© Tuychiev G. The development of block encryption algorithm based on IDEA32-4 and RFWKIDEA32-4 networks using transformation of the encryption algorithm AES // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 2, p. 148-158.

СОЗДАНИЕ БЛОЧНОГО АЛГОРИТМА ШИФРОВАНИЯ НА ОСНОВЕ СЕТЕЙ IDEA32–4 И RFWKIDEA32–4 С ИСПОЛЬЗОВАНИЕМ ПРЕОБРАЗОВАНИЯ АЛГОРИТМА ШИФРОВАНИЯ AES

Гулом Туйчиев

Национальный университет Узбекистана им. Мирзо Улугбека, Республика Узбекистан

ТУЙЧИЕВ Гулом Нумонович, к.т.н.

Год и место рождения: 1981 год, г. Самарканд, Республика Узбекистан.
Образование: Национальный университет Узбекистана им. Мирзо Улугбека, 2002.
Должность: преподаватель кафедры информатики и прикладного программирования.
Научные интересы: информационная безопасность.
Публикации: более 35 научных публикаций.
E-mail: blasterjon@gmail.com

Аннотация. *На сегодняшний день одним из наиболее эффективных симметричных блочных шифров является AES. В статье разработаны алгоритмы блочного шифрования AES–IDEA32–4 и AES–RFWKIDEA32–4 на основе сети IDEA32–4 и RFWKIDEA32–4. В алгоритме шифрования AES–IDEA32–4 в качестве раундовой функции выбраны преобразования SubBytes(), ShiftRows(), MixColumns(), AddRoundKey(), а в алгоритме шифрования AES–RFWKIDEA32–4 в качестве раундовой функции выбраны преобразования SubBytes(), ShiftRows(), MixColumns(). Длина блока алгоритмов шифрования равна 512 битам, количество раундов равно 10, 12, 14 и длина ключа изменяется от 256 бит до 1024 бит с шагом 128 бит.*

Ключевые слова: *криптография, симметричный алгоритм, преобразования, раунд, раундовая функция, ключ, зашифрование, расшифрование.*

Введение

Advanced Encryption Standard (AES), также известный как Rijndael–симметричный алгоритм блочного шифрования, принятый в качестве стандарта шифрования правительством США по результатам конкурса AES [14, 15]. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES. AES основан на архитектуре квадрат и количество раундов n равно 10, 12, 14, длина блока равна 128 битам и длина ключа равна 128, 192 и 256 битам. Данный шифр состоит из преобразований SubBytes(), ShiftRows(), MixColumns(), AddRound Key() и InvSubBytes(), InvShiftRows(), InvMix Columns(). При зашифровании используются преобразования SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() и при расшифровании InvSub Bytes(), InvShiftRows(), InvMixColumns(), AddRoundKey().

В данном шифре 16 байтовый, т.е. 128 битовый блок (t_0, t_1, …, t_{15}) записывается в массив State следующим образом:

t_0	t_4	t_8	t_{12}
t_1	t_5	t_9	t_{13}
t_2	t_6	t_{10}	t_{14}
t_3	t_7	t_{11}	t_{15}

Преобразование SubBytes() является единственным нелинейным преобразованием алгоритма шифрования AES. В данном преобразовании каждый байт массива State преобразуется в S–блоке и преобразование SubBytes() можно представить следующим образом:

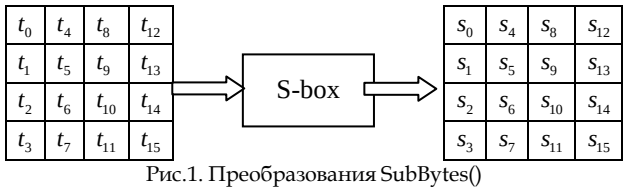

Рис.1. Преобразования SubBytes()

В преобразовании ShiftRows() строки массива State сдвигаются влево на различное число байтов. Первая строка сдвигается на 1 байт, вторая строка на 2 байта и третья строка на 3 байта. Это преобразование можно представить следующим образом:

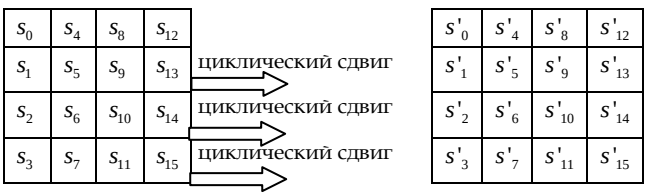

Рис.2. Преобразования ShiftRows()

В преобразовании MixColumns() столбцы массива рассматриваются в качестве многочлена над $GF(2^8)$ и умножаются по модулю x^4+1 на многочлен $g(x)=\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$. Это может быт представлено следующим образом:

$$\begin{bmatrix} p_{4i} \\ p_{4i+1} \\ p_{4i+2} \\ p_{4i+3} \end{bmatrix} = \begin{bmatrix} 02\,03\,01\,01 \\ 01\,02\,03\,01 \\ 01\,01\,02\,03 \\ 03\,01\,01\,02 \end{bmatrix} \begin{bmatrix} s'_{4i} \\ s'_{4i+1} \\ s'_{4i+2} \\ s'_{4i+3} \end{bmatrix}, i=\overline{0...3}.$$

Значение p_i, $i=\overline{0...15}$ вычисляется следующим образом:

$$y_{4i}=(\{02\}\bullet s'_{4i})\oplus(\{03\}\bullet s'_{4i+1})\oplus s'_{4i+2}\oplus s'_{4i+3},$$
$$y_{4i+1}=s'_{4i}\oplus(\{02\}\bullet s'_{4i+1})\oplus(\{03\}\bullet s'_{4i+2})\oplus s'_{4i+3},$$
$$y_{4i+2}=s'_{4i}\oplus s'_{4i+1}\oplus(\{02\}\bullet s'_{4i+2})\oplus(\{03\}\bullet s'_{4i+3}),$$
$$y_{4i+4}=(\{03\}\bullet s'_{4i})\oplus s'_{4i+1}\oplus s'_{4i+2}\oplus(\{02\}\bullet s'_{4i+3}).$$

Преобразование MixColumns() представляется следующим образом:

Рис. 3. Преобразования MixColumns()

В преобразовании AddRoundKey() элементы массива сложатся по XOR с элементами массива ключа, т.е. $p'_i=p_i\oplus k_i$. Это преобразование представляется следующим образом:

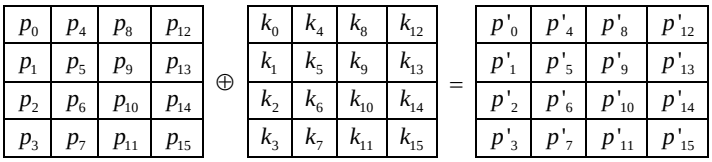

Рис. 4. Преобразования AddRoundKey()

Описание сети IDEA32–4 и RFWKIDEA32–4 приведено в статье [3, 4] и аналогично как у сети Фейстеля, при зашифровании и расшифровании используется один и тот же алгоритм. В сети применена одна раундовая функция, имеющая четыре входных и выходных блоков и в качестве раундовой функции можно использовать любые преобразования.

Используя раундовую функцию ГОСТ 28147–89 [2] в качестве раундовой функции сети IDEA4–2 [1], RFWKIDEA4–2 [5], RFWKPES4–2 [6] разработаны алгоритмы шифрования GOST28147–89–IDEA4–2 [7], GOST28147–89–RFWKIDEA4–2 [16], GOST28147–89–RFWKPES4–2 [17]. Кроме этого, использую преобразования SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() алгоритма шифрования AES в качестве раундовую функцию сети IDEA8–1 [8], RFWKIDEA8–1 [8], PES8–1 [9], RFWKPES8–1 [10], IDEA16–1 [11], PES32–1 [12] и RFWKPES32–1 [13] разработаны алгоритмы шифрования AES–IDEA8–1 [18], AES–RFWKIDEA8–1 [19], AES–PES8–1 [20], AES–RFWKPES8–1 [21], AES–IDEA16–1 [22], AES–PES32–1 [23] и AES–RFWKPES32–1 [23].

