УДК 681.3

А. В. Муравьев, А. Н. Березин, Д. Н. Молдовян

ПРОТОКОЛ СТОЙКОГО ШИФРОВАНИЯ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ КОРОТКИХ КЛЮЧЕЙ

Предложены способ и протокол гарантированной защиты информации, передаваемой по открытым каналам, путем ее криптографического преобразования при использовании разделяемых секретных ключей малого размера (до 56 бит).

Ключевые слова: *шифрование, криптографические протоколы, секретный ключ, стойкость, задача дискретного логарифмирования, коммутативный шифр.*

Введение. Применяемые в системах защиты информации криптографические схемы с секретным ключом (одноключевые) обеспечивают гарантированную стойкость шифрования сообщений при использовании ключей достаточно большого размера, например 128 или 256 бит. На практике же существует необходимость срочной передачи конфиденциальной информации, когда и отправитель, и получатель имеют ключи лишь малого размера (от 32 до 56 бит). Использование таких ключей непосредственно в алгоритмах симметричного шифрования позволяет потенциальному нарушителю определить эти ключи методом полного перебора по ключевому пространству. В этом случае возникает необходимость обеспечения приемлемого уровня стойкости шифрования, например, равного 2^{128} операциям.

Для решения данной задачи следует включить в процесс шифрования алгоритм коммутативного шифрования, не требующий использования разделяемых (общих) секретных ключей [1, 2] (так называемое бесключевое шифрование, которое позволяет обеспечить необходимый уровень стойкости). Недостатком данного алгоритма является невозможность обеспечить аутентификацию сообщений. В предлагаемых протоколах для аутентификации сообщений используется разделяемый секретный ключ малого размера, благодаря чему потенциальный нарушитель не может выдать себя за отправителя или получателя сообщений, также он не имеет вычислительной возможности определить секретный ключ методом полного перебора.

Протокол передачи сообщения без обмена ключами. В качестве процедуры коммутативного шифрования возможно использование трехпроходного протокола Шамира [3], что позволяет передать секретное сообщение по открытому каналу связи без использования процедуры распределения ключей. В основе протоколов данного типа лежит стойкий алгоритм коммутативного шифрования, для которого выполняется условие

$$E_A\left(E_B\left(M\right)\right)=E_B\left(E_A\left(M\right)\right),$$

где E — функция криптографического преобразования, A и B — неразделяемые секретные ключи отправителя и получателя соответственно, M — преобразуемое сообщение.

При использовании данного протокола пересылка сообщения M по открытому каналу связи осуществляется следующим образом.

1. Отправитель шифрует сообщение M по своему ключу A и посылает его получателю: $C_1=E_A(M)$.

2. Получатель шифрует криптограмму C_1 по своему ключу B и посылает отправителю: $C_2=E_B(C_1)=E_B(E_A(M))$.

3. Отправитель, используя процедуру расшифровывания D по своему ключу A, преобразует криптограмму C_2 и посылает получателю: $C_3=D_A(C_2)=D_A(E_B(E_A(M)))=D_A(E_A(E_B(M)))=$ $=E_B(M)$. Исходя из полученного шифр-текста C_3, получатель, используя процедуру рас-

шифровывания D по своему ключу B, восстанавливает сообщение M по формуле $M = D_B(E_B(M))$.

Ключи A и B могут выбираться произвольно, и для каждого передаваемого сообщения возможна выработка новых пар ключей. Очевидно, что обмен ключами не происходит, поэтому данный протокол может называться протоколом бесключевого шифрования. Однако протоколы данного типа уязвимы для атаки „человек посередине“, т.е. потенциальный нарушитель может выдавать себя как легальный участник протокола.

