УДК 004.056.55

А. А. Кузнецов

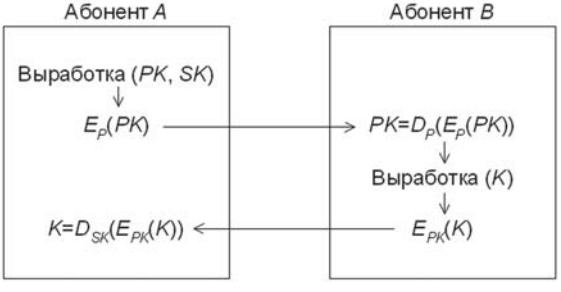
ОРГАНИЗАЦИЯ ЗАЩИЩЕННОГО КАНАЛА СВЯЗИ С ПОМОЩЬЮ КОРОТКИХ СИММЕТРИЧНЫХ КЛЮЧЕЙ

Рассмотрен способ совместного использования симметричных и открытых ключей, позволяющий выполнять аутентификацию абонентов при организации защищенного канала связи, используя короткий исходный симметричный ключ.

Организация защищенных каналов связи обычно сопряжена с необходимостью использования сертификатов открытых ключей или качественных симметричных ключей [1]. В первом случае пользователю требуется получить сертификат, что для среднестатистического человека может оказаться задачей нетривиальной [2, 3], а использование открытых ключей без сертификатов создает опасность возникновения атаки “человек посередине”. Во втором же случае пользователю необходимо запоминать и по другому защищенному каналу связи передавать собеседнику длинный и качественный симметричный ключ или пароль.

Существует, однако, способ организации защищенных каналов связи без использования сертификатов с применением простых и коротких симметричных ключей. Рассмотрим его подробнее.

Предположим, что необходимо установить защищенный канал связи между абонентами A и B, у которых имеется общий, неизвестный никому более пароль P (например, длиной два-три символа) из множества паролей мощностью N. Рассмотрим последовательность действий для выработки качественного общего симметричного ключа (рисунок).



Протокол установления связи:

PK — псевдооткрытый ключ; *SK* — секретный ключ; *P* — пароль; *K* — симметричный ключ

Абонент A.

1. Вырабатывает пару ключей, состоящую из открытого (для удобства назовем его "псевдооткрытым" ключом) и секретного;

2. Преобразует псевдооткрытый ключ таким образом, чтобы он не содержал избыточные данные (т.е., чтобы не существовало критерия, по которому было бы возможно определить допустимость ключа);

3. Зашифровывает псевдооткрытый ключ с помощью пароля P;

4. Отправляет абоненту B.

Абонент B.

5. Расшифровывает псевдооткрытый ключ с помощью пароля P;

6. Преобразует псевдооткрытый ключ к исходной форме;

7. Вырабатывает случайный симметричный ключ;

8. Зашифровывает его с помощью полученного псевдооткрытого ключа;

9. Отправляет зашифрованный симметричный ключ абоненту A.

Абонент A.

10. Расшифровывает симметричный ключ с помощью своего секретного ключа.

Ключ был назван псевдооткрытым, поскольку, с одной стороны, он является открытым по определению метода асимметричного шифрования, с другой стороны, он неизвестен никому, кроме абонентов A и B. Зашифрованное сообщение, содержащее псевдооткрытый ключ, не должно включать в себя какие-либо избыточные данные, такие как контрольная сумма передаваемого ключа, или другие зависимые данные, позволяющие злоумышленнику достаточно легко определять допустимость или недопустимость проверяемого ключа.

Следует отметить, что псевдооткрытый ключ должен применяться однократно; т.е. для каждого нового абонента необходимо заново вырабатывать пару секретного и псевдоотрытого ключей. Предположим, что пользователь A использует одинаковые псевдооткрытые ключи для всех абонентов. Если среди абонентов окажется злоумышленник, то он, зная псевдооткрытый ключ, сможет легко подобрать исходные короткие симметричные ключи, использующиеся для других абонентов.

После того, как установлен длинный общий симметричный ключ, при шифровании сообщений следует использовать модификатор ключа [4].

Рассмотрим возможные действия злоумышленника в этой ситуации.