В этой статье разработан блочный алгоритм шифрования AES–IDEA32–4 и AES–RFWKIDEA32–4 на основе сети IDEA32–4 и RFWKIDEA32–4 с использованием преобразования алгоритма шифрования AES. Длина блока алгоритмов шифрования равна 1024 битам, количество раундов равно 10, 12, 14 и длина ключа является переменной и изменяется от 256 бит до 1024 бит с шагом 128 бит, т.е. длина ключа равна 256, 384, 512, 640, 768, 896 и 1024 битам.

Структура алгоритма шифрования AES–IDEA32–4

В алгоритме шифрования AES–IDEA32–4 в качестве раундовой функции использованы преобразования SubBytes(), ShiftRows(), MixColumns(), AddRoundKey() алгоритма шифрования AES. Схема n–раундового алгоритма шифрования AES–IDEA32–4 приведена на Рис.5 и длина подблоков X^0, X^1, …, X^{31}, длина раундовых ключей $K_{36(i-1)}$, $K_{36(i-1)+1}$, ..., $K_{36(i-1)+31}$, $i=\overline{1...n+1}$, K_{36n+32}, K_{36n+33}, ..., K_{36n+95} равна 32 битам. А длина раундовых ключей $K_{36(i-1)+32}$, $K_{36(i-1)+33}$, $K_{36(i-1)+34}$, $K_{36(i-1)+35}$, $i=\overline{1...n}$ равна 128 битам.

Рассмотрим раундовую функцию алгоритма шифрования AES–IDEA32–4. Сначала 32 битные подблоки T^0, T^1, ..., T^{15} разбиваются на 8 битные подблоки t_0^0, t_1^0, ..., t_{15}^0, t_0^1, t_1^1, ..., t_{15}^1, …, t_0^3, t_1^3, ..., t_{15}^3 следующим образом: $t_i^0=sb_{i \bmod 4}(T^{idiv4})$, $t_i^1=sb_{i \bmod 4}(T^{idiv4+4})$, $t_i^2=sb_{i \bmod 4}(T^{idiv4+8})$, $t_i^3=sb_{i \bmod 4}(T^{idiv4+12})$, $i=\overline{0...15}$. Здесь *div*-целая часть от деления, *mod*-остаток от деления, $sb_0(X)=x_0x_1...x_7$, $sb_1(X)=x_8x_9...x_{15}$, $sb_2(X)=x_{16}x_{17}...x_{23}$, $sb_3(X)=x_{24}x_{25}...x_{31}$ и $X=x_0x_1...x_{31}$.

В качестве элементов массива State первой раундовой функции выбраны t_0^0, t_1^0, ..., t_{15}^0, второй раундовой функции выбраны t_0^1, t_1^1, ..., t_{15}^1 и четвертой раундовой функции выбраны t_0^3, t_1^3, ..., t_{15}^3.

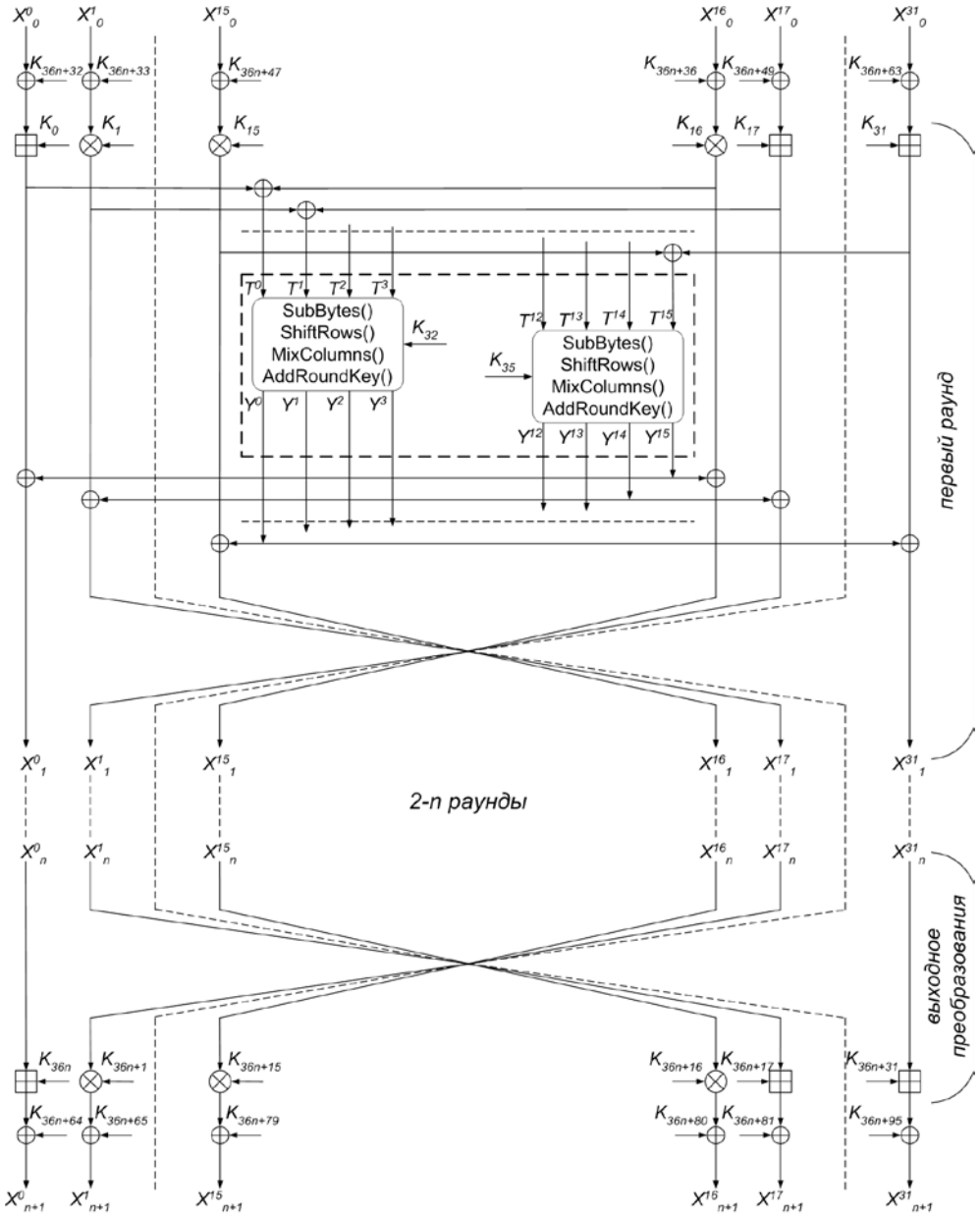

Рис. 5. Структура *n*–раундового алгоритма шифрования AES–IDEA32–4

После чего выполняются преобразования SubBytes(), ShiftRows(), MixColumns(), AddRoundKey(). В преобразовании AddRoundKey() 128 битные ключи разбиваются на 32 битные ключи, т.е. $K^j_{36(i-1)+32}$, $K^j_{36(i-1)+33}$, $K^j_{36(i-1)+34}$, $K^j_{36(i-1)+35}$, $j=\overline{0...3}$. Здесь $K_{36(i-1)+32}=K^0_{36(i-1)+32}\,||\,K^1_{36(i-1)+32}\,||\,K^2_{36(i-1)+32}\,||\,K^3_{36(i-1)+32}$, $K_{36(i-1)+33}=K^0_{36(i-1)+33}\,||\,K^1_{36(i-1)+33}\,||\,K^2_{36(i-1)+33}\,||\,K^3_{36(i-1)+33}$, $K_{36(i-1)+34}=K^0_{36(i-1)+34}\,||\,K^1_{36(i-1)+34}\,||\,K^2_{36(i-1)+34}\,||\,K^3_{36(i-1)+34}$, $K_{36(i-1)+35}=K^0_{36(i-1)+35}\,||\,K^1_{36(i-1)+35}\,||\,K^2_{36(i-1)+35}\,||\,K^3_{36(i-1)+35}$.

