УДК 004.056

С.Н. Новиков, О.И. Солонская

Исследование возможности обеспечения конфиденциальности в мультисервисных сетях связи

Представлены результаты исследования многократного «вложения» криптографических алгоритмов шифрования. Показано, что данный подход существенно сокращает время шифрования при сохранении требуемого уровня конфиденциальности информации.

Ключевые слова: конфиденциальность, метод «вложения», составные ключи.

Постановка задачи

Известно, что время шифрования, в том числе, зависит от длины ключа L_k [1] и в общем случае имеет следующий вид:

$$t_{\text{ш}} = AL_k^n + B\,, \tag{1}$$

где $t_{\text{ш}}$ – время, отводимое на шифрование; A, B и n – постоянные, значения которых определяются криптографическими алгоритмами.

Высокоскоростные приложения и службы электросвязи, функционирующие в реальном масштабе времени в мультисервисных сетях связи (МСС), чувствительны ко времени задержки $t_{\text{з}}$. Следовательно, должно выполняться неравенство:

$$t_{\text{з. кр}} \le t_{\text{з}} + t_{\text{ш}}\,,$$

где $t_{\text{з. кр}}$ – время задержки критическое, отводимое на шифрование и передачу информации. Условно примем $t_{\text{з}} = 0$.

Таким образом, существует критичная, конечная длина ключа $L_{k\,\text{кр}}$, превышение которой приведет к недопустимому увеличению времени задержки $t_{\text{з. кр}}$ (рис. 1) и как следствие снижение качества обслуживания (*QoS*) пользователей МСС.

По мнению авторов, решение данной проблемы (уменьшение $t_{\text{ш}}$ при сохранении требуемого уровня конфиденциальности передаваемой информации) возможно за счет использования многократного шифрования – «вложения» криптографических алгоритмов [1].

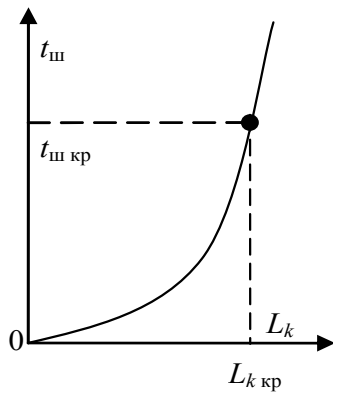

Рис. 1. Зависимость времени, затрачиваемого на шифрование, от длины ключа

Теоретические аспекты многократного шифрования

Пусть l – количество «вложенных» алгоритмов шифрования, т.е. выполняются следующие преобразования, соответственно, зашифрования и расшифрования:

$$y = E_{k_l}\left\{...E_{k_i}[...E_{k_1}(x)]\right\},\ x = D_{k_1}\left\{...D_{k_i}[...D_{k_l}(y)]\right\}. \tag{2}$$

Общая длина составного ключа определяется выражением

$$L_{k_{\text{общ}}} = \sum_{i=1}^{l} L_{k_i};\ L_{k_i} = \text{const}.$$

Время задержки при этом сокращается (рис. 2).

График зависимости $t_{\text{ш}} = f(L_{k\,\text{сост}})$ представлен сложной кривой, состоящей из участков графиков зависимостей $t_{\text{ш}} = f(L_{k\,1})$, …, $t_{\text{ш}} = f(L_{k\,i})$, …, $t_{\text{ш}} = f(L_{k\,l})$. Для определения общего времени задержки $t_{\text{ш. сост}}$ для процедур, описываемых (2), заменим искомую составную функцию на линейную ($f_0(L_{k\,\text{сост}})$), так как соответствующие первые производные равны.

Учитывая (1) и характер $f_0(L_{k\,\text{сост}})$, получим следующее отношение функций для шифрования «длинным» и составным ключами (для простоты $B = 0$):

$$\frac{t_{\text{з}}}{t_{\text{зсост}}} = \frac{AL_{k\text{сост}}^n + B}{l\left(A\left(\frac{L_{k\text{сост}}}{l}\right)^n + B\right)} = \frac{AL_{k\text{сост}}^n + B}{lA\left(\frac{L_{k\text{сост}}}{l}\right)^n + lB} = \frac{AL_{k\text{сост}}^n}{lA\left(\frac{L_{k\text{сост}}}{l}\right)^n} = l^{n-1},$$

где $t_{\text{ш}}$ – время, отводимое на процедуру шифрования одним алгоритмом; $t_{\text{ш. сост}}$ – время, отводимое на процедуру шифрования алгоритмом, состоящим из нескольких однотипных алгоритмов; l – количество алгоритмов в составном; n – степенной показатель функции, описывающий алгоритм.

