ОЦЕНКА ЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТИ СТАНДАРТА АЛГОРИТМА ШИФРОВАНИЯ AES-FIPS-197

Узаков Ортик Шаймарданович,
Каршинский филиал ташкентского университета информационных технологий имени Мухаммада аль-Хоразмий, Кафедра «Информационных технологии», ассистент

Оценка экспоненциальной сложности дешифрования шифр текстов позволит дать ответ на вопрос, “каким должен быть крипто стойкий алгоритм шифрования”, чтобы дешифрование шифр текста не было практически возможным без исходного ключа шифрования.

В 2001 году стандартом шифрования данных был принять AES (Advanced Encryption Standard) (FIPS -197) за основу которого был взять алгоритм шифрования RIJNDAEL, разработанный Бельгийскими специалистами Йон Дэмен (Joan Daemen) и Винсент Рюмен (Vincent Rijmen), начальные буквы фамилий которых и образуют название алгоритма – *RIJNDAEL*. RIJNDAEL – это итерационный блочный алгоритм шифрования, имеющий архитектуру "Квадрат". Алгоритм шифрования имеет переменную длину блоков и различные длины ключей. Длина ключа и длина блока могут быть равными независимо друг от друга 128, 192 или 256 битам. В стандарте *AES* определена длина блока данных, равная 128 битам.

Промежуточные результаты преобразований, выполняемых в рамке алгоритма, называются *состояниями (State).* Состояние можно предоставить в виде прямоугольного массива байтов. В общем случае число столбцов N_b равно $N_b = l:32$, где $l=128, 192, 256$ - длина блока входных данных в битах. При размере блока входных данных, равном $l=128$ битам, этот 128:8 = 16-байтовый массив имеет 4 строки и 4 столбца, каждая строка и каждый столбец в этом случае могут рассматриваться как 4 ×8= 32- разрядные слова (Рис. 1 а), где a_i –байт блока данных. В случае $l = 192$, имеем $N_b = l:32=6$ и при $l = 256$, имеем $N_b = l:32=8$, где значения 6 и 8 определяют число столбцов таблицы состояний. Таким образом, в случае $l = 128$ имеем таблицу состояний 4×4, при $l = 192$ имеем таблицу состояний 4×6, при $l = 256$ имеем таблицу состояний 4×8. Входные данные для шифра обозначаются как байты состояния, например, при $l = 128$ в порядке $s_{00}, s_{10}, s_{20}, s_{30}, s_{01}, s_{11}, s_{21}, s_{31}, s_{02}, s_{12}, s_{22}, s_{32}, s_{03}, s_{13}, s_{23}, s_{33}$ (Рис.1 б). Аналогично, 128 битовый ключ шифрования представляется байтами $k_{00}, k_{10}, k_{20}, k_{30}, k_{01}, k_{11}, k_{21}, k_{31}$, $k_{02}, k_{12}, k_{22}, k_{32}, k_{03}, k_{13}, k_{23}, k_{33}$ (Рис. 1 в).

a_0	a_4	a_8	a_{12}
a_1	a_5	a_9	a_{13}
a_2	a_6	a_{10}	a_{14}
a_3	a_7	a_{11}	a_{15}

а)

s_{00}	s_{01}	s_{02}	s_{03}
s_{10}	s_{11}	s_{12}	s_{13}
s_{20}	s_{21}	s_{22}	s_{23}
s_{30}	s_{31}	s_{32}	s_{33}

б)

k_{00}	k_{01}	k_{02}	k_{03}
k_{10}	k_{11}	k_{12}	k_{13}
k_{20}	k_{21}	k_{22}	k_{23}
k_{30}	k_{31}	k_{32}	k_{33}

в)

Рис. 1. Пример представления 128-разрядного блока данных в виде массива *State*.

а) пример представления блока $a_{i,}$, где a_i - байты блока данных, а каждый столбец - одно 32-разрядное слово;

б) пример представления блока входных данных (N_b= 4), где s_{ij} - байты блока данных, находящиеся на пересечении *i*-й строки и *j*-го столбца.;

в) пример представления ключа шифрования (N_k= 4), где k_{ij} - байты ключа, находящиеся на пересечении *i*-й строки и *j*-го столбца.