Элементы массива ключей k^0_0, k^0_1, …, k^0_{15} первой раундовой функции, k^1_0, k^1_1, …, k^1_{15} второй раундовой функции и k^3_0, k^3_1, …, k^3_{15} четвертой раундовой функции вычисляются следующим образом: $k^0_i=sb_{i \bmod 4}(K^{i\,div\,4}_{36(i-1)+32})$, $k^1_i=sb_{i \bmod 4}(K^{i\,div\,4}_{36(i-1)+33})$, $k^2_i=sb_{i \bmod 4}(K^{i\,div\,4}_{36(i-1)+34})$, $k^3_i=sb_{i \bmod 4}(K^{i\,div\,4}_{36(i-1)+35})$, $i=\overline{0...15}$. После преобразования AddRoundKey() 8 битовые выходные значения объединятся и получется шестнадцать 32 битных подблока Y^0, Y^1, ..., Y^{15}. Здесь Y^0, Y^1, Y^2, Y^3 –выходное значение от первой раундовой функции, Y^4, Y^5, Y^6, Y^7 –выходное значение от четвертой раундовой функции, Y^{12}, Y^{13}, Y^{14}, Y^{15} –выходное значение от второй раундовой функции и $Y^0=p^0_0'\,||\,p^0_1'\,||\,p^0_2'\,||\,p^0_3'$, $Y^1=p^0_4'\,||\,p^0_5'\,||\,p^0_6'\,||\,p^0_7'$, $Y^2=p^0_8'\,||\,p^0_9'\,||\,p^0_{10}'\,||\,p^0_{11}'$, $Y^3=p^0_{12}'\,||\,p^0_{13}'\,||\,p^0_{14}'\,||\,p^0_{15}'$, $Y^4=p^1_0'\,||\,p^1_1'\,||\,p^1_2'\,||\,p^1_3'$, $Y^5=p^1_4'\,||\,p^1_5'\,||\,p^1_6'\,||\,p^1_7'$, $Y^6=p^1_8'\,||\,p^1_9'\,||\,p^1_{10}'\,||\,p^1_{11}'$, $Y^7=p^1_{12}'\,||\,p^1_{13}'\,||\,p^1_{14}'\,||\,p^1_{15}'$, $Y^8=p^2_0'\,||\,p^2_1'\,||\,p^2_2'\,||\,p^2_3'$, $Y^9=p^2_4'\,||\,p^2_5'\,||\,p^2_6'\,||\,p^2_7'$, $Y^{10}=p^2_8'\,||\,p^2_9'\,||\,p^2_{10}'\,||\,p^2_{11}'$, $Y^{11}=p^2_{12}'\,||\,p^2_{13}'\,||\,p^2_{14}'\,||\,p^2_{15}'$, $Y^{12}=p^3_0'\,||\,p^3_1'\,||\,p^3_2'\,||\,p^3_3'$, $Y^{13}=p^3_4'\,||\,p^3_5'\,||\,p^3_6'\,||\,p^3_7'$, $Y^{14}=p^3_8'\,||\,p^3_9'\,||\,p^3_{10}'\,||\,p^3_{11}'$, $Y^{15}=p^3_{12}'\,||\,p^3_{13}'\,||\,p^3_{14}'\,||\,p^3_{15}'$.

S–блоки преобразования SubBytes() приведены в 1–4–таблице и являются единственным

нелинейным преобразованием. Длина входных и выходных блоков S–блоков равна восьми битам. Первый S–блок применен в первой раундовой функции, второй S–блок применен во второй раундовой функции.

Первый S–блок алгорима шифрования AES–IDEA32–4 Таблица 1

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0xFE	0x90	0x1B	0xA1	0x0C	0x97	0x44	0x12	0x26	0x49	0x2D	0x9B	0xB6	0x86	0x1F	0x5B
0x1	0x4A	0x2F	0xA8	0xD0	0x65	0x1A	0x34	0xAE	0x6E	0x64	0x36	0xCC	0x01	0x47	0x88	0x81
0x2	0x93	0x54	0x59	0x61	0x57	0x7E	0x9F	0x3B	0xF5	0x07	0x0B	0xEE	0x6A	0xDE	0x66	0xAC
0x3	0xDA	0xB0	0xF2	0x63	0x56	0xCA	0x9A	0x70	0x38	0x9D	0x8D	0x3A	0x13	0x21	0x00	0xB9
0x4	0x20	0x6F	0xAA	0xF4	0xB4	0x04	0xF8	0x94	0x91	0xAD	0xC6	0x40	0x39	0x7A	0x48	0x5E
0x5	0xD1	0xF7	0x09	0x62	0x10	0x14	0xE2	0xB8	0xD7	0x0A	0xBA	0x0F	0xCE	0xBF	0x5A	0xD9
0x6	0xB7	0xC0	0x5F	0x25	0xE7	0xFF	0xC4	0x1E	0x96	0x87	0xAB	0x72	0x33	0x9C	0xE3	0xFD
0x7	0x73	0x76	0x05	0xD5	0x19	0x41	0x4F	0x3D	0x18	0xD3	0x7C	0x50	0x3F	0xF6	0x4C	0x15
0x8	0x7B	0xB3	0xDD	0x22	0x6B	0x8A	0xD6	0x0E	0x52	0xA5	0x32	0xDC	0xCF	0xC9	0x16	0xC8
0x9	0x1C	0xCD	0x5D	0x0D	0xB2	0xDB	0xBB	0xE4	0x74	0x80	0xCB	0xEC	0xAF	0x2B	0x82	0x3C
0xA	0x98	0x84	0xED	0xC2	0x2C	0x78	0xC3	0x89	0x23	0x55	0x2E	0xBE	0xFB	0x28	0x4B	0x03
0xB	0xA9	0xE8	0x17	0xE6	0x77	0x24	0x1D	0xBD	0xA6	0x42	0x7D	0x53	0x8F	0xE1	0x8C	0x60
0xC	0x69	0x43	0x83	0x08	0x85	0xE5	0x71	0xF0	0xF1	0x4D	0xF9	0x67	0x8E	0x58	0x06	0x46
0xD	0x2A	0x3E	0x31	0x6D	0x6C	0xEB	0xDF	0x11	0x5C	0xB5	0x02	0x8B	0xFC	0xC1	0xC5	0xA3
0xE	0xD8	0xC7	0xD2	0x7F	0x35	0x9E	0x95	0x68	0x30	0x27	0xBC	0xB1	0x99	0xA0	0x79	0xEF
0xF	0x37	0xD4	0xA4	0xF3	0xFA	0xE9	0xA7	0x75	0x45	0x92	0xEA	0x51	0xA2	0xE0	0x29	0x4E

