УДК 681.322

Е.Н. Асташкина, И.В. Лысенко

Национальный аэрокосмический университет имени Н.Е. Жуковского «ХАИ», Харьков

ПОДХОД К ФОРМИРОВАНИЮ РАСПИСАНИЯ КЛЮЧЕЙ ДЛЯ БЛОЧНОГО СИММЕТРИЧНОГО КРИПТОАЛГОРИТМА ГОСТ 28147-89

Предлагается подход к формированию расписания ключей криптоалгоритма ГОСТ 28147-89 в целях повышения его криптостойкости. В рамках данного подхода рассматриваются две модели формирования расписания ключей.

Ключевые слова: *конфиденциальность, блочный криптоалгоритм, расписание ключа.*

Введение

Суть блочного криптопреобразования заключается в возможности выбора произвольного отображения $E_K (E_K \in E)$, позволяющего каждому, кому известен ключ *K*, выполнять прямые и обратные преобразования соответственно над исходными и зашифрованными блоками данных. Однако без знания ключа *K* практически невозможно установить, какое отображение использовалось, если даже имеется несколько значений исходных и преобразованных величин. При этом множество E должно быть достаточно большим, чтобы нельзя было выполнить процедуру полного перебора всех возможных отображений E_K [1]. Идеальным считается вариант, когда каждому ключу K соответствует свое уникальное отображение E_K.

Стоит заметить, что весьма редко встречаются алгоритмы шифрования, которые используют ключ шифрования (или его фрагменты) в «чистом» виде (таким алгоритмом является, например, стандарт шифрования ГОСТ 28147-89). Подавляющее большинство алгоритмов шифрования выполняет существенную модификацию исходного ключа для его последующего использования в процессе криптопреобразований. Такая модификация называется расширением ключа или расписанием ключей (key extension, keys schedule) [2].

На практике обычно формируется некоторое базовое отображение E', называемое раундовым, или цикловым, которое выполняется заданное число раз так, что в каждом раунде используется разные раундовые ключи $K^{(i)}$ (подключи), формируемые на основе базового ключа K. Объединение раундовых ключей называют расширенным ключом. Расширенный ключ можно представить в следующем виде [1]:

$$Q^{(e)} = Q^{(e,1)} \| Q^{(e,2)} \| \ldots \| Q^{(e,r)},$$

где e – режим преобразования данных (e = 0 – прямое и e = 1 – обратное преобразование данных) и

$$\forall j = 1,2,\ldots,r \; Q^{(e,j)} = K^{(j+e(r-2j+1))},$$

т.е. ключ $Q^{(e)}$ является функцией от двух переменных, а именно:

$$Q^{(e)} = H(K, e),$$

где K – основной ключ.

Цель статьи – разработка моделей формирования расписания ключей для блочного симметричного криптоалгоритма ГОСТ 28147-89.

1. Анализ процедур расписания ключей блочных симметричных криптоалгоритмов

С учѐтом сказанного выше алгоритм шифрования можно логически разделить на два субалгоритма: собственно шифрующие преобразования и процедура расширения ключа (рис. 1).

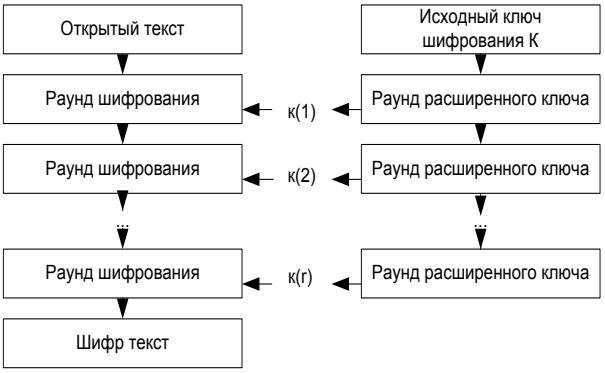

Рис. 1. Назначение процедуры расширения ключа

К процедуре расширения ключа предъявляется немало требований, целью которых является повышение криптостойкости и других характеристик алгоритма. Например, весьма желательно, чтобы процедура расширения ключа могла вычислять ключи «на лету» (on-the-fly), т.е. параллельно с шифрующими преобразованиями: это позволит как распараллеливать вычисления в многопроцессорных системах, так и не тратить память для хранения всего расширенного ключа при шифровании в условиях ограниченных ресурсов.

