользователей хотят обменяться секретными сведениями, они генерируют ключ, который будет использован только для передачи этого сообщения. Его называют сеансовым ключом. Сеансовый ключ генерируется с участием центра доверия при помощи одного из протоколов.

• Протоколы обмена ключами. Выработка секретного ключа и обмен им производится по незащищенным каналам связи между участниками взаимодействия, которые до этого не имели общего секретного ключа. Используя криптосистемы с открытым ключом, партнеры, не доверяющие посредникам и лишенные возможности встретиться, могут договориться об общем секретном ключе в режиме «онлайн» в соответствии с протоколом об обмене ключей. Это наиболее распространенное приложение техники шифрования с открытым ключом. Сначала стороны предварительно согласовывают секретный ключ. Затем для шифрования фактической информации применяется симметричный шифр с согласованным ключом.

Недостаток методов, использующих центр распределения ключей, заключается в том, что в центре известно, кому и какие ключи назначены, что позволяет читать все сообщения, циркулирующие в информационной системе. При прямом обмене ключами возникает проблема аутентификации подлинности субъектов. Она решается двумя способами:

1. Механизм «запрос – ответ». Если пользователь А желает быть уверенным, что сообщения, полученные от В, не являются ложными, он включает в посылаемое для В сообщение непредсказуемый элемент (запрос). При ответе пользователь В должен выполнить некоторую операцию над этим элементом (например, прибавить число). Причем это невозможно осуществить заранее, так как неизвестно, какое случайное число придет в запросе. После получения ответа с результатами действий пользователь А может быть уверен, что сеанс является подлинным. Недостатком этого метода является возможность установления – пусть сложной – закономерности между запросом и ответом.

2. Механизм отметки времени («временной штемпель»). Он подразумевает фиксацию времени для каждого сообщения. В этом случае каждый пользователь ИС может знать, насколько «старым» является пришедшее сообщение. При использовании отметок времени встает проблема допустимого временного интервала задержки для подтверждения подлинности сеанса, так как сообщение с «временным штемпе-

лем» не может быть передано мгновенно. Кроме того, компьютерные часы получателя и отправителя должны быть абсолютно синхронизированы.

Большинство известных протоколов распределения ключей служат для выработки общего сеансового ключа для двух участников. Для обмена ключами, как правило, используются алгоритм RSA или более эффективный алгоритм Диффи – Хелмана, позволяющий двум пользователям без посредников обмениваться ключом, который может быть использован затем для симметричного шифрования [3].

В настоящее время более актуальной задачей является распределение ключей для группы участников. Такая задача возникает при организации безопасной связи внутри групп абонентов, при аутентификации участников группы, при формировании групповой цифровой подписи, при организации конференц-связи и т.д.

Криптографические протоколы, в которых происходят выработка и распространение ключей, называются протоколами распределения ключей. Проблема распределения ключей для групп участников может быть решена несколькими способами. Общий ключ может не вырабатываться в протоколе, а приобретаться заранее кем-то из участников (например, с помощью простой почты, курьерской службы или при помощи центра выдачи ключей) и отправляться затем всем остальным участникам. Такие протоколы носят название протоколов распространения ключей. Очевидно, уровень защиты в таком случае оказывается невысоким. Для обеспечения более высокого уровня безопасности могут быть использованы протоколы обмена ключами, в которых каждый участник группы делает свой вклад при генерации ключа. В обоих случаях только действующие участники группы имеют доступ к общей секретной величине (ключу).

До недавнего времени основным математическим аппаратом, используемым при реализации протоколов обмена ключами, были циклические группы простого порядка p. Проблема, лежащая в основе этих протоколов, – проблема дискретного логарифмирования (вычисление показателя x по известным $g^x mod\ p$ и образующему элементу g). Однако перед современной криптографией стоит проблема повышения стойкости алгоритмов и уменьшения размеров блоков данных и ключей. Самый очевидный путь решения этой проблемы – представление блоков информации в криптографических алгоритмах не только в виде чисел (или элементов конечных полей), но и в виде иных алгебраических объектов большей сложности. Одним из весьма подходящих типов таких объектов оказались точки эллиптических кривых.

Особый интерес к эллиптической криптографии обусловлен теми преимуществами, которые дает ее применение: высокое быстродействие и небольшая длина ключа. По оценкам специалистов, криптосистемы на основе эллиптических кривых обеспечивают самую высокую надежность на 1 бит ключа из всех известных систем с открытым ключом. Это достигается благодаря сложности базового алгоритма – вычисления дискретных логарифмов в группе точек эллиптической кривой (вычисление множителя k по известным kG и образующей точке G). Меньшая длина ключей приводит к ускорению вычислений, снижению потребляемой мощности, меньшей загрузке памяти и периферийных устройств. Таким образом, эллиптические кривые оказываются очень привлекательными для построения криптографических алгоритмов большой стойкости.