Второй S–блок алгорима шифрования AES–IDEA32–4 Таблица 2

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0x07	0xDE	0x20	0x1A	0xDD	0x11	0x3D	0x97	0x26	0x18	0x2B	0xD3	0xE7	0xC4	0xB2	0x90
0x1	0x45	0x91	0xAD	0x6E	0xCB	0xC7	0xAE	0x85	0xC6	0x2C	0x14	0x9E	0xF8	0x60	0xBC	0x0B
0x2	0x83	0x0F	0x2A	0x59	0x52	0xF4	0x41	0x31	0x0A	0xD0	0x12	0x35	0x54	0x16	0x96	0x3F
0x3	0x84	0xCF	0xC5	0xE3	0xB5	0xB6	0x34	0x8C	0x6C	0xFB	0xC9	0xD6	0x70	0xE9	0x1F	0x78
0x4	0x0E	0x21	0x17	0xED	0x5D	0x8D	0x2F	0x4C	0x39	0xD8	0x74	0xAF	0x8B	0x66	0xFF	0xE5
0x5	0x89	0xB0	0xA8	0x04	0x2D	0xBF	0xF7	0x9F	0xA1	0xF5	0x25	0x80	0x24	0x50	0x77	0xD9
0x6	0x00	0x5C	0x02	0x7B	0x82	0xE0	0xCE	0x55	0xF6	0x23	0xF0	0x36	0x61	0x1C	0x10	0x5A
0x7	0xD1	0xA4	0x6A	0x1B	0x9A	0x48	0x30	0x19	0x7D	0x33	0x4E	0x9D	0xA3	0x57	0x6D	0x58
0x8	0x81	0x92	0x4B	0xB4	0xB3	0x06	0x46	0x67	0x27	0x88	0x86	0xAC	0xC3	0xEB	0x05	0x0C
0x9	0xEF	0x79	0xB8	0x3A	0x75	0x63	0xC2	0xDF	0x1E	0xEC	0x51	0x8F	0x62	0x03	0x56	0xFE
0xA	0x8E	0x7E	0x68	0xE6	0xCC	0xDC	0x01	0x5B	0x53	0xE8	0x76	0xB7	0x72	0x5E	0xA2	0x42
0xB	0x4A	0x1D	0xE2	0x65	0x43	0x9C	0x08	0xEA	0xD5	0x15	0xA9	0xC0	0x73	0xAA	0x2E	0xBE
0xC	0x09	0xF2	0xB1	0x4F	0x99	0x38	0x6B	0x7F	0x98	0x8A	0xC8	0x71	0x94	0xCD	0x37	0x87
0xD	0xE4	0x44	0xDB	0x9B	0x7C	0x40	0xF1	0xCA	0x5F	0xBA	0xA5	0xE1	0xBD	0xBB	0x29	0xA0
0xE	0x3E	0x93	0xD4	0x13	0x49	0xA6	0xAB	0xEE	0x3C	0xC1	0x0D	0x28	0x69	0xFD	0x3B	0xD2
0xF	0xF3	0xFC	0x6F	0x22	0x95	0xFA	0x32	0xF9	0xDA	0x64	0xA7	0x7A	0x47	0x4D	0xB9	0xD7

Третий S–блок алгорима шифрования AES–IDEA32–4 Таблица 3

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0xE0	0x86	0x57	0x8E	0xB1	0x94	0x39	0xAC	0x78	0x97	0x4D	0xB3	0x68	0xE9	0x02	0xAD
0x1	0xD0	0x83	0x75	0x7C	0xC5	0xDE	0x42	0xEE	0xF0	0x4C	0x8C	0xAF	0x1F	0x7E	0x00	0xFB
0x2	0xC1	0xCD	0x63	0x90	0x8A	0x04	0xE6	0x22	0xD5	0x84	0xA3	0x14	0xA5	0x95	0x82	0x20
0x3	0xC0	0xF3	0xC7	0x5E	0x03	0x34	0x3A	0xED	0x65	0x28	0xDC	0xAB	0x25	0x6A	0x96	0x08
0x4	0xE3	0x79	0xBB	0x5C	0xA6	0xC3	0x7B	0xD3	0x0F	0xA9	0x13	0x6C	0xEC	0x51	0x1E	0x71
0x5	0xF5	0x1B	0x6D	0xD7	0x62	0x37	0x33	0x81	0x6E	0x2A	0x4F	0xF6	0x61	0x93	0x24	0x87
0x6	0xE1	0x88	0xF8	0x3F	0xEF	0x69	0xDD	0x8B	0x1D	0x60	0x32	0x23	0x50	0xA1	0xBA	0xA7
0x7	0xAA	0x76	0x4A	0xA0	0x99	0xE5	0x0C	0xB9	0x10	0x3B	0xCA	0x98	0x77	0x92	0x4B	0xBE
0x8	0xD8	0xB4	0xD2	0x2D	0x2C	0xCE	0xE7	0x7F	0x56	0xDB	0xD9	0x5B	0xE8	0x73	0xF9	0xFA
0x9	0x45	0x26	0x36	0x38	0x3D	0x49	0xC6	0xA8	0xB8	0x72	0xBD	0xDA	0x67	0xD6	0xBC	0x30
0xA	0xF4	0x27	0x53	0x46	0xC4	0x9F	0xCF	0x89	0xA4	0x44	0x0A	0x1A	0x3C	0x91	0x59	0xD1
0xB	0xFC	0x8F	0x70	0x66	0xFF	0xB6	0xCC	0x5D	0x9C	0xA2	0x43	0xDF	0x12	0x74	0x55	0x19
0xC	0xE2	0x2B	0x35	0xE4	0xAE	0x21	0x64	0x09	0x80	0xC2	0xF2	0x0B	0x9B	0xEA	0x0D	0xF7
0xD	0x5F	0xFE	0x9E	0xB7	0x3E	0xC8	0x1C	0xEB	0xBF	0x2F	0x58	0x47	0x2E	0x01	0x54	0x40
0xE	0x0E	0x9A	0xB2	0x8D	0xCB	0x6F	0x5A	0x6B	0x17	0xF1	0xD4	0x7A	0x7D	0x07	0x16	0x9D
0xF	0x05	0x29	0x52	0x4E	0xB5	0x06	0x15	0x31	0xB0	0x48	0x41	0x11	0xC9	0xFD	0x18	0x85

Четвертый S–блок алгорима шифрования AES–IDEA32–4 Таблица 4

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0	0x7F	0xE1	0xA8	0xCD	0x3A	0xA3	0x1A	0x4F	0x1F	0xA0	0xC6	0x38	0x5F	0x52	0xF5	0x4E
0x1	0xBF	0xF8	0x2A	0x07	0xE6	0x89	0xF1	0x49	0x3F	0xC7	0xCF	0x4C	0x80	0x05	0xF7	0x10
0x2	0xFE	0xCA	0x70	0xBB	0xD5	0xEF	0x65	0x75	0xA6	0xE3	0x78	0xAF	0x62	0xA2	0xF9	0x77
0x3	0xFF	0x3C	0xE4	0x85	0xF4	0x2F	0x19	0x4A	0x6A	0x5B	0x8B	0x54	0x6E	0x5D	0xA1	0xDB
0x4	0x7C	0x1E	0x14	0x87	0x61	0xFC	0x1C	0xBC	0xC0	0x56	0xB4	0x47	0x4B	0xB2	0x81	0x32

Окончание таблицы 4

0x5	0x26	0x98	0x46	0xA4	0x71	0x2C	0x34	0xFA	0x45	0x59	0xC4	0x25	0x72	0xB8	0x6F	0xE0
0x6	0x7E	0xD7	0x13	0x00	0x48	0x5E	0x8A	0xD4	0x82	0x73	0x35	0x74	0xB3	0x7A	0x15	0x60
0x7	0x55	0x29	0xDD	0x7B	0x96	0x66	0xC3	0x16	0xB7	0x18	0xD1	0x97	0x28	0xB9	0xDC	0x0D
0x8	0x93	0x23	0xBD	0x42	0x43	0xC9	0x64	0x04	0xA9	0x90	0x92	0x9C	0x53	0x30	0x12	0x11
0x9	0xEA	0x6D	0x2D	0x1B	0x02	0xDE	0xE5	0x57	0x17	0x31	0x0E	0x91	0x68	0xA5	0x0F	0x37
0xA	0x27	0x6C	0xB0	0xE9	0xE7	0x8C	0xC8	0xD6	0x63	0xEB	0xD9	0x99	0x03	0xBA	0x9E	0xBE
0xB	0x0B	0xCC	0x33	0x69	0x08	0x21	0xCB	0x86	0x8F	0x79	0xF0	0x88	0xB5	0x2B	0xAA	0x9A
0xC	0x7D	0x58	0x2E	0x67	0x4D	0x76	0x6B	0xDA	0xFB	0xFD	0x3D	0xD8	0x94	0x51	0xC2	0x24
0xD	0x84	0x09	0x8D	0x20	0x01	0xD3	0x83	0x50	0x0C	0x40	0x9F	0xE8	0x41	0xF6	0xAB	0xF3
0xE	0xC1	0x95	0x39	0xCE	0xD0	0x44	0x9D	0x5C	0xAC	0x3E	0xA7	0x1D	0x06	0xEC	0xAD	0x8E
0xF	0xEE	0x5A	0xB1	0xC5	0x22	0xED	0xAE	0x36	0x3B	0xDF	0xF2	0xB6	0xD2	0x0A	0x9B	0xE2

Рассмотрим процесс шифрования в алгоритме AES–IDEA32–4. Сначала 1024 битный блок открытого текста X разбивается на 32 битные подблоки X_0^0, X_0^1, …, X_0^{31} и выполняются следующие шаги:

1) Подблоки X_0^0, X_0^1, …, X_0^{31} суммируются по XOR с соответствующими раундовыми ключами K_{36n+32}, K_{36n+33}, ..., K_{36n+63}: $X_0^i = X_0^i \oplus K_{36n+32+i}$, $i = \overline{0...31}$.