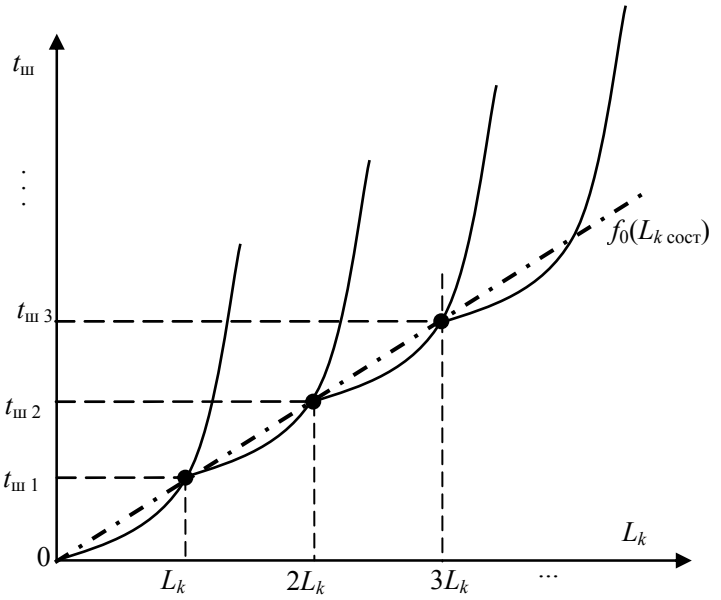

Рис. 2. Зависимости времени, затрачиваемого на шифрование, от длины составного ключа

Таким образом, чем больше первая производная сложной функции $f = AL^n_{k\text{сост}} + B$, тем меньше время шифрования при последовательном использовании l алгоритмов с ключом $\frac{L_{k\text{сост}}}{l}$, в сравнении с применением одного алгоритма с $L_{k\text{сост}}$.

Результаты натурного эксперимента «вложения» криптографических алгоритмов шифрования

Предложенный подход применения составных ключей можно использовать только в том случае, если функция $f(L_k)$ имеет нелинейный характер.

Все криптографические алгоритмы делятся на две большие группы: симметричные и асимметричные. Преимуществом асимметричных по сравнению с первыми является отсутствие необходимости распределения секретных ключей по закрытым каналам связи, однако длины используемых ключей у них значительно больше. Ниже приведена таблица, сопоставляющая длину ключа симметричного алгоритма с длиной ключа асимметричного алгоритма с аналогичной криптостойкостью [1].

Сопоставление длин ключей различных криптографических алгоритмов

Симметричные алгоритмы	Асимметричные алгоритмы
56	384
64	512
80	768
112	1792
256	2304

В свою очередь асимметричные алгоритмы условно можно разделить на следующие группы:

1) алгоритмы, базирующиеся на проблеме факторизации больших чисел (*RSA*, *DSA*);

2) алгоритмы, базирующиеся на задаче о дискретном логарифме (система Диффи–Хеллмана, схема Эль-Гамаля, схема Шнорра);

3) алгоритмы на эллиптических кривых над конечными полями (*ECDSA*, *ECDH*, ГОСТ Р 34.10-2001).

Применим предложенный подход многократного «вложения» шифрования к системе *RSA*, так как время вычисления односторонних функций одинаково велико у всех алгоритмов и имеет нелинейную зависимость.

На рис. 3 представлены результаты натурного эксперимента шифрования алгоритмом *RSA* блока данных объемом 1 Кбайт при:

1) изменении длины ключа от 256 до 2048 бит (кривая *1*);

2) использовании составного 256-битного ключа (кривая *2*).

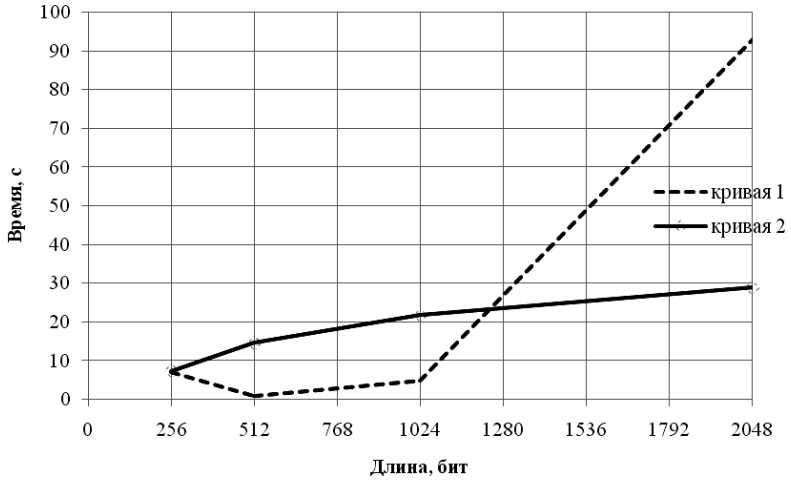

Рис. 3. Сравнение временных зависимостей при обычном шифровании и при шифровании с составным ключом

Выводы

Показано, что многократное «вложение» криптографических асимметричных алгоритмов шифрования существенно сокращает время шифрования при сохранении требуемого уровня конфиденциальности информации.

Литература

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.

2. Wiener Michael J. DES is not a group / Michael J. Wiener, Keith W. Campbell // Lecture Notes In Computer Science. – 1992. – Vol. 740. – P. 512–520.

Новиков Сергей Николаевич
Канд. техн. наук, профессор, зав. каф. «Безопасность и управление в телекоммуникациях» Сибирского государственного университета телекоммуникаций и информатики (СибГУТИ)
Тел.: (383) 269-82-45
Эл. почта: snovikov@mbit.ru

Солонская Оксана Игоревна
Канд. техн. наук, доцент каф. «Безопасность и управление в телекоммуникациях» СибГУТИ
Тел.: (383) 269-82-45, +7-913-938-36-85
Эл. почта: solonskaya@gmail.com

Novikov S.N., Solonskaya O.I.
Research of confidentiality ensuring in multiservice network

In paper produced results of multiple embedding public-key algorithms research. Experiments shows that such algorithms considerably decrease encryption time and confidentiality remain at the same level which is request by the users.
Keywords: confidentiality, embedding method, complex keys