Новый способ применения бесключевого шифрования. Шифрование сообщений по разделяемому ключу малого размера не является безопасным, так как при перехвате криптограммы практически возможно нахождение ключа путем перебора по ключевому пространству. Для обеспечения требуемого уровня стойкости представляется уместным передача сообщения с использованием протокола бесключевого шифрования и аутентификация сообщений, выполняемая по разделяемому ключу малого размера. Причем такой вариант применения разделяемого секретного ключа принципиально отличается от его применения в процедурах шифрования сообщений, так как у потенциального нарушителя будет лишь одна попытка угадать секретный ключ и навязать ложное сообщение, тогда как при шифровании у него имеется возможность многократного опробования различных значений ключа. Вероятность обмана в случае применения секретного ключа для аутентификации составляет 2^{-k}, где k — длина ключа (в битах). Например, при использовании 32-битового ключа вероятность составит 2^{-32}, что пренебрежимо мало даже для достаточно критичных применений. Благодаря этому представляется возможным использовать ключи малого размера для аутентификации сообщений в протоколах бесключевого шифрования. При практической реализации необходимо обеспечить неразрывность процедуры аутентификации и бесключевого шифрования.

Аутентификация шифр-текстов. Значения шифр-текстов C_1, C_2, C_3, получаемых в результате выполнения протокола коммутативного шифрования, являются вычислительно неотличимыми от случайных значений. Шифрование криптограмм по разделяемому короткому ключу с использованием симметричного алгоритма $G_K(C)$, где G_K — алгоритм симметричного шифрования [4] по ключу K, не позволяет потенциальному нарушителю найти значение разделяемого короткого ключа, а для легального получателя появляется возможность аутентификации отправителя шифр-текстов. При использовании такого подхода протокол стойкого шифрования по ключу малого размера выглядит следующим образом.

1. Отправитель шифрует сообщение M по своему неразделяемому ключу A: $C_1 = E_A(M)$; полученную криптограмму C_1 зашифровывает по разделяемому секретному ключу K с использованием алгоритма симметричного шифрования [4]: $S_1 = G_K(C_1)$; полученное значение S_1 отправляет получателю.

2. Получатель расшифровывает шифр-текст S_1 по разделяемому ключу K и получает значение C_1: $C_1 = G^{-1}{}_K(S_1)$; шифрует криптограмму C_1 по своему неразделяемому ключу B: $C_2 = E_B(C_1)$; полученную криптограмму C_2 зашифровывает по разделяемому секретному ключу K с использованием алгоритма симметричного шифрования [4]: $S_2 = G_K(C_2)$; полученное значение S_2 посылает отправителю.

3. Отправитель расшифровывает шифр-текст S_2 по разделяемому ключу K и получает значение C_2: $C_2 = G^{-1}{}_K(S_2)$; затем, используя процедуру расшифровывания D по своему неразделяемому ключу A, преобразует криптограмму C_2 и посылает получателю: $C_3 = D_A(C_2) = E_B(M)$.

Получатель расшифровывает сообщение M из шифр-текста C_3: $M = D_B(E_B(M))$. Использование на первых двух шагах протокола дополнительного симметричного шифрования по общему разделяемому ключу позволяет предотвратить атаки со стороны активного нарушителя, т.е. происходит взаимная аутентификация пересылаемого сообщения получателем и отправителем.

В качестве функции криптографического преобразования $E_K(M)$, обеспечивающей свойство коммутативности, может использоваться алгоритм шифрования Полига — Хеллмана [2], основанный на вычислительной трудности задачи дискретного логарифмирования по модулю простого числа. Базовой операцией в данном протоколе является операция возведения в степень по модулю большого простого числа p. Шифрование сообщения $M < p$ выполняется путем возведения его в некоторую степень e, взаимно простую с числом $p-1$: $C = E(M) = M^e \bmod p$. Криптограмма C расшифровывается посредством возведения ее в степень d: $M = D(C) = C^d \bmod p$. Выбор степени d осуществляется при выполнении условия $M = C^d = M^{ed} \bmod p$ для любого $M < p$, для чего степени e и d выбираются такими, чтобы выполнялось условие $ed = 1 \bmod p - 1$. Пара (e,d) составляет локальный ключ отправителя сообщения. Для обеспечения 128-битовой стойкости необходимо использовать в качестве модуля простое число p размером не менее 2 464 бита, причем разложение на множители числа $p-1$ должно содержать, по крайней мере, один большой простой множитель q размером не менее 256 бит.