2) Подблоки X_0^0, X_0^1, …, X_0^{31} умножаются и суммируются с соответствующими раундовыми ключами $K_{36(i-1)}$, $K_{36(i-1)+1}$, ..., $K_{36(i-1)+31}$ и вычисляются T^0, T^1, ..., T^{15} следующим образом:

$T^j = (X_{i-1}^j + K_{36(i-1)+j}) \oplus (X_{i-1}^{16+j} \cdot K_{36(i-1)+16+j})$, при j=0, 2, 4, 6, 8, 10, 12, 14 и $T^j = (X_{i-1}^j \cdot K_{36(i-1)+j}) \oplus (X_{i-1}^{16+j} + K_{36(i-1)+16+j})$, при j=1, 3, 5, 7, 9, 11, 13, 15, $i = 1$.

3) Подблоки T^0, T^1, ..., T^{15} записываются в четырех массивах State и выполняются преобразования SubBytes(), ShiftRows(), MixColumns(), AddRoundKey(). После преобразования получатся 32 битные подблоки Y^0, Y^1, ..., Y^{15}.

4) Подблоки Y^0, Y^1, ..., Y^{15} суммируются по XOR с соответствующими подблоками X_{i-1}^j, т.е. $X_{i-1}^j = X_{i-1}^j \oplus Y_{15-j}$, $X_{i-1}^{j+16} = X_{i-1}^{j+16} \oplus Y_{7-j}$, $j = \overline{0...15}$, $i = 1$.

5) В конце раунда кроме подблоков X_i^0 и X_{i-1}^{31} все подблоки поменяются местами, $X_i^j = X_{i-1}^{15+j}$, $X_i^{j+15} = X_{i-1}^j$ $j = \overline{1...15}$, $i = 1$.

6) Повторяя шаги 2–5 n раз, т.е. $i = \overline{2...n}$, получим 32 битные подблоки X_n^0, X_n^1, …, X_n^{31}.

7) В выходном преобразовании раундовые ключи K_{36n}, K_{36n+1}, ..., K_{36n+31} умножаются и суммируются с соответствующими подблоками, т.е.

$X_{n+1}^0 = X_n^0 + K_{36n}$, $X_{n+1}^{31} = X_n^{31} + K_{36n+31}$, $X_{n+1}^j = X_n^{31-j} \cdot K_{36n+j}$, при j=1, 3, 5, 7, 9, 11, 13, 15, 16, 18, 20, 22, 24, 26, 28, 30 и $X_{n+1}^j = X_n^{31-j} + K_{36n+j}$, при j=2, 4, 6, 8, 10, 12, 14, 17, 19, 21, 23, 25, 27, 29.

8) Подблоки X_{n+1}^0, X_{n+1}^1, …, X_{n+1}^{31} суммируются по XOR с соответствующими раундовыми ключами K_{36n+64}, K_{36n+65}, ..., K_{36n+95}: $X_{n+1}^j = X_{n+1}^j \oplus K_{36n+64+j}$, $j = \overline{0...31}$. В качестве шифртекста открытого текста X принимается объединение 32 битных подблоков $X_{n+1}^0 \| X_{n+1}^1 \| ... \| X_{n+1}^{31}$.

Генерация ключей алгоритма шифрования AES–IDEA32–4

В n–раундовом алгоритме шифрования AES–IDEA32–4 в каждом раунде применяются 32 раундовые ключи длиной по 32 бита, четыре ключа длиной 128 битаи в выходном преобразовании 32 раундовые ключи длиной 32 бит. Кроме этого, до первого раунда и после выходного преобразования применяются 32 раундовые ключи длиной 32 бит. Общее число 32 битных раундовых ключей равно 32n+96 и 128 битных раундовых ключей равно 16n. Если 128 битные раундовые ключи преобразовать в четыре 32 битных ключа, то общее число 32 битных ключей равно 48n+96. При зашифровании на Рис.5, вместо K_i используются раундовые ключи зашифрования K_i^c, при расшифровании раундовые ключи расшифрования K_i^d.

При генерации раундовых ключей как у алгоритма шифрования AES используется массив Rcon: Rcon=[0x00000001, 0x00000002, 0x00000004, 0x00000008, 0x00000010, 0x00000020, 0x00000040, 0x00000080, 0x00000100, 0x00000200, 0x00000400, 0x00000800, 0x00001000, 0x00002000, 0x00004000, 0x00008000, 0x00010000, 0x00020000, 0x00040000, 0x00080000, 0x00100000, 0x00200000, 0x00400000, 0x00800000, 0x01000000, 0x02000000, 0x04000000, 0x08000000, 0x10000000, 0x20000000, 0x40000000, 0x80000000].

Ключ алгоритма шифрования K длиной l ($256 \le l \le 1024$) бит разбивается на 32 битовые раундовые ключи $K_0^{c'}$, $K_1^{c'}$,..., $K_{Lenght-1}^{c'}$, $Lenght = l/32$, здесь $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^{c'} = \{k_0, k_1, ..., k_{31}\}$, $K_1^{c'} = \{k_{32}, k_{33}, ..., k_{63}\}$,..., $K_{Lenght-1}^{c'} = \{k_{l-32}, k_{l-31}, ..., k_{l-1}\}$ и $K = K_0^{c'} \| K_1^{c'} \| ... \| K_{Lenght-1}^{c'}$. После чего вычисляется $K_L = K_0^{c'} \oplus K_1^{c'} \oplus ... \oplus K_{Lenght-1}^{c'}$. Если $K_L = 0$ тогда в качестве K_L выбирается 0xC5C31537, т.е. $K_L = 0$xC5C31537. При генерации раундовых ключей $K_i^{c'}$, $i = \overline{Lenght...48n+95}$ используются преобразования *SubBytes32()* и *RotWord32()*, здесь *SubBytes32()*–преобразование 32 битного подблока в S–блоке, т.е. $SubBytes32(X) = S_0(sb_0(X)) \| S_1(sb_1(X)) \| S_2(sb_2(X)) \| S_3(sb_3(X))$, *RotWord32()*– циклический сдвиг 32 битового подблока налево на 1 бит. Здесь S_0, S_1, S_2 и S_3 – S–блоки, приведенные в 1 - 4–таблице. Если

выполняются условия $i \bmod 3 = 1$, тогда раундовые ключи вычисляются как

$K_i^{c'} = SubBytes32(K_{i-Lenght+1}^{c'}) \oplus SubBytes32(RotWord32(K_{i-Lenght}^{c'}))$

$\oplus Rcon[i \bmod 32] \wedge K_L$, иначе

$K_i^{c'} = SubBytes32(K_{i-Lenght}^{c'}) \oplus SubBytes32(K_{i-Lenght+1}^{c'}) \wedge K_L$.

