УДК 004.056.55,519.1

КЛЮЧЕВОЕ РАСПИСАНИЕ В СИСТЕМАХ БЛОЧНОГО ШИФРОВАНИЯ

Романько Д.А.,
аспирант, Финансовый университет, Москва, Россия
dmax.rda@gmail.com

Аннотация. *Свойства ключевого расписания являются определяющими при оценке стойкости алгоритма блочного шифрования, так как при определенных условиях плохо подобранное ключевое расписание (или использование так называемых слабых и частично слабых ключей) может ослабить криптографические свойства итеративного блочного шифра. Приведены способы построения ключевого расписания некоторых известных алгоритмов блочного шифрования, отмечены их свойства. Предложен способ построения альтернативного ключевого расписания.*

Ключевые слова: *блочный шифр; ключевое расписание; раундовый ключ.*

KEY SHEDULE IN BLOCK CIPHER SYSTEMS

Romanko D.A.,
Post-graduate student, Financial University, Moscow, Russia
dmax.rda@gmail.com

Abstract. *The strength of block cipher is determined by the properties of key schedule. Under some circumstances key shedule which was chosen improperly (or in case of using so-called weak keys and semi-weak keys) could make the block cipher weaker. Some examples of building key schedule in modern well-known block ciphers are given. The alternative way of key schedule building is suggested.*

Keywords: *block cipher; key schedule; round key.*

Пусть K — ключ итеративного блочного алгоритма шифрования. Тогда ключевым расписанием называется система функций $\{\theta_1, \theta_2, \ldots, \theta_r\}$, при помощи которой ключ K расширяется до r ключей $k_1, \ldots, k_r$. В большинстве случаев r — число раундов итеративного блочного шифра.

Рассмотрим ключевое расписание алгоритмов DES, ГОСТ 28147–89, ГОСТ Р 34.10–2015 «Магма» и «Кузнечик», AES (с длинами ключей 128, 192 и 256 битов).

1. Ключевое расписание алгоритма DES

DES (Data Encryption Standard) — итеративный 16-раундовый блочный алгоритм шифрования с длиной блока 64 бита и длиной ключа 64 бита, 8 из которых являются проверочными и не используются при шифровании. Введен в действие в США в 1977 г. как национальный стандарт. В настоящее время заменен на AES (в 2002 г.), однако 3DES, полностью основанный на DES, продолжает использоваться по всему миру (например, в стандартах S/MIME, ANSI X9.17).

В процессе генерации раундовых ключей для каждого из 16 раундов алгоритма DES генерируется 48-битный раундовый ключ, определяемый при помощи ряда преобразований. Сначала выполняется перестановка битов ключа по *табл. 1* (в ячейках приведены номера битов исходного ключа).

Научный руководитель: ***Фомичев В.М.,*** *доктор физико-математических наук, профессор, профессор Финансового университета, НИЯУ МИФИ, ведущий научный сотрудник ФИЦ ИУ РАН, научный консультант ООО «Код Безопасности».*

Таблица 1

Начальная перестановка ключа

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Таблица 2

Число битов сдвига в зависимости от раунда

Раунд	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Сдвиг	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Таблица 3

Усеченная подстановка ключа

14	17	11	24	1	5	3	28	15	6	21	10
23	19	11	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

То есть первым битом после преобразования станет 57-й бит исходного ключа и т.д. Получившийся 56-битовый вектор делится на два 28-битовых вектора. Оба вектора сдвигаются влево на одинаковое число шагов в соответствии с *табл. 2*.

Из полученного 56-битового вектора выбирается 48 битов (по 24 бита из каждой 28-битовой половины) — реализуется усеченная подстановка в соответствии с *табл. 3*.