Число раундов N_r в алгоритме RIJNDAEL зависит от значений N_b и N_k как показано в таблице 1. В стандарте AES определено соответствие между размером ключа, размером блока данных и числом раундов шифрования, как показано в таблице 2:

Таблица 1. Число раундов N_r как функция от длины ключа N_k и длины блока N_b.

N_r	$N_b = 4$	$N_b = 6$	$N_b = 8$
$N_k = 4$	10	12	14
$N_k = 6$	12	12	14
$N_k = 8$	14	14	14

Таблица 2. Соответствие между длиной ключа, размером блока данных и числом раундов в стандарте AES.

Стандарт	Длина ключа (N_k)	Размер блока данных (N_b)	Число раундов (N_r)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Ниже рассчитаем степень экспоненциальной сложности для стандарта алгоритма шифрования AES-128, схема алгоритма шифрования приведена на рис. 2.

Вначале мы имеем значение выходного блока данных *B*(128 бит), вычисляем значение раундового ключа десятого раунда шифрования, который складывается по операции XOR с выходом значения операции сдвига строк *ShiftRows*( ). Для нахождения раундового $AddRoundKey = ShiftRows \oplus B$ ключа необходимо 2^{128} операций полного перебора – степень экспоненциальной сложности данного преобразования.

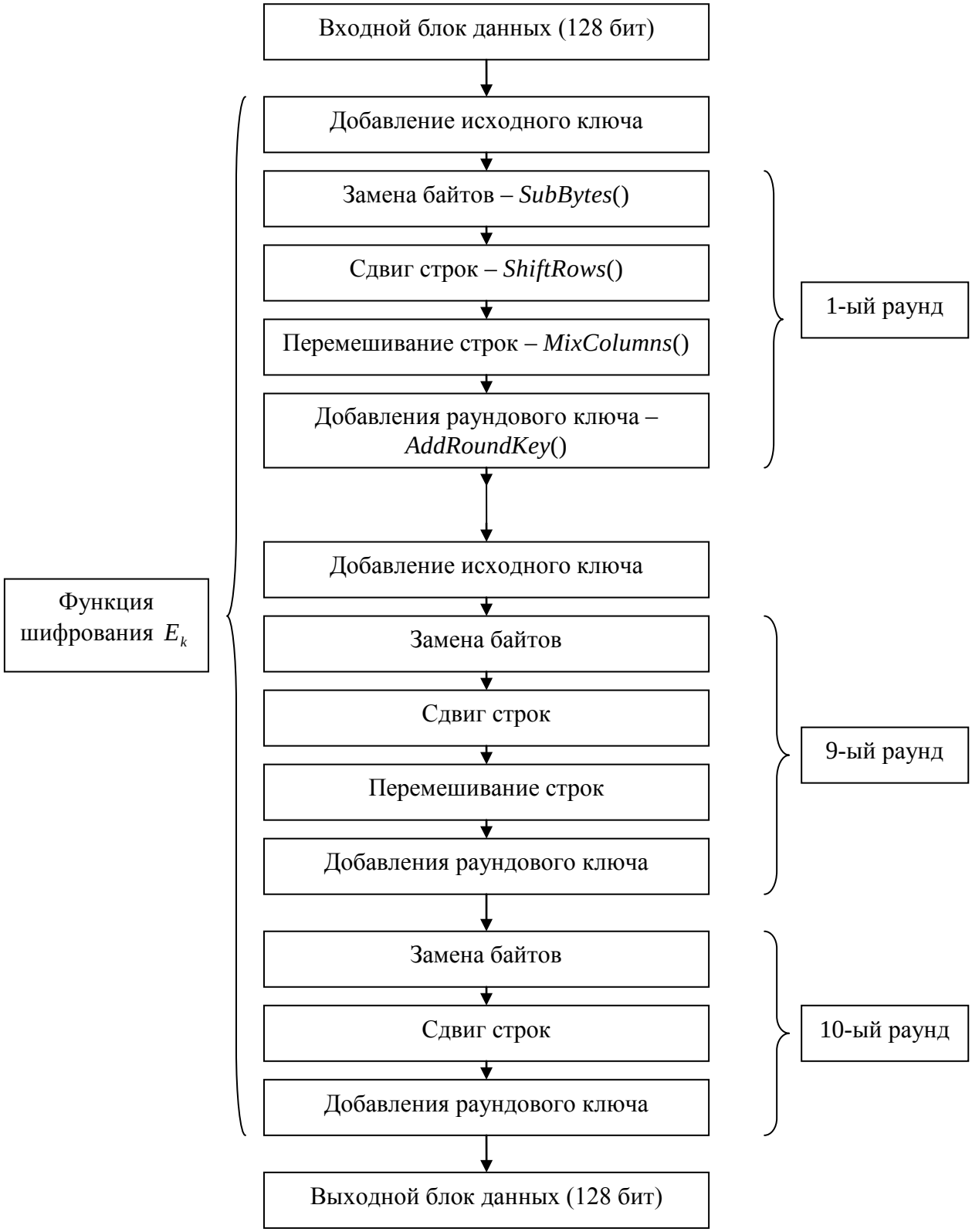

Рисунок 2. Схема стандарта алгоритма шифрования AES.

Таблица 3. Таблица зависимости числа сдвига строк от длины входного блока.

L	N_b	C_0	C_1	C_2	C_3
128	4	0	1	2	3
192	6	0	1	2	3
256	8	0	1	3	4

Одновременно мы имеем значение выхода операции сдвига строк ShiftRows() десятого раунда шифрования.

Далее мы находим значение входа операции сдвига строк ShiftRows(). Преобразование сдвига строк ShiftRows() – побайтового сдвига строк массива состояний на различное количество байт. Нулевая строка $S'_{00}\ S'_{01}\ S'_{02}\ S'_{03}$ остается без сдвига. Остальные 3 строки состояния циклически сдвигаются влево на различное число байтов. Значения сдвигов первой строки C_1 , второй строки C_2 , третьей строки C_3 зависят от длины блока N_b –количество 32-разрядных (битных) слов или l -длины блока данных в битах и задаются таблицей 3. Данное преобразование не дает никакой сложности.