После каждой генерации раундовых ключей значение K_L циклически сдвигается влево на 1 бит.

Раундовые ключи расшифрования вычисляются на основе раундовых ключей зашифрования и ключи расшифрования выходного преобразования связаны с ключами зашифрования следующим образом:

$$(K_{48n}^{d'}, K_{48n+1}^{d'}, K_{48n+2}^{d'}, K_{48n+3}^{d'}, K_{48n+4}^{d'}, K_{48n+5}^{d'}, K_{48n+6}^{d'}, K_{48n+7}^{d'},$$
$$K_{48n+8}^{d'}, K_{48n+9}^{d'}, K_{48n+10}^{d'}, K_{48n+11}^{d'}, K_{48n+12}^{d'}, K_{48n+13}^{d'}, K_{48n+14}^{d'},$$
$$K_{48n+15}^{d'}, K_{48n+16}^{d'}, K_{48n+17}^{d'}, K_{48n+18}^{d'}, K_{48n+19}^{d'}, K_{48n+20}^{d'}, K_{48n+21}^{d'},$$
$$K_{48n+22}^{d'}, K_{48n+23}^{d'}, K_{48n+24}^{d'}, K_{48n+25}^{d'}, K_{48n+26}^{d'}, K_{48n+27}^{d'}, K_{48n+28}^{d'},$$
$$K_{48n+29}^{d'}, K_{48n+30}^{d'}, K_{48n+31}^{d'}) = (-K_0^{c'}, (K_1^{c'})^{-1}, -K_2^{c'}, (K_3^{c'})^{-1},$$
$$-K_4^{c'}, (K_5^{c'})^{-1}, -K_6^{c'}, (K_7^{c'})^{-1}, -K_8^{c'}, (K_9^{c'})^{-1}, -K_{10}^{c'}, (K_{11}^{c'})^{-1},$$
$$-K_{12}^{c'}, (K_{13}^{c'})^{-1}, -K_{14}^{c'}, (K_{15}^{c'})^{-1}, (K_{16}^{c'})^{-1}, -K_{17}^{c'}, (K_{18}^{c'})^{-1}, -K_{19}^{c'},$$
$$(K_{20}^{c'})^{-1}, -K_{21}^{c'}, (K_{22}^{c'})^{-1}, -K_{23}^{c'}, (K_{24}^{c'})^{-1}, -K_{25}^{c'}, (K_{26}^{c'})^{-1}, -K_{27}^{c'},$$
$$(K_{28}^{c'})^{-1}, -K_{29}^{c'}, (K_{30}^{c'})^{-1}, -K_{31}^{c'}).$$

При n=10 формула выглядит следующим образом:

$$(K_{480}^{d'}, K_{481}^{d'}, K_{482}^{d'}, K_{483}^{d'}, K_{484}^{d'}, K_{485}^{d'}, K_{486}^{d'}, K_{487}^{d'}, K_{488}^{d'}, K_{489}^{d'},$$
$$K_{490}^{d'}, K_{491}^{d'}, K_{492}^{d'}, K_{493}^{d'}, K_{484}^{d'}, K_{495}^{d'}, K_{496}^{d'}, K_{497}^{d'}, K_{498}^{d'}, K_{499}^{d'},$$
$$K_{500}^{d'}, K_{501}^{d'}, K_{502}^{d'}, K_{503}^{d'}, K_{504}^{d'}, K_{505}^{d'}, K_{506}^{d'}, K_{507}^{d'}, K_{508}^{d'}, K_{509}^{d'},$$
$$K_{510}^{d'}, K_{511}^{d'}) = (-K_0^{c'}, (K_1^{c'})^{-1}, -K_2^{c'}, (K_3^{c'})^{-1}, -K_4^{c'}, (K_5^{c'})^{-1},$$
$$-K_6^{c'}, (K_7^{c'})^{-1}, -K_8^{c'}, (K_9^{c'})^{-1}, -K_{10}^{c'}, (K_{11}^{c'})^{-1}, -K_{12}^{c'}, (K_{13}^{c'})^{-1},$$
$$-K_{14}^{c'}, (K_{15}^{c'})^{-1}, (K_{16}^{c'})^{-1}, -K_{17}^{c'}, (K_{18}^{c'})^{-1}, -K_{19}^{c'}, (K_{20}^{c'})^{-1},$$
$$-K_{21}^{c'}, (K_{22}^{c'})^{-1}, -K_{23}^{c'}, (K_{24}^{c'})^{-1}, -K_{25}^{c'}, (K_{26}^{c'})^{-1}, -K_{27}^{c'},$$
$$(K_{28}^{c'})^{-1}, -K_{29}^{c'}, (K_{30}^{c'})^{-1}, -K_{31}^{c'}).$$

Таким же образом, ключи расшифрования второго, третьего и n–раунда связаны с ключами зашифрования следующим образом:

$$(K_{48(i-1)}^{d'}, K_{48(i-1)+1}^{d'}, K_{48(i-1)+2}^{d'}, K_{48(i-1)+3}^{d'}, K_{48(i-1)+4}^{d'}, K_{48(i-1)+5}^{d'}, K_{48(i-1)+6}^{d'},$$
$$K_{48(i-1)+7}^{d'}, K_{48(i-1)+8}^{d'}, K_{48(i-1)+9}^{d'}, K_{48(i-1)+10}^{d'}, K_{48(i-1)+11}^{d'}, K_{48(i-1)+12}^{d'},$$
$$K_{48(i-1)+13}^{d'}, K_{48(i-1)+14}^{d'}, K_{48(i-1)+15}^{d'}, K_{48(i-1)+16}^{d'}, K_{48(i-1)+17}^{d'}, K_{48(i-1)+18}^{d'},$$
$$K_{48(i-1)+19}^{d'}, K_{48(i-1)+20}^{d'}, K_{48(i-1)+21}^{d'}, K_{48(i-1)+22}^{d'}, K_{48(i-1)+23}^{d'}, K_{48(i-1)+24}^{d'},$$
$$K_{48(i-1)+25}^{d'}, K_{48(i-1)+26}^{d'}, K_{48(i-1)+27}^{d'}, K_{48(i-1)+28}^{d'}, K_{48(i-1)+29}^{d'}, K_{48(i-1)+30}^{d'},$$
$$K_{48(i-1)+31}^{d'}) = (-K_{48(n-i+1)}^{c'}, (K_{24(n-i+1)+30}^{c'})^{-1}, -K_{48(n-i+1)+29}^{c'},$$
$$(K_{48(n-i+1)+28}^{c'})^{-1}, -K_{48(n-i+1)+27}^{c'}, (K_{48(n-i+1)+26}^{c'})^{-1}, -K_{48(n-i+1)+25}^{c'},$$
$$(K_{48(n-i+1)+24}^{c'})^{-1}, -K_{48(n-i+1)+23}^{c'}, (K_{48(n-i+1)+22}^{c'})^{-1}, -K_{48(n-i+1)+21}^{c'},$$
$$(K_{48(n-i+1)+20}^{c'})^{-1}, -K_{48(n-i+1)+19}^{c'}, (K_{48(n-i+1)+18}^{c'})^{-1}, -K_{48(n-i+1)+17}^{c'},$$
$$(K_{48(n-i+1)+16}^{c'})^{-1}, (K_{48(n-i+1)+15}^{c'})^{-1}, -K_{48(n-i+1)+14}^{c'}, (K_{48(n-i+1)+13}^{c'})^{-1},$$
$$-K_{48(n-i+1)+12}^{c'}, (K_{48(n-i+1)+11}^{c'})^{-1}, -K_{48(n-i+1)+10}^{c'}, (K_{48(n-i+1)+9}^{c'})^{-1},$$
$$-K_{48(n-i+1)+8}^{c'}, (K_{48(n-i+1)+7}^{c'})^{-1}, -K_{48(n-i+1)+6}^{c'}, (K_{48(n-i+1)+5}^{c'})^{-1},$$
$$-K_{48(n-i+1)+4}^{c'}, (K_{48(n-i+1)+3}^{c'})^{-1}, -K_{48(n-i+1)+2}^{c'}, (K_{48(n-i+1)+1}^{c'})^{-1},$$
$$-K_{48(n-i+1)+31}^{c'}), i = \overline{2...n}.$$

$$K_{48(i-1)+32+j}^{d'} = K_{48(n-i)+32+j}^{c'},\ j = \overline{0...15},\ i = \overline{2...n}.$$