В зависимости от предъявляемого уровня стойкости протоколы обмена ключами должны обладать рядом криптографических свойств [4].

1. Протокол обладает свойством *контрибутивности*, если сформированный ключ зависит от секретных данных, внесенных каждым из участников протокола.
2. Протокол обладает свойством *совершенной опережающей секретности*, если компрометация долговременных ключей (то есть долговременной секретной информации) не компрометирует сеансовых ключей (получаемых в результате выполнения протокола).
3. Протокол обеспечивает *неявную аутентификацию ключа*, если каждый участник протокола уверен, что никакая другая сторона не могла получить доступ к сеансовому ключу (за исключением злоумышленника внутри группы).
4. Протокол обладает свойством *аутентичности,* если он обеспечивает неявную аутентификацию ключа.

Для описания протоколов будут использоваться следующие основные обозначения:

n – число участников группы;

M_i – i-й участник группы;

E – эллиптическая кривая порядка q над полем порядка p (p, q – простые);

G – образующая точка эллиптической кривой;

k_i – долговременный секретный ключ (секретное число) i-го участника;

k_iG – долговременный открытый ключ i-го участника;

r_i – кратковременный секретный ключ (секретное число) i-го участника;

r_iG – кратковременный открытый ключ i-го участника;

K_{ij} – общий долговременный секрет пары участников i и j;

S_n – групповой (сеансовый) ключ, вырабатываемый участниками в протоколе;

$\rightarrow$ – обозначает передачу информации (сообщения) от одного участника другому;

Z^*_p – циклическая группа порядка p конечного поля.

Следует отметить, что вырабатываемый общий секрет (ключ) в протоколах обмена ключами на основе эллиптических кривых представляет собой некоторую точку кривой. В качестве же самого ключа можно использовать, например, x-координату полученной точки.

Протокол обмена ключами для групп участников на основе эллиптических кривых

Пусть $M=\{M_1,M_2,...,M_n\}$ – множество пользователей, которым необходимо выработать общий ключ S_n. Протокол выполняется в три этапа. На первом этапе (n-1 шагов) идет сбор информации от отдельных участников группы, на втором этапе всем рассылается материал для вычисления общего ключа. И, наконец, на третьем этапе каждый участник вычисляет групповой ключ.

Пусть $K_{in}=Q_x$ – общий долговременный секрет участников M_i и M_n, где $Q=k_ik_nG$, а Q_x – x-координата этой точки.

Схематически протокол можно представить следующим образом:

Этап 1

шаг i (i=1,...,n-1)

Участник M_i выбирает случайное $r_i \in Z^*_p$.

$$M_i \rightarrow M_{i+1}: \left\{ \frac{r_1...r_i}{r_j} G, j \in [1,i] \right\} \bigcup \{r_1...r_iG\}$$

Этап 2

Участник M_n выбирает случайное $r_n \in Z^*_p$.

$$M_n \rightarrow M_i: \left\{ \frac{r_1...r_n}{r_i} K_{in} G, i \in [1,n-1] \right\}$$

Групповой ключ M_n вычисляет как $S_n= r_1r_2...r_nG$

Этап 3

Участник M_i находит: $k_ik_nG \rightarrow Q_x \rightarrow Q_x^{-1}=K_{in}^{-1}$.

Участник M_i вычисляет групповой ключ:

$$S_n = r_i\left(\frac{r_1...r_n}{r_i} K_{in}G \right) K_{in}^{-1} = r_1r_2...r_nG.$$

Пример работы протокола для случая четырех участников.

Этап 1

$M_1 \rightarrow M_2$: r_1G

$M_2 \rightarrow M_3$: r_1G, r_2G, r_1r_2G

$M_3 \rightarrow M_4$: r_1r_2G, r_1r_3G, r_2r_3G, $r_1r_2r_3G$

Этап 2

$M_4 \rightarrow M_1$: $r_2r_3r_4G$

$M_4 \rightarrow M_2$: $r_1r_3r_4G$

$M_4 \rightarrow M_3$: $r_1r_2r_4G$; $S_4= r_1r_2r_3r_4G$

Этап 3

M_1, M_2, M_3: $S_4= r_1r_2r_3r_4G$

Отметим, что последнего участника M_n принято называть *контролирующим группы*, так как через него проводятся ключевые операции протокола. Он отвечает за использование аутентичных ключей K_{in}, от которых и зависит аутентификация. Следовательно, участник M_n должен быть лицом, которому все доверяют. Например, это может быть схема с доверенным сервером в качестве M_n.

Утверждение 1. Протокол обмена ключами для групп участников на основе эллиптических кривых обладает свойствами *контрибутивности и аутентичности.*

Доказательство

Пусть:

r_1, r_2,...,r_n – секретные кратковременные ключи участников протокола;

$S_2= r_1r_2...r_nG$ – сеансовый ключ, вырабатываемый в протоколе;

k_i – секретный долговременный ключ участника M_i;

Q_x – x-координата точки $Q=k_ik_nG$;

Z – злоумышленник, который способен изменять, задерживать, добавлять сообщения;

c_n– кратковременный ключ злоумышленника Z.