Далее мы находим значение входа операции замены байтов *SubBytes*() - побайтовой подстановки в S-блоках с фиксированной таблицей замен размерностью 16×16, включающееся двух преобразований входного байта:

1) Первое преобразование каждого байта состояния s_{ij} преобразуется на мультипликативный обратный элемент s_{ij}^{-1} поля $GF(2^8)$, по-другому выражаясь, получение обратного элемента относительно умножения в поле $GF(2^8)$, т.е. $s_{ij}s_{ij}^{-1} \equiv 1 \bmod(x^8 + x^4 + x^3 + x + 1)$, при этом нулевой элемент $\{00\}$ переходит сам в себя;

2) Второе преобразование обеспечивает над полем $GF(2)$ аффинное преобразование обратного элемента $b = s_{ij}^{-1}$ (1) по правилу $Cb + c_0 \bmod(x^8 + 1) = b'$ следующим образом:

$$\begin{bmatrix} 10001111 \\ 01000111 \\ 11100011 \\ 11110001 \\ 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} \qquad (1)$$

Эти два преобразования осуществляются в конечных полях, поэтому число значений результата преобразований конечное и результаты этих двух преобразования даются по таблице 4.

Таблица 4. S-блок стандарта алгоритма шифрования AES-128.

X\Y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	12	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	62	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	Be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	18	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	Ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4d	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

В стандарте алгоритма шифрования AES S-блок является известным и данное преобразование никакой сложности не дает. Таким образом мы получили выход из девятого раунда алгоритма шифрования.

В раундах с девятого по первый мы выполняем аналогичные преобразования восстановления всех остальных раундовых ключей. За исключением того, что в данных раундах мы имеем дело ещё с одним преобразованием – перемешивание столбцов *MixColumns*. В этом преобразование столбцы состояния рассматриваются как многочлены степени не более трех с коэффициентами из поля $GF(2^8)$ и умножаются по модулю x^4+1 на многочлен $g(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$.