В процессе криптографического анализа алгоритма впервые было введено понятие слабого ключа, и связано оно со свойством ключевого расписания, заключающемся в совпадении раундовых ключей на различных раундах шифрования. Например, если при разделении 56-битового вектора на два 28-битовых вектора обе половины состоят из одинаковых битов, то все раундовые ключи совпадают. Некоторые пары ключей переводят открытый текст в идентичный шифртекст [1],

что означает, что один ключ может расшифровать сообщение, полученное на другом ключе. В [2] понятие «слабый ключ» обобщено, а предложенный подход к анализу ключевого расписания может быть применен к любому итеративному блочному алгоритму шифрования. Подробно проблема слабого ключевого расписания DES-алгоритма рассмотрена в [3–5].

2. Ключевое расписание алгоритма ГОСТ 28147–89

ГОСТ 28147–89 — стандарт шифрования, опубликованный в 1990 г. в СССР [6]. Действующий стандарт РФ. Число раундов — 32, длина блока алгоритма — 64 бита, длина ключа — 256 битов. Длина каждого раундового ключа составляет 32 бита.

Ключевое расписание представляется следующим образом: исходный ключ $K = (w_1, w_2, w_3,..., w_{256})$, $w_j \in V_1$, $j = 1,...,256$, разбивается на восемь 32-битных векторов k_i, $i = 1,...,8$:

$$k_1 = (w_{32}, w_{31},..., w_1),$$
$$k_2 = (w_{64}, w_{63},..., w_{33}),$$
$$...,$$
$$k_8 = (w_{256}, w_{255},..., w_{225}),$$

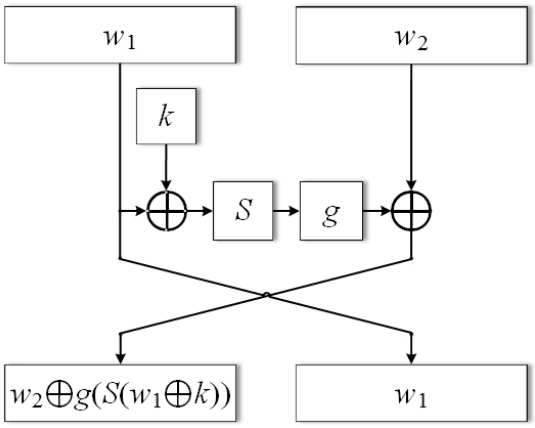
затем раундовые ключи выбираются по правилу:

$$(k_1,...k_8, k_1,..., k_8, k_1,..., k_8, k_8,..., k_1). \quad (1)$$

Из (1) следует, что любой ключ алгоритма ГОСТ 28147–89 является 8-слабым. Существует ряд атак, основанных, в частности, на слабостях ключевого расписания [7–9], а в работе [10] обосновывается необходимость модификации ключевого расписания и приводится альтернативный метод генерации раундовых ключей. Однако данный метод лишь меняет порядок раундовых ключей, не решая при этом проблему появления слабых и частично слабых ключей.

3. Ключевое расписание алгоритмов ГОСТ Р 34.10–2015

С 1 января 2016 г. в России начал действовать новый стандарт блочного шифрования — ГОСТ Р 34.10–2015 [11], включающий в себя два итеративных блочных алгоритма шифрования: с длиной блока 64 бита («Магма») и с длиной блока 128 битов («Кузнечик»). Ключ обоих алгоритмов имеет длину 256 битов.



Графическое представление преобразования (3)

3.1. Итеративный блочный алгоритм шифрования с длиной блока 64 бита «Магма»

«Магма» реализует 32-раундовый итеративный блочный алгоритм шифрования, основанный на петле Фейстеля. Длина раундовых ключей — 32 бита.

Для генерации раундовых ключей исходный ключ K длины 256 бит разбивается на восемь 32-битных блоков k_i, $i = 1,...,8$:

$$K = (k_1, k_2,..., k_8), \quad (1)$$

которые используются в следующем порядке, аналогично ГОСТ 28147–89:

$$(k_1,...k_8, k_1,..., k_8, k_1,..., k_8, k_8,..., k_1). \quad (2)$$

Из (2) следует, что, как и в ГОСТ 28147–89, любой ключ является 8-слабым. Из-за конструктивных особенностей «Магмы» атаки [7–9] могут быть применены к данному итеративному блочному алгоритму шифрования.