Уменьшение вычислительной сложности протокола стойкого шифрования по короткому разделяемому ключу K может быть достигнуто при использовании случайного простого числа p в качестве модуля алгоритма коммутативного шифрования и путем шифрования p по ключу K перед его отправкой по открытому каналу (например, отправитель секретного сообщения генерирует случайное простое число p и направляет его получателю в виде криптограммы $\sigma = G_K(p)$). При использовании этого механизма активный нарушитель, выдающий себя за отправителя или получателя сообщения, имеет только одну попытку угадывания секретного ключа K. Если нарушитель выдает себя за отправителя, то это будет обнаружено получателем, так как при расшифровывании им криптограммы σ будет получено число, отличное от p. Если нарушитель выдает себя за получателя, то это будет обнаружено отправителем, так как при расшифровывании криптограммы σ нарушителем будет получено число, отличное от p. Поскольку вмешательство активного нарушителя ведет к получению различных значений модуля, то пропадает свойство коммутативности, и пересылаемое отправителем сообщение не совпадает с сообщением, доставленным получателю в ходе протокола бесключевого шифрования. Последний факт может быть обнаружен с помощью хэш-функции, присоединяемой к сообщению.

При использовании механизма шифрования модуля числа p протокол стойкого шифрования по короткому ключу содержит следующие шаги.

1. Отправитель сообщения M генерирует случайное простое число p (достаточно большого размера), шифрует p по разделяемому ключу K и получает его преобразованное значение $\sigma = G_K(p)$; вычисляет значение h хэш-функции от M; затем, используя алгоритм Полига — Хеллмана, шифрует M по неразделяемому ключу A, получает шифр-текст $C_1 = M^A \bmod p$ и направляет получателю секретного сообщения значения C_1, h и σ по открытому каналу.

2. Получатель расшифровывает шифр-текст σ по разделяемому ключу K, получает значение простого числа p, зашифровывает значение C_1 по неразделяемому ключу B по формуле $C_2 = C_1^B \bmod p$ и направляет отправителю шифр-текст C_2 по открытому каналу.

3. Отправитель расшифровывает шифр-текст C_2 и посылает значение C_3 получателю: $C_3 = C_2^{A^{-1}} \bmod p$.

4. Получатель восстанавливает сообщение M из полученного шифр-текста C_3 по формуле $M = C_3^{B^{-1}} \bmod p$; затем вычисляет значение хэш-функции от M и сравнивает его с h: если сравниваемые значения равны, то получатель делает вывод о подлинности полученного секретного сообщения.

Результаты аутентификации. В обоих вариантах реализации протокола обеспечена неразрывность процедур аутентификации и коммутативного шифрования. Это позволяет избежать активных атак, в которых нарушитель пытается играть роль легального участника протокола. Значения, получаемые в ходе выполнения протокола, вычислительно неотличимы от случайных значений, их шифрование по разделяемому секретному ключу исключает возможность определения короткого ключа методом перебора всех возможных комбинаций разделяемого секретного ключа по ключевому пространству. В этом случае у атакующего отсутствует вычислительно эффективный критерий отбраковки неверных значений ключа. Возможны и другие варианты построения протоколов шифрования с использованием разделяемых ключей малого размера. Представляют интерес конечные поля векторов [5], конечные группы точек эллиптической кривой [6], конечные поля двоичных многочленов, степени которых являются простыми числами Мерсенна [7], также возможна реализация протокола с использованием двух трудных задач [8].

Заключение. Показана принципиальная возможность построения протоколов шифрования по разделяемому секретному ключу малого размера. В основе предложенного способа лежит идея использования бесключевого шифрования совместно с процедурами аутентификации шифр-текстов. В качестве механизма аутентификации используется алгоритм симметричного шифрования по короткому разделяемому ключу некоторых значений, получаемых или используемых в алгоритме коммутативного шифрования. Предложен конкретный вариант реализации протокола на основе алгоритма коммутативного шифрования Полига — Хеллмана. Для обеспечения стойкости протокола, равной 2^{80}, 2^{128} и 2^{160} операциям модульного умножения, следует использовать простое число p, имеющее разрядность 1 024, 2 464 и 4 320 бит соответственно.