Для удобства если вводить обозначение (2.3.1), что

$$\begin{aligned} &s_{00} = s'_{00}, s_{10} = s'_{11}, s_{20} = s'_{22}, s_{30} = s'_{33}, \\ &s_{01} = s'_{01}, s_{10} = s'_{12}, s_{21} = s'_{23}, s_{31} = s'_{30}, \\ &s_{02} = s'_{02}, s_{12} = s'_{13}, s_{22} = s'_{20}, s_{32} = s'_{31}, \\ &s_{03} = s'_{03}, s_{13} = s'_{10}, s_{23} = s'_{21}, s_{33} = s'_{32}. \end{aligned} \qquad (1)$$

Столбцы таблицы состояний, всегда состоящие из четырех байт, представляется полиномами третьей степени: $s(x) = s_{3j}x^3 + s_{2j}x^2 + s_{1j}x + s_{0j} (\mathrm{mod}\, x^4 + 1)$, j=0,1,2,3,4. Коэффициенты $s(x) = s_{3j}x^3 + s_{2j}x^2 + s_{1j}x + s_{0j} (\mathrm{mod}\, x^4 + 1)$ принимают значения в интервале от нуля $0_{10} = (00000000)_2$ до $255_{10} = (11111111)_2$. Преобразованный столбец $s'(x)$ есть $g(x) \otimes s(x) \bmod (x^4 + 1) = s'(x)$.

Это последнее равенство преобразования в матричном виде имеет вид (3) (конечно с учетом модуля умножения):

$$\begin{bmatrix} s'_{0j} \\ s'_{1j} \\ s'_{2j} \\ s'_{3j} \end{bmatrix} = \begin{bmatrix} \{02\}\{03\}\{01\}\{01\} \\ \{01\}\{02\}\{03\}\{01\} \\ \{01\}\{01\}\{02\}\{03\} \\ \{03\}\{01\}\{01\}\{02\} \end{bmatrix} \bullet \begin{bmatrix} s_{0j} \\ s_{1j} \\ s_{2j} \\ s_{3j} \end{bmatrix} = \begin{bmatrix} (\{02\} \bullet s_{0j}) \oplus (\{03\} \bullet s_{1j}) \oplus s_{2j} \oplus s_{3j} \\ s_{0j} \oplus (\{02\} \bullet s_{1j}) \oplus (\{03\} \bullet s_{2j}) \oplus s_{3j} \\ s_{0j} \oplus s_{1j} \oplus (\{02\} \bullet s_{2j}) \oplus (\{03\} \bullet s_{3j}) \\ (\{03\} \bullet s_{0j}) \oplus s_{1j} \oplus s_{2j} \oplus (\{02\} \bullet s_{3j}) \end{bmatrix} \quad (3).$$

Данное преобразование никакой сложности не представляет.

После восстановления входного значения первого раунда мы восстанавливаем значение исходного ключа (128 бит) (операция XOR) – степень экспоненциальной сложности так же составляет 2^{128} операций полного перебора. Получаем значение исходного входного блока открытого текста и значение исходного и 10-ти раундовых ключей.

Таким образом, в алгоритме AES степень экспоненциальной сложности зависит от длины входного блока и размера ключа. В таблице 5 приведены значения степень экспоненциальной сложности стандарта алгоритма шифрования AES.

Таблица 5. Степень экспоненциальной сложности стандарта алгоритма шифрования AES.

AES-128		
Тип преобразования	Вид преобразования	Степень экспоненциальной сложности
Операция побитного сложения по модулю 2	$AddRoundKey = ShiftRows \oplus B$	2^{128}
Один раунд шифрования	2^{128}	2^{128}
10 раундов шифрования	$2^{128*10}2^{128}$	2^{1408}
AES-192		
Операция побитного сложения по модулю 2	$AddRoundKey = ShiftRows \oplus B$	2^{192}
Один раунд шифрования	2^{192}	2^{192}
12 раундов шифрования	$2^{192*12}2^{192}$	2^{2496}
AES-256		
Операция побитного сложения по модулю 2	$AddRoundKey = ShiftRows \oplus B$	2^{256}
Один раунд шифрования	2^{256}	2^{256}
14 раундов шифрования	$2^{256*14}2^{256}$	2^{3840}

В заключение хочется отметить, с использованием в данной методов оценки экспоненциальной сложности можно дать оценку стойкости других алгоритмов шифрования.

Литература

1. Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши” - Тошкент, 2008 394 бет.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. -М.: издательство ТРИУМФ, 2003 - 816 стр.
3. Практическая криптография. Нильс Фергюсон, Брюс Шнайер. 2005.