3.2. Итеративный блочный алгоритм шифрования с длиной блока 128 битов «Кузнечик»

«Кузнечик» реализует 10-раундовый (один из которых — завершающий) итеративный блочный алгоритм шифрования, представляющий собой подстановочно-перестановочную сеть. Длина раундовых ключей — 128 битов.

Пусть задано преобразование g линейного регистра левого сдвига длины 128 с функцией обратной связи f_g. То есть при заполнении регистра $(x_1, x_2,..., x_m)$

$$g(x_1, x_2,..., x_m) = x_2,..., x_m, f_g(x_1, x_2 ..., x_m),$$

где f_g — линейная функция обратной связи, определенная в стандарте [11].

Пусть задано преобразование петли Фейстеля:

$$F[k](w_1, w_2) = (w_2 \oplus g(S(w_1 \oplus k)), w_1), \quad (3)$$

где S — нелинейное преобразование, определенное в стандарте [11], k, w_1, $w_2 \in V_{128}$. Графическое представление (3) приведено на *рисунке*.

Пусть ключ итеративного блочного алгоритма шифрования $K = (w_1, w_2, w_3,..., w_{256})$, тогда раундовые ключи вырабатываются по правилу:

$$k_1 = (w_1, w_2,..., w_{128}),$$
$$k_2 = (w_{129}, w_{130},..., w_{256}),$$
$$(k_{2i+1}, k_{2i+2}) = F_j[C_{8(i-1)+8}]...F_j[C_{8(i-1)+1}](k_{2i-1}, k_{2i}),$$

где $i = 1, 2, 3, 4$, C_j, $j = 1,...,32$ — константы, определенные в стандарте [11].

Если $k_1 = k_2$, ключ «Кузнечика» является 9-слабым.

4. Ключевое расписание алгоритма AES

В 1997 г. был объявлен конкурс на разработку нового стандарта блочного шифрования. К 2000 г. в финал вышли алгоритмы Rijndael, Serpent, Twofish, RC6, MARS, из которых, по результатам голосования Rijndael был выбран победителем и стал известен как AES (Advanced Encryption Standard) [12]. Является действующим стандартом шифрования США.

AES — итеративный блочный алгоритм шифрования с длиной блока 128 битов, реализующий подстановочно-перестановочную сеть с 10, 12 или 14 раундами и ключом 128, 192 или 256 битов соответственно [13]. Длина каждого раундового ключа AES составляет 128 битов.

Ключ алгоритма K представляется как NK 32-битных векторов, где NK определяется длиной выбранного ключа: $K = (w_1,..., w_{NK})$.

Пусть задано преобразование $g(x_1, x_2, x_3, x_4) = (x_2, x_3, x_4, x_1)$, $x_1, x_2, x_3, x_4 \in V_{32}$.

4.1. Алгоритм AES-128

В случае AES-128, $NK = 4$. Раундовые ключи генерируются по правилу:

$$k_1 = K = (w_1, w_2, w_3, w_4),$$
$$k_i = (w_{4(i-1)} \oplus w_{4(i-2)+1}, w_{4(i-1)+1} \oplus w_{4(i-2)+2},$$
$$w_{4(i-1)+2} \oplus w_{4(i-2)+3}, S(g(w_{4(i-1)+3})) \oplus w_{4(i-1)} \oplus C_i),$$

где $i = 2, ..., 11$; S — нелинейная замена (S-box), определенная в стандарте [13], C_i — константы, получаемые по закону, определенному в стандарте [13], $i = 2,...,11$.