Существует специальная классификация [1] блочных шифров по типу используемой процедуры генерации расширенного ключа (табл. 1), в соответствии с которой каждому алгоритму может быть присвоен двузначный индекс. При этом первый символ имеет всего два значения (1 или 2), а второй — три (A, B, C). К *первой* группе относятся блочные шифры, для которых знание раундового ключа позволяет определить все или некоторые биты основного ключа или остальных раундовых ключей. К этой группе относятся все шифры, в которых используется так называемое *расписание ключей,* когда каждый раундовый ключ является подмножеством битов основного ключа.

Ко *второй* группе относятся блочные шифры, для которых главным критерием является зависимость битов раундовых ключей от всех или не всех битов основного ключа. К этой группе относится большинство современных блочных шифров, участвовавших в конкурсе AES.

Таблица 1

Классификация процедур генерации расширенного ключа

Индекс	Характеристика	Примеры
1A	Знание раундового ключа позволяет однозначно восстановить основной ключ и остальные раундовые ключи	SPECTR-128,NDC
1B	Знание раундового ключа позволяет восстановить некоторые биты основного ключа и/или остальных раундовых ключей	DES, ГОСТ, SPECTR-H64
1C	Знание раундового ключа позволяет восстановить некоторые биты основного ключа и/или остальных раундовых ключей после выполнения некоторых сравнительно простых арифметических операций	Rijndael, Crypton, DEAL, IDEA
2A	Не все биты основного ключа используются для формирования раундового ключа, и знание раундового ключа не позволяет восстановить основной или расширенный ключ	DFC, CAST-128
2B	Все биты основного ключа используются для формирования каждого раундового ключа, но знание раундового ключа не позволяет восстановить основной или расширенный ключ	Blowfish, LOK1-97, Serpent, CAST-256, Twofish, RC6,E2, Mars, Frog, HPC
2C	Каждый раундовый ключ формируется независимо от остальных раундовых ключей, и размерность расширенного ключа совпадает с размерностью основного ключа	DES с независимыми ключами

2. Процедуры расширения ключа в криптоалгоритме ГОСТ 28147-89

Расписание ключей, как правило, подразумевает, что каждый раундовый ключ является обычным подмножеством основного ключа. Классическим примером использования расписания ключей являются DES и ГОСТ 28147-89.

Отечественный алгоритм шифрования ГОСТ 28147-89 определен в стандарте [3]. Алгоритм шифрует данные 64-битными блоками с использованием 256-битного ключа шифрования. Выполняется 32 раунда преобразований, в каждом из которых предусмотрены следующие операции (рис. 2.).

1. Один из 32-битных субблоков данных складывается с 32-битным значением ключа раунда Ki по модулю 2^{32}.

2. Результат предыдущей операции разбивается на 8 фрагментов по 4 бита, которые параллельно «прогоняются» через 8 таблиц замен S1…S8. Таблицы замен в стандарте не определены. 4-битные фрагменты (после замен) объединяются обратно в 32-битный субблок, значение которого циклически сдвигается влево на 11 бит.

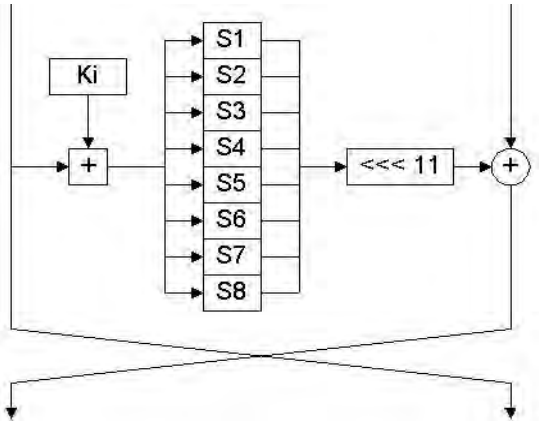

Рис. 2. Раунд алгоритма ГОСТ 28147-89

4. Обработанный предыдущими операциями субблок накладывается на необработанный с помощью побитовой логической операции «исключающее или» (XOR).

5. Субблоки меняются местами.

Процедура расширения ключа в алгоритме ГОСТ 28147-89 фактически отсутствует: в раундах шифрования последовательно используются 32-битные фрагменты K1…K8 исходного 256-битного

ключа шифрования в следующем порядке: K1, K2, K3, K4, K5, K6, K7, K8, за исключением последних 8 раундов – в раундах с 25-го по 31-й фрагменты используются в обратном порядке.

Использование процедур генерации расширенного ключа является элементом, призванным повысить стойкость шифра, или, как замечается в [1], по крайней мере, упростить доказательную базу этой стойкости. Действительно, наличие такой процедуры позволяет рассматривать раундовые ключи в качестве независимых равновероятно распределенных случайных величин.

3. Способы построения расписания ключей

Существует несколько способов построения расписания ключей [2].