Доказательство утверждения носит конструктивный характер.

1. Контрибутивность протокола следует непосредственно из его построения, так как сформированный в результате протокола ключ S_n зависит от секретных данных $r_1,r_2.,...,\ r_n$.

2. Допустим, злоумышленник перехватил все сообщения первого и второго этапов протокола и собирается получить общий ключ с участником M_i. Сообщение, которое он может перенаправить M_i, в общем виде выглядит как c_nG. Участник M_i вычислит сеансовый ключ как $K_{in}^{-1}r_ic_nG$. Таким образом, чтобы получить общий с M_i ключ, злоумышленник должен знать K_{in}. Эту величину он может получить двумя способами: либо из перехваченного на втором этапе сообщения

$\left\{\frac{r_1...r_n}{r_i}K_{in}G\right\}$, либо при вычислении точки $Q=k_ik_nG$. Однако оба способа приводят его к необходимости решения задачи дискретного логарифмирования в группе точек эллиптической кривой. Аналогично показывается, что злоумышленник не может получить общий ключ с остальными участниками. Таким образом, протокол обладает свойством аутентичности.

Утверждение 2. Протокол обмена ключами для групп участников на основе эллиптических кривых обладает свойством *совершенной опережающей секретности*.

Доказательство утверждения носит конструктивный характер.

Допустим, злоумышленник скомпрометировал долговременные ключи K_{in}. Тогда он, перехватив сообщения второго этапа, может вычислить множество $\left\{\frac{r_1...r_n}{r_i}G, i\in[1,n-1]\right\}$. Однако чтобы получить сеансовый ключ $r_1r_2...r_nG$, ему необходимо знать хотя бы один из кратковременных секретных ключей r_i, что упирается в проблему дискретного логарифмирования в группе точек эллиптической кривой.

Ещё одно важное свойство протоколов – это *подтверждение ключа*. Не для каждого протокола это свойство является необходимым: например, оно не нужно, если взаимодействие с полученным ключом происходит немедленно. Однако свойство подтверждения ключа является желательным для протоколов обмена по следующим причинам:

1. Протоколы обмена становятся более сильными и автономными.

2. Исключается возможность вычисления неправильного ключа без обнаружения этого (в случае перерыва между выработкой общего ключа и непосредственно передачей данных).

Полное подтверждение ключа достигается путем получения каждым участником группового ключа и доказательства всем, что он знает этот ключ. Для рассмотренного выше протокола *подтверждение ключа* можно определить как *подтверждение ключа для контролирующего группы* (*участника* M_n). Это может быть легко достигнуто путем добавления величины $F(S_n(M_n))$ в последнее сообщение протокола (рассылка всем участникам группы), где $S_n(M_n)$ обозначает ключ, вычисленный участником M_n, а F – некоторую хэш-функцию (то есть для которой по аргументу легко получить значение, но по значению трудно найти аргумент). Например, M_n может разослать всем S_xG, где S_x – x-координата точки-ключа S_n, полученного контролирующим группы M_n. Далее участник группы M_i вычисляет $S_n(M_i)$ и проверяет равенство: $S_x(M_i)G= S_xG$.

Следует отметить, что подтверждение ключа и неявная аутентификация ключа образуют полезный в некоторых случаях дополнительный эффект протокола – *аутентификацию участника* M_n для всех участников группы. Это еще раз доказывает необходимость выделения M_n как «особого» участника группы.

Что же касается свойства целостности ключа, то в вышеприведенном протоколе оно не достигается. Активный противник может провести какое-либо умножение числа на точку на любом из этапов протокола. Тем самым злоумышленник, не имея возможности получить общий ключ с кем-либо из участников протокола, может легко нарушить целостность ключа. Для обеспечения целостности можно воспользоваться дополнительными средствами обеспечения целостности данных во время передачи по сети [5].

Список литературы

1. Кнут Д.Э. Искусство программирования. Т. 2. Получисленные алгоритмы. М.: Издательский дом «Вильямс», 2004. 832 с.

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Изд-во «Триумф», 2003. 816 с.

3. Смарт Н. Криптография. М.: Изд-во «Техносфера», 2006. 528 с.

4. Ивонин М.В. URL: http://itsecure.org.ua/id.35803_1.html (дата обращения 15.06.2008).

5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных сетях. М.: Радио и связь, 2001. 376 с.

KEY MANAGEMENT IN CRYPTOGRAPHIC SYSTEMS

I.A. Fomina

Some problems of encryption key management are considered. Requirements for key management protocols are described. An approach to constant-round group key management based on elliptic curves is proposed. Proofs of the protocol characteristics are presented.

Keywords: cryptography, cryptosystems, encryption, security, authenticity, key management protocols, elliptic curves.