4.1. Алгоритм AES-192

В случае AES-192, $NK = 6$. Раундовые ключи генерируются по правилу:

$$k_1 = (w_1, w_2, w_3, w_4),$$
$$k_2 = (w_5, w_6, w_6 \oplus w_3, w_7 \oplus w_4),$$
$$k_i = (y_{i,1},..., y_{i,4}),$$

$$y_{i,j} = w_{4(i-1)+j-1} \oplus w_{4(i-2)-2+j},$$

если $(4(i - 1) + j)$ не кратно 6;

$$y_{i,j} = S(g(w_{4(i-1)+j-1})) \oplus w_{4(i-2)-2+j} \oplus C_i,$$

если $(4(i - 1) + j)$ кратно 6,

где $i = 3,...,13$; $j = 1,...,4$; S — нелинейная замена (S-box), определенная в стандарте [13]; C_i — константы, получаемые по закону, определенному в стандарте [13]; $i = 3,...,13$.

4.3. Алгоритм AES-256

В случае AES-256, $NK = 8$. Раундовые ключи генерируются по правилу:

$$k_1 = (w_1, w_2, w_3, w_4),$$
$$k_2 = (w_5, w_6, w_7, w_8),$$
$$k_i = (y_{i,1},..., y_{i,4}),$$

$$y_{i,j} = w_{4(i-1)+j-1} \oplus w_{4(i-3)+j},$$ если $(4(i - 1) + j)$

не кратно 8 и $(4(i - 2) + j)$ не кратно 8,

$$y_{i,j} = S(g(w_{4(i-1)+j-1})) \oplus w_{4(i-3)+j} \oplus C_i,$$

если $(4(i - 1) + j)$ кратно 8,

$y_{i,j} = S(w_{4(i-1)+j-1}) \oplus w_{4(i-3)+j}$, если $(4(i - 2) + j)$ кратно 8,

где $i = 3,...,15$; $j = 1,...,4$; S — нелинейная замена (S-box), определенная в стандарте [13]; C_i — кон-

станты, получаемые по закону, определенному в стандарте [13]; $i = 3, \ldots, 15$.

В работе [14] приводятся недостатки ключевого расписания итеративного блочного алгоритма шифрования AES (с длинами ключей 128, 192 и 256) и обосновывается необходимость его модификации.

5. Выводы

Шифрующие подстановки итеративных блочных алгоритмов шифрования по своим свойствам должны быть близки к случайным подстановкам, в таком случае итеративный блочный шифр можно назвать «идеальным» [12]. В частности, важно, чтобы набор раундовых ключей по своим свойствам был похож на случайную бесповторную выборку из множества двоичных векторов заданной размерности. В связи с этим возникает задача построения ключевого расписания, исключающего возможность повторений раундовых ключей в генерируемом наборе. Данная задача рассматривается, например, в [15, 16].