Использование предвычислений для формирования расширенного ключа позволяет обеспечить сложную зависимость раундовых ключей от секретного ключа. При этом расширенный ключ представляет собой псевдослучайную последовательность. Недостатком этого подхода является снижение скорости шифрования в приложениях, требующих частой смены ключей. *Непосредственное использование секретного ключа* заключается в использовании частей (размером 32 или 64 бита) секретного ключа в качестве раундовых ключей. Примером шифров, в которых используется такой подход, является российский стандарт ГОСТ 28147-89. Недостатком такого подхода к формированию раундовых ключей является то, что раундовые ключи являются явно зависимыми, что может быть использовано при криптоанализе. Кроме того, оценка стойкости шифра, выполняемая при его проектировании, существенно усложняется необходимостью учѐта данного обстоятельства.

Недостатком представляется также наличие большого числа слабых ключей, т.е. таких ключей, для которых процедура зашифрования совпадает с процедурой расшифрования. Достоинством непосредственного использования частей секретного ключа в качестве раундовых ключей является то, что обеспечивается сохранение высокой скорости шифрования в режиме частой смены ключей.

Формирование раундовых подключей в процессе шифрования блока данных. В этом подходе при аппаратной реализации в качестве первого раундового ключа используется часть секретного ключа, а при выполнении первого раунда шифрования осуществляется формирование второго раундового подключа. При выполнении второго раунда шифрования вычисляется третий раундовый ключ и т. д. Такой ход формирования раундовых ключей имеет место как при выполнении зашифрования, так и при выполнении расшифрования. Учитывая связь между очередностью использования раундовых ключей в этих двух режимах, легко увидеть важность обеспечения формирования одинаковых раундовых ключей на i-м раунде расшифрования и (R–i+1)-м раунде зашифрования, где R – число раундов криптоалгоритма.

Преобразование подключей в зависимости о*т преобразуемых данных* заключается в том, что части секретного ключа используются непосредственно, но перед их наложением на подблоки данных они преобразуются с помощью операций, зависящих от текущего значения одного из подблоков данных. Такое преобразование (механизм внутреннего усложнения ключа) может быть выполнено одновременно с преобразованием другого подблока данных, поэтому оно не приводит к снижению скорости шифрования, хотя обеспечивает существенное улучшение характеристик раундового преобразования.

4. Формирование ключей для криптоалгоритма ГОСТ 28147-89

По нашему мнению, на основе объединения первого и второго из упомянутых подходов может быть предложен ещѐ один. Его идея состоит в том, чтобы элементы множества подключей выбирались на каждом раунде не строго установленным и известным образом, а случайно. Для этого, очевидно, потребуется сформировать процедуру, которая бы по некоторому несекретному правилу позволяла бы каждому раунду криптопреобразования ставить в соответствие подключ из заданного множества подключей. Очевидно, что в данной ситуации необходимо обеспечить приѐмной стороне знание установленного порядка использования подключей (расписания ключей) на раундах криптопреобразования.

Предлагаемый подход может быть реализован, исходя из двух соображений (моделей):

1) формирование расписания ключей производится *независимо* от базового (исходного) ключа;

2) формирование расписания ключей производится *в зависимости* от базового (исходного) ключа.

Каждая из указанных моделей, в свою очередь, может иметь различные реализации. Одна из возможных реализаций первой модели иллюстрируется рис. 3.

Для генерации подключей исходный 256-битный ключ разбивается на восемь 32-битных блоков: $K_1 \ldots K_8$.

Ключи $K_9 \ldots K_{24}$ являются циклическим повторением ключей $K_1 \ldots K_8$ (нумеруются от младших битов к старшим). Ключи $K_{25} \ldots K_{32}$ являются ключами $K_1 \ldots K_8$, идущими в обратном порядке.

Чтобы избавиться от явной зависимости раундовых ключей от секретного ключа, будет генерироваться еще одна процедура, которая независимо

от секретного ключа будет представлять собой набор перестановок Π_i, где $\Pi_i = \{\Pi_{ij}\}$, $j = \overline{1,4}$. Эта процедура позволит представить ключ в виде псевдослучайной последовательности K_1. Следует заметить, что кроме секретного ключа К, при личной встрече передается значение Π_0. Перед шифрованием к сообщению M_i добавляется набор перестановок Π_i, который в процессе расшифрования разделяется и используется для дешифрования сообщения M_{i+1}.