Статья подготовлена по результатам работы, выполненной при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта № 14-07-00061-а.

СПИСОК ЛИТЕРАТУРЫ

1. *Schneier B.* Applied Cryptography: Protocols, Algorithms and Source Code. N. Y.: John Wiley & Sons, 1996. 758 p.

2. Pat. 4424414, US. Exponentiation Cryptographic Apparatus and Method / *M. E. Hellman, S. C. Pohlig*. 1984.

3. *Молдовян Н. А.* Введение в криптосистемы с открытым ключом. СПб: БХВ — Петербург, 2007. 286 с.

4. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: Изд-во стандартов, 1989. 20 с.

5. *Молдовяну П. А., Молдовян Д. Н., Морозова Е. В., Пилькевич С. В.* Повышение производительности процедур коммутативного шифрования // Вопросы защиты информации. 2009. № 4. С. 24—31.

6. *Молдовян Н. А., Рыжков А. В.* Способ коммутативного шифрования на основе вероятностного кодирования // Вопросы защиты информации. 2013. № 3. С. 3—10.

7. *Демьянчук А. А., Молдовян Н. А., Рыжков А. В.* Выбор „идеальных“ параметров в схеме двухшаговой аутентификации и коммутативном шифре // Изв. СПбГЭТУ „ЛЭТИ“. 2013. № 8. С. 15—18.

8. *Berezin A. N., Moldovyan N. A., Shcherbakov V. A.* Cryptoschemes based on difficulty of simultaneous solving two different difficult problems // Computer Science Journal of Moldova. 2013. Vol. 21, N 2(62). P. 280—290.

Сведения об авторах

Антон Владимирович Муравьев — аспирант; СПИИРАН, научно-исследовательский отдел проблем информационной безопасности; E-mail: muravev.anton@gmail.com

Андрей Николаевич Березин — аспирант; Санкт-Петербургский государственный электротехнический университет „ЛЭТИ“ им. В. И. Ульянова, кафедра автоматизированных систем обработки информации и управления; E-mail: a.n.berezin.ru@gmail.com

Дмитрий Николаевич Молдовян — СПИИРАН, научно-исследовательский отдел проблем информационной безопасности; научный сотрудник; E-mail: mdn.spectr@mail.ru

Рекомендована СПИИРАН

Поступила в редакцию
10.06.14 г.

УДК 004.056

Е. В. Дойникова, И. В. Котенко

АНАЛИЗ ТЕКУЩЕЙ СИТУАЦИИ И ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ ПО БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ СИСТЕМЫ ПОКАЗАТЕЛЕЙ ЗАЩИЩЕННОСТИ

Рассматривается подход к отслеживанию текущей ситуации по защищенности компьютерной сети и поддержке принятия решений по реагированию на инциденты, нарушающие информационную безопасность. Подход основан на использовании предлагаемой системы показателей защищенности и разработанных алгоритмов их расчета.

Ключевые слова: *оценивание защищенности, показатели защищенности, графы атак, графы зависимостей сервисов, события информационной безопасности.*

Введение. Сложность архитектуры современных компьютерных сетей и проводимых против них атак, а также многообразие событий, нарушающих информационную безопасность, обусловливает необходимость автоматизированной поддержки принятия решений по реагированию на инциденты (information security incident). Основой для принятия решений по реагированию могут служить показатели защищенности, корректно отражающие текущую ситуацию по безопасности компьютерной сети.

В настоящей статье предлагается система показателей защищенности, приводится ряд известных и модифицированных алгоритмов расчета отдельных и интегральных показателей и рассматривается общий подход к анализу ситуации и принятию решений по безопасности на основе предложенной системы показателей.

Релевантные работы. На данный момент существует большое количество исследований в области применения показателей защищенности для анализа безопасности компьютерных сетей. Однако в большинстве работ анализируются отдельные показатели и не учитываются разные типы информации по безопасности. Так, в работах [1, 2] рассматриваются показатели, рассчитываемые на основе информации о составе и характеристиках объектов ком-