Раундовые ключи расшифрования первого раунда связаны к раундовым ключам зашифрования следующим образом:

$$(K_0^{d'}, K_1^{d'}, K_2^{d'}, K_3^{d'}, K_4^{d'}, K_5^{d'}, K_6^{d'}, K_7^{d'}, K_8^{d'}, K_9^{d'}, K_{10}^{d'}, K_{11}^{d'},$$
$$K_{12}^{d'}, K_{13}^{d'}, K_{14}^{d'}, K_{15}^{d'}, K_{16}^{d'}, K_{17}^{d'}, K_{18}^{d'}, K_{191}^{d'}, K_{20}^{d'}, K_{21}^{d'}, K_{22}^{d'}, K_{23}^{d'},$$
$$K_{24}^{d'}, K_{25}^{d'}, K_{26}^{d'}, K_{27}^{d'}, K_{28}^{d'}, K_{28}^{d'}, K_{29}^{d'}, K_{30}^{d'}, K_{31}^{d'}, K_{32}^{d'}, K_{33}^{d'}, K_{34}^{d'},$$
$$K_{35}^{d'}, K_{36}^{d'}, K_{37}^{d'}, K_{38}^{d'}, K_{38}^{d'}, K_{39}^{d'}, K_{40}^{d'}, K_{41}^{d'}, K_{42}^{d'}, K_{43}^{d'}, K_{44}^{d'}, K_{45}^{d'},$$
$$K_{46}^{d'}, K_{47}^{d'}) = (-K_{48n}^{c'}, (K_{48n+1}^{c'})^{-1}, -K_{48n+2}^{c'}, (K_{48n+3}^{c'})^{-1}, -K_{48n+4}^{c'},$$
$$(K_{48n+5}^{c'})^{-1}, -K_{48n+6}^{c'}, (K_{48n+7}^{c'})^{-1}, -K_{48n+8}^{c'}, (K_{48n+9}^{c'})^{-1}, -K_{48n+10}^{c'},$$
$$(K_{48n+11}^{c'})^{-1}, -K_{48n+12}^{c'}, (K_{48n+13}^{c'})^{-1}, -K_{48n+14}^{c'}, (K_{48n+15}^{c'})^{-1},$$
$$(K_{48n+16}^{c'})^{-1}, -K_{48n+17}^{c'}, (K_{48n+18}^{c'})^{-1}, -K_{48n+19}^{c'}, (K_{48n+20}^{c'})^{-1},$$
$$-K_{48n+21}^{c'}, (K_{48n+22}^{c'})^{-1}, -K_{48n+23}^{c'}, (K_{48n+24}^{c'})^{-1}, -K_{48n+25}^{c'},$$
$$(K_{48n+26}^{c'})^{-1}, -K_{48n+27}^{c'}, (K_{48n+28}^{c'})^{-1}, -K_{48n+29}^{c'}, (K_{48n+30}^{c'})^{-1},$$
$$-K_{48n+31}^{c'}, K_{48(n-1)+32}^{c'}, K_{48(n-1)+33}^{c'}, K_{48(n-1)+34}^{c'}, K_{48(n-1)+35}^{c'},$$
$$K_{48(n-1)+36}^{c'}, K_{48(n-1)+37}^{c'}, K_{48(n-1)+38}^{c'}, K_{48(n-1)+39}^{c'}, K_{48(n-1)+40}^{c'},$$
$$K_{48(n-1)+41}^{c'}, K_{48(n-1)+42}^{c'}, K_{48(n-1)+43}^{c'}, K_{48(n-1)+44}^{c'}, K_{48(n-1)+45}^{c'},$$
$$K_{48(n-1)+46}^{c'}, K_{48(n-1)+47}^{c'}).$$

Раундовые ключи расшифрования, примененные до первого раунда и после выходного преобразования связаны с ключами зашифрования следующим образом: $K_{48n+32+j}^{d'} = K_{48n+64+j}^{c'}$, $K_{48n+64+j}^{d'} = K_{48n+32+j}^{c'}$, $j = \overline{0...31}$.

Раундовые ключи зашифрования K_i^c связаны с ключами $K_i^{c'}$ следующим образом: $K_{36i+j}^c = K_{48i+j}^{c'}$, $j = \overline{0...31}$, $K_{36i+32}^c = K_{48i+32}^{c'} \| K_{48i+33}^{c'} \| K_{48i+34}^{c'} \| K_{48i+35}^{c'}$, $K_{36i+33}^c = K_{48i+36}^{c'} \| K_{48i+37}^{c'} \| K_{48i+38}^{c'} \| K_{48i+39}^{c'}$, $K_{36i+34}^c = K_{48i+40}^{c'} \| K_{48i+41}^{c'} \| K_{48i+42}^{c'} \| K_{48i+43}^{c'}$, $K_{36i+35}^c = K_{48i+44}^{c'} \| K_{48i+45}^{c'} \| K_{48i+46}^{c'} \| K_{48i+47}^{c'}$. Таким же образом, раундовые ключи расшифрования K_i^d связаны с ключами $K_i^{d'}$ следующим образом:

$$K_{36i+j}^d = K_{48i+j}^{d'}, \ j = \overline{0...31},$$
$$K_{36i+32}^d = K_{48i+32}^{d'} \| K_{48i+33}^{d'} \| K_{48i+34}^{d'} \| K_{48i+35}^{d'},$$
$$K_{36i+33}^d = K_{48i+36}^{d'} \| K_{48i+37}^{d'} \| K_{48i+38}^{d'} \| K_{48i+39}^{d'},$$
$$K_{36i+34}^d = K_{48i+40}^{d'} \| K_{48i+41}^{d'} \| K_{48i+42}^{d'} \| K_{48i+43}^{d'},$$
$$K_{36i+35}^d = K_{48i+44}^{d'} \| K_{48i+45}^{d'} \| K_{48i+46}^{d'} \| K_{48i+47}^{d'}.$$

Структура алгоритма шифрования AES–RFWKIDEA32–4.

Схема *n*–раундового алгоритма шифрования AES–RFWKIDEA32–4 приведена на Рис.6 и длина подблоков X^0, X^1, …, X^{31}, длина раундовых ключей $K_{32(i-1)}$, $K_{32(i-1)+1}$, ..., $K_{32(i-1)+31}$, $i = \overline{1...n+1}$, K_{32n+32}, K_{32n+33}, ..., K_{32n+95} равны 32 битам.