Список источников

1. *Шнайер Б.* Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке Си / Б. Шнайер. М.: Триумф, 2002. 610 с.
2. *Фомичев В.М.* Методы дискретной математики в криптологии / В.М. Фомичев. М.: Диалог-МИФИ, 2010. 424 с.
3. *Alfred J.M.* Handbook of Applied Cryptography (Discrete Mathematics and Its Applications) / J.M. Alfred, P.C. van Oorschot, S.A. Vanstone. CRC Press, 1996. P. 796.
4. *Matsui M.* Linear Cryptanalysis Method for DES Cipher. / M. Matsui // Advances in Cryptology EUROCRYPT'93 Proceedings. Berlin: Springer-Verlag, 1994. P. 386–397.
5. *Moore J.H.* Cycle Structure of the DES with Weak and Semi-Weak Keys. / J.H. Moore, G.J. Simmons // Advances in Cryptology CRYPTO'86 Proceedings. Berlin: Springer-Verlag, 1987, pp. 2–32.
6. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М.: ИПК Издательство стандартов, 1996.
7. *Pudovkina M.A.* Related-Key Attack on Block Ciphers with Weak Recurrent Key Schedules / M. Pudovkina // Foundations and Practice of Security. Berlin: Springer-Verlag, 2011, pp. 90–101.
8. *Rudskoy V.* On zero practical significance of "Key recovery attack on full GOST block cipher with zero time and memory" / V. Rudskoy // Cryptology ePrint Archive, Report 2010/111. 2010. 24 p.
9. Isobe T.A Single-Key Attack on the Full GOST Block Cipher / T. Isobe *// Journal of Cryptology*, 2013, no. 26, pp. 172–189.
10. *Асташкина Е.Н.* Подход к формированию расписания ключей для блочного симметричного криптоалгоритма ГОСТ 28147–89. / Е.Н. Асташкина, И.В. Лысенко // *Системи обробки інформації.* 2010. № 6. С. 30–34.
11. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
12. *Ferguson N.* Cryptography Engineering: Design Principles and Practical Applications / N. Ferguson, B. Schneier, T. Kohno. Wiley Publishing, Inc. 2010. 353 p.
13. Federal Information Processing Standards Publication 197 "Specification for the ADVANCED ENCRYPTION STANDARD (AES)" — Gaithersburg: National Institute of Standards and Technology (NIST), 2001. 51 p.
14. *May L.* Strengthening the Key Schedule of the AES. / L. May, M. Henricksen, W. Millan, G. Carter, E. Dawson // Information Security and Privacy. Berlin: Springer-Verlag, 2002. P. 226–240.
15. *Романько Д.А.* О способах построения криптографических генераторов с заданным показателем бесповторности выходных последовательностей. / Д.А. Романько, В.М. Фомичев // Томский гос. ун-т. Прикладная дискретная математика. Приложение № 9. С. 65–67.
16. *Фомичев В.М.* О ключевом расписании блочных шифров без слабых ключей / В.М. Фомичев // Томский гос. ун-т. Прикладная дискретная математика. Приложение № 9. С. 70–73.

УДК 343.98

НЕОТЛОЖНЫЕ ДЕЙСТВИЯ В ОРГАНИЗАЦИИ ПОСЛЕ ИНЦИДЕНТА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гайстер С.В.,
студент, Финансовый университет, Москва, Россия
sergeygaister@yandex.ru

Аннотация. *Сегодня имеются веские основания полагать, что применяемые в настоящее время большинством организаций меры не обеспечивают необходимого уровня безопасности субъектов, участвующих в процессе информационного взаимодействия, и не способны в необходимой степени противостоять разного рода воздействиям с целью доступа к критичной информации и дезорганизации работы информационных систем. Целью данной статьи является изучение рекомендаций для организаций, пострадавших от инцидентов в сфере информационной безопасности (ИБ), на основе исследования Национального центра по защите инфраструктуры США. Формулируется немедленная последовательность действий при обнаружении инцидента в рамках российской действительности.*

Ключевые слова: *компьютерная криминалистика; инциденты ИБ; информационная безопасность организации.*

IMMEDIATE ACTIONS IN THE ORGANIZATION AFTER THE INCIDENT IN THE SPHERE OF INFORMATION SECURITY

Gaister S.V.,
student, Financial University, Moscow, Russia
sergeygaister@yandex.ru

Abstract. *Today, there are strong reasons to believe that the measures currently applied by most organizations do not provide the necessary level of security for the actors involved in the information communication process and are not able to withstand the necessary effects in order to access critical information and work disorganization information systems. The purpose of this article is to study recommendations for organizations affected by incidents in the field of information security (IS), based on the study of the National Center for Infrastructure Protection in the United States. An immediate sequence of actions is formulated when an incident is detected within the framework of Russian reality.*

Keywords: *computer forensics; IS incidents; information security of the organization.*

Научный руководитель: ***Крылов Г.О.,*** *доктор физико-математических наук, профессор, Финансовый университет.*