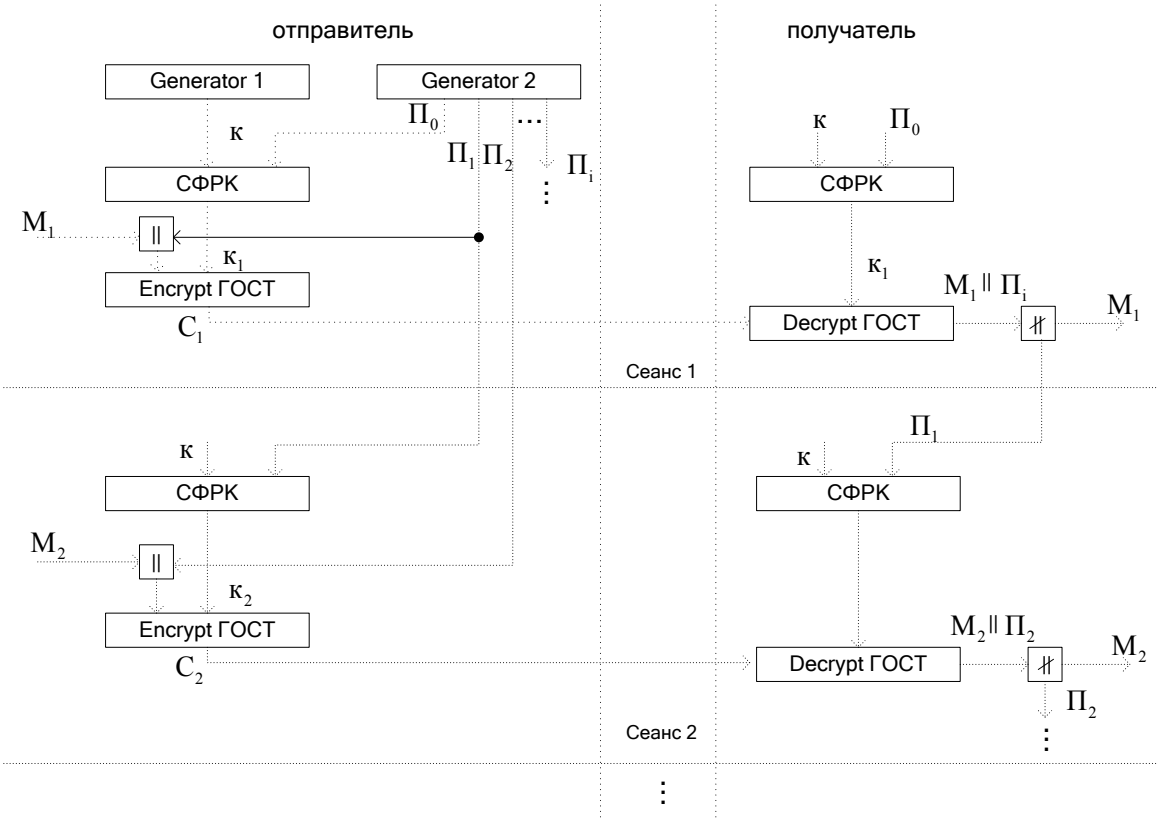

Рис. 3. Реализация формирования расписания ключей для криптоалгоритма ГОСТ 28147-89 независимо от базового ключа

Что касается второй модели, то суть одной из возможных её реализаций заключается в следующем.

В ГОСТе известен порядок использования подключей на раундах шифрования. Высокая криптостойкость обеспечивается большой длиной ключа. Повысить криптостойкость, на наш взгляд, можно, если сделать *неизвестной* для злоумышленника последовательность выбора подключей. Для этого необходимо реализовать несекретную процедуру (рис. 4), которая бы в зависимости от начального ключа (всех 256 бит) позволяла бы организовать перестановку 8 подключей 4 раза (для 32-х раундов).

Например, ситуация может быть следующей:

$$\underbrace{SK_2SK_0SK_4SK_6SK_3SK_5SK_1SK_7}_{\Pi_1};$$

$$\underbrace{SK_3SK_5SK_0SK_4SK_1SK_2SK_7SK_4}_{\Pi_2};$$

$$\underbrace{SK_0SK_7SK_3SK_5SK_4SK_6SK_2SK_1}_{\Pi_3};$$

$$\underbrace{SK_5SK_2SK_7SK_0SK_4SK_1SK_3SK_6}_{\Pi_4}.$$

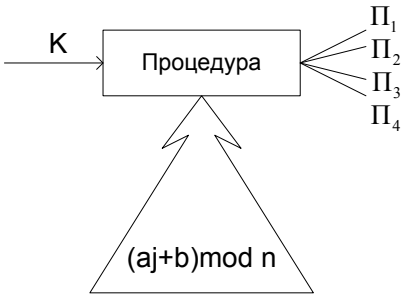

Рис. 4. Реализация формирования расписания ключей для криптоалгоритма ГОСТ 28147-89 в зависимости от базового ключа

Всего может быть

$$N_в = 8!8!8!8! = (8!)^4 =$$

$$= 2642908293365760000 \approx 26 \cdot 10^{17}$$

вариантов выбора 8 подключей для 32 раундов шифрования.