1. *Подмена псевдооткрытого ключа, не зная пароля P.* Если злоумышленник зашифрует собственный открытый ключ с помощью пароля, отличного от P, абонент B после расшифрования получит неверный псевдооткрытый ключ, а следовательно, подготовленный им

симметричный ключ не сможет правильно расшифровать ни абонент A, ни злоумышленник. Таким образом, злоумышленник может нарушить процесс установки защищенного канала связи, однако, он не в состоянии получить какую-либо секретную информацию. Успешную подмену злоумышленник может осуществить лишь с вероятностью $p = 1/N$.

2. *Попытка определить пароль P.* С помощью пароля P зашифрован псевдооткрытый ключ, не содержащий никакой избыточной информации. Таким образом, расшифровывание с помощью *любого* пароля даст некоторый псевдооткрытый ключ, без возможности проверки его правильности.

3. *Осуществление дешифрования симметричного ключа, переданного абонентом B.* Отметим, что злоумышленнику также неизвестен и псевдооткрытый ключ. Следовательно, он вынужден производить дешифрование для каждого возможного варианта псевдооткрытого ключа. Таким образом, сложность такой атаки возрастает в N раз по сравнению с простым дешифрованием информации, зашифрованной открытым ключом.

Таким образом, в этом протоколе *качество* исходного симметричного ключа (пароля) определяет *вероятность* успешной атаки "человек посередине". Например, используется пароль из алфавита, включающего, скажем, 64 символа — большие и маленькие английские буквы, цифры. Вероятность осуществления атаки "человек посередине" при использовании пароля, состоящего из двух символов этого алфавита, $p = 2{\cdot}10^{-4}$, из трех символов — $p = 4{\cdot}10^{-6}$.

Кроме того, при наличии ограничений на размеры используемых ключей (симметричный ключ — до 40 бит, открытый ключ — не более 128 бит) такой протокол позволяет значительно увеличить стойкость системы. По сложности дешифрования ключу размером 128 бит для алгоритма эль-Гамаля, например, соответствует симметричный ключ размером порядка 60 бит [5, 6]. В этом случае при использовании исходного симметричного ключа размером 40 бит будет получена эффективная длина ключа порядка 100 бит.

Приведем пример формирования псевдооткрытого ключа для алгоритма эль-Гамаля. В классической схеме эль-Гамаля открытый и секретный ключи связаны между собой соотношением [1]:

$$y = g^x \bmod m, \tag{1}$$

где x — секретный ключ; $(y,\ g,\ m)$ — открытый ключ; m — простое число, общее для группы пользователей [1] и встроенное в криптосистему.

В случае, если с помощью исходного короткого ключа шифруется вся тройка (y, g, m), злоумышленник может опробовать короткие ключи, например, проверяя простоту числа m. Чтобы этого избежать, передаче подлежит только пара чисел (y, g).

Положим, что число m состоит из s двоичных разрядов. Выработаем случайный вектор g', состоящий из s разрядов. Определим g как

$$g = g' \bmod m.$$

Затем по уравнению (1) вычисляем y. А y' определяем как

$$y' = y + mr,$$

где r — случайное число, выбранное таким образом, что $r \geqslant 0 \wedge y' < 2^s$.

Далее производим шифрование $E_P(y', g')$.

Абонент B, получив и расшифровав y' и g', вычисляет y и g:

$$y = y' \bmod m \quad \text{и} \quad g = g' \bmod m.$$

Таким образом, рассмотренный способ позволяет установить защищенный канал связи и обеспечить аутентификацию абонентов при использовании достаточно простого и короткого симметричного ключа или пароля.

СПИСОК ЛИТЕРАТУРЫ

1. Шнайер Б. Прикладная криптография. – М.: Триумф, 2002. – 816 с.
2. Фергюсон Н., Шнайер Б. Практическая криптография. – М.: Издательский дом “Вильямс”, 2005. – 424 с.
3. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. – СПб.: Питер, 2003. – 368 с.
4. Масленников М. Е. Практическая криптография. – СПб.: БХВ-Петербург, 2003. – 464 с.
5. Петров А. А. Компьютерная безопасность: Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.
6. Столингс В. Криптография и защита сетей: Принципы и практика. – М.: Издательский дом “Вильямс”, 2001. – 672 с.

Статья поступила в редакцию 17.01.2006

Александр Александрович Кузнецов родился в 1983 г., окончил МГТУ им. Н.Э. Баумана в 2004 г. Аспирант кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор 28 научных работ в области защиты информации.

A.A. Kuznetsov (b. 1983) graduated from the Bauman Moscow State Technical University in 2004. Post-graduate of “Information Security” department of the Bauman Moscow State Technical University. Author of 28 publications in the field of data protection.