Поскольку среднее число вариантов перебора подключей, необходимое для определения истинного варианта, использованного при шифровании, при случайном выборе этих вариантов и при условии их

равновероятности и независимости равно

$$(N_в – 1)/2,$$

то если вычислительные ресурсы злоумышленника позволяют ему перебирать 10^6 вариантов в секунду, ему потребуется для этого 41950 лет.

Реализация данной процедуры должна основываться на использовании отображения, позволяющего установить взаимнооднозначное соответствие между значениями функции и еѐ аргументами при том, что область определения и область значения функции совпадают. Математическим объектом, удовлетворяющим данному условию, является подстановка.

Поэтому вариантом реализации такого подхода может быть использование преобразований, положенных в основу шифров моноалфавитной подстановки (замены), таких как, например, аффинная система Цезаря, идея криптопреобразований в рамках которой состоит в том, что символы шифртекста получаются из символов исходного текста на основе отображения вида

$$j_i \rightarrow (aj_i + b)(\mathrm{mod}\ m),$$

где j_i – числовой код i-го символа открытого текста;

m – основание (число символов) алфавита исходного текста;

$(aj_i + b)(\mathrm{mod}\ m)$ – числовой код соответствующего символа шифртекста.

При этом a ,b – целые числа, такие, что

$$0 < a, b < m,$$

а числа a и m должны быть взаимно-простыми.

Заключение

Использование рассмотренного подхода, как предполагается, должно усилить криптостойкость алгоритма ГОСТ за счѐт отсутствия зависимости раундовых ключей от секретного ключа (модель 1) и неизвестности для злоумышленника последовательности выбора подключей на раундах шифрования (и большой трудоѐмкости решения этой задачи).

Ещѐ одним аргументом в пользу предлагаемого подхода является то, что, как замечено в [1], «использование секретных подстановок в ГОСТ 28147-89 затрудняет подробное исследование по проблеме потайных входов, что усиливает недоверие независимых пользователей».

При этом под потайным входом (потайной лазейкой) понимается наличие некоторого секрета, преднамеренно внедрѐнного разработчиком криптоалгоритма с целью раскрытия содержимого зашифованных данных без знания секретного ключа пользователей либо раскрытия секретного ключа.

Данное обстоятельство, можно предположить, усугубляется ещѐ и тем фактом, что алгоритм ГОСТ разрабатывался специалистами спецслужб бывшего Советского Союза.

Целью дальнейших исследований является программная реализация предложенного подхода к формированию процедуры расширения ключа для алгоритма ГОСТ 28147-89, а также проверка его работоспособности.

Список литературы

1. Молдовян А.А. Криптография: скоростные шифры / А.А. Молдовян, Н.А. Молдовян, Н.Д. Гуц, Б.В. Изотов. – СПб.: БХВ-Петербург, 2002. – 496 с.

2. Молдовян Н.А. Криптография. От примитивов к синтезу алгоритмов / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. – СПб.: БХВ-Петербург, 2004. – 448 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: ТРИУМФ, 2003. – 816 с.

Поступила в редколлегию 8.09.2010

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

ПІДХІД ДО ФОРМУВАННЯ РОЗКЛАДУ КЛЮЧІВ ДЛЯ БЛОЧНОГО СИМЕТРИЧНОГО КРИПТОАЛГОРИТМА ГОСТ 28147-89

Є.М. Асташкіна, І.В. Лисенко

Пропонується підхід до формування розкладу ключів криптоалгоритма ГОСТ 28147-89з метою підвищення його криптостійкості. В межах даного підходу розглядається дві моделі формування розкладу ключів.

Ключові слова: *конфіденційність, розширення ключа, блочний криптоалгоритм.*

THE APPROACH TO THE FORMATION OF BLOCK SCHEDULING KEYS FOR SYMMETRIC CRYPTOGRAPHIC ALGORITHM GOST 28147-89

Y.N. Astashkina, I.V. Lysenko

In order to increase cryptographic proofness of the cryptographic algorithm GOST 28147-89 an approach to the formation of keys schedule for this algorithm is proposed. Two models of the keys schedule formation are considered relatively this approach.

Keywords: *confidentiality, keys schedule, block cipher.*