В отличие от алгоритма шифрования AES–IDEA32–4 в алгоритме шифрования AES–RFWKIDEA32–4 в качестве раундовой функции использованы преобразования SubBytes(), ShiftRows(), MixColumns() алгоритма шифрования AES. Как у алгоритма шифрования AES–IDEA32–4, в алгоритме AES–RFWKIDEA32–4 32 битные подблоки T^0, T^1, ..., T^{31} разбиваются на 8 битные подблоки t_0^0, t_1^0, ..., t_{15}^0, t_0^1, t_1^1, ..., t_{15}^1, …, t_0^3, t_1^3, ..., t_{15}^3. После чего выполняются преобразования SubBytes(), ShiftRows(), MixColumns(). После преобразования MixColumns() получается 32 битные подблоки Y^0, Y^1, ..., Y^{31}. Здесь

$Y^0 = p_0^0 \| p_1^0 \| p_2^0 \| p_3^0$, $Y^1 = p_4^0 \| p_5^0 \| p_6^0 \| p_7^0$,
$Y^2 = p_8^0 \| p_9^0 \| p_{10}^0 \| p_{11}^0$, $Y^3 = p_{12}^0 \| p_{13}^0 \| p_{14}^0 \| p_{15}^0$,
$Y^4 = p_0^1 \| p_1^1 \| p_2^1 \| p_3^1$, $Y^5 = p_4^1 \| p_5^1 \| p_6^1 \| p_7^1$,
$Y^6 = p_8^1 \| p_9^1 \| p_{10}^1 \| p_{11}^1$, $Y^7 = p_{12}^1 \| p_{13}^1 \| p_{14}^1 \| p_{15}^1$,
$Y^8 = p_0^2 \| p_1^2 \| p_2^2 \| p_3^2$, $Y^9 = p_4^2 \| p_5^2 \| p_6^2 \| p_7^2$,
$Y^{10} = p_8^2 \| p_9^2 \| p_{10}^2 \| p_{11}^2$, $Y^{11} = p_{12}^2 \| p_{13}^2 \| p_{14}^2 \| p_{15}^2$,
$Y^{12} = p_0^3 \| p_1^3 \| p_2^3 \| p_3^3$, $Y^{13} = p_4^3 \| p_5^3 \| p_6^3 \| p_7^3$,
$Y^{14} = p_8^3 \| p_9^3 \| p_{10}^3 \| p_{11}^3$, $Y^{15} = p_{12}^3 \| p_{13}^3 \| p_{14}^3 \| p_{15}^3$.

В качестве S–блоков преобразования SubBytes() взяты S–блоки преобразования SubBytes() алгоритма шифрования AES–IDEA32–4.

Рассмотрим процесс шифрования в алгоритме AES–RFWKIDEA32–4. Сначала 1024 битный блок открытого текста X разбивается на 32 битные подблоки X_0^0, X_0^1, …, X_0^{31} и выполняются следующие шаги:

1) Подблоки X_0^0, X_0^1, …, X_0^{31} суммируются по XOR с соответствующими раундовыми ключами K_{32n+32}, K_{32n+33}, ..., K_{32n+63}: $X_0^i = X_0^i \oplus K_{32n+32+i}$, $i = \overline{0...31}$.

2) Подблоки X_0^0, X_0^1, …, X_0^{31} умножаются и суммируются с соответствующими раундовыми ключами $K_{32(i-1)}$, $K_{32(i-1)+1}$, ..., $K_{32(i-1)+31}$ и вычисляются T^0, T^1, ..., T^{31} следующим образом:

$T^j = (X_{i-1}^j + K_{32(i-1)+j}) \oplus (X_{i-1}^{16+j} \cdot K_{32(i-1)16+j})$, при *j*=0, 2, 4, 6, 8, 10, 12, 14 и $T^j = (X_{i-1}^j \cdot K_{32(i-1)+j}) \oplus (X_{i-1}^{16+j} + K_{32(i-1)+j})$, при j=1, 3, 5, 7, 9, 11, 13, 15, $i = 1$.

3) Подблоки T^0, T^1, ..., T^{15} записываются в четырех массивах State и выполняются преобразования SubBytes(), ShiftRows(), MixColumns(). После преобразования получатся 32 битные подблоки Y^0, Y^1, ..., Y^{15}.

4) Подблоки Y^0, Y^1, ..., Y^{15} суммируются по XOR с соответствующими подблоками X_{i-1}^j, т.е. $X_{i-1}^j = X_{i-1}^j \oplus Y_{15-j}$, $X_{i-1}^{j+16} = X_{i-1}^{j+16} \oplus Y_{15-j}$, $j = \overline{0...15}$, $i = 1$.

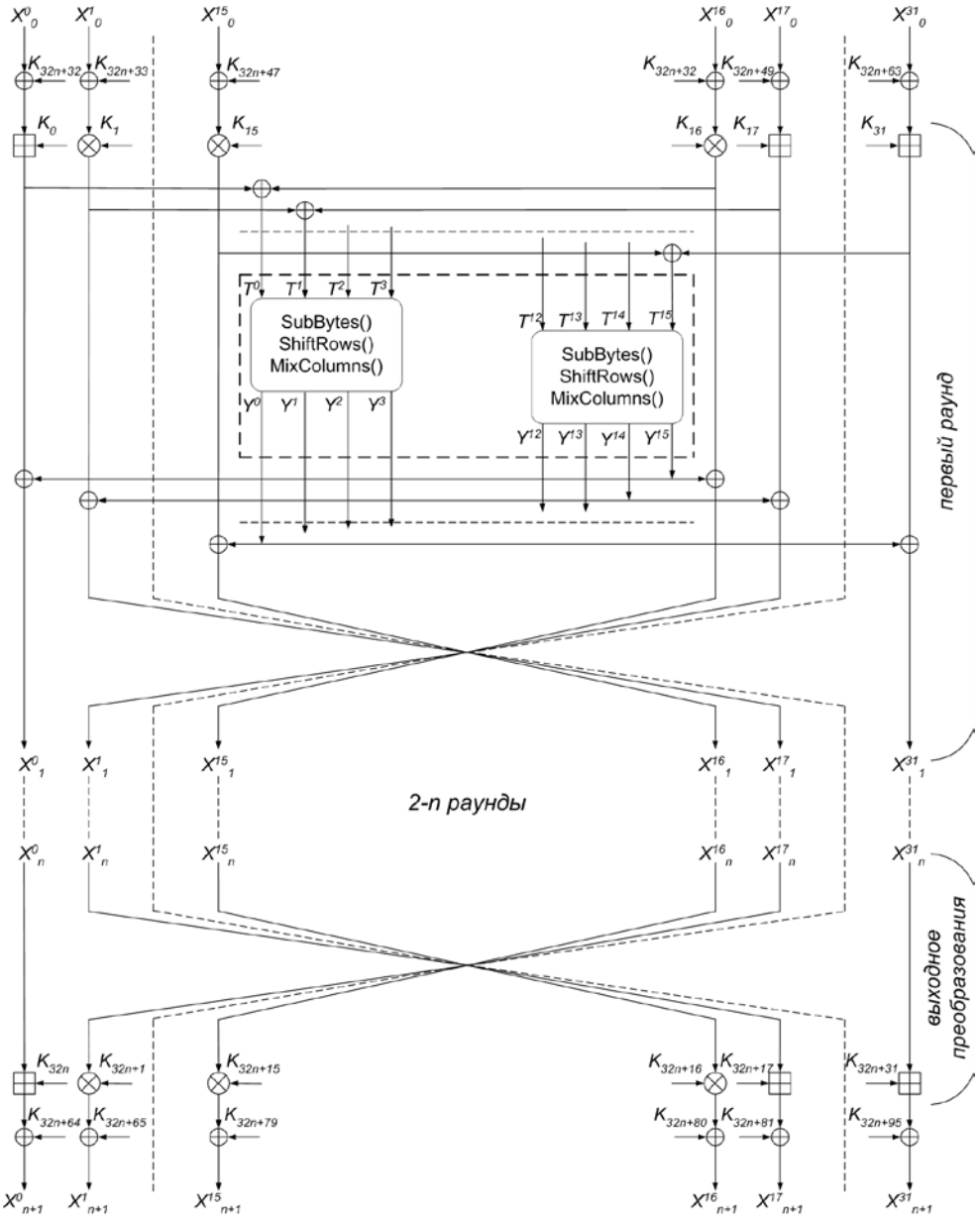

Рис. 6. Структура n –раундового алгоритма шифрования AES–RFWKIDEA32–4

5) В конце раунда кроме подблоков X_i^0 и X_{i-1}^{31} все подблоки поменяются местами, $X_i^j = X_{i-1}^{15+j}$, $X_i^{j+15} = X_{i-1}^j$ $j = \overline{1...15}$, $i = 1$.

6) Повторяя шаги 2–5 n раз, т.е. $i = \overline{2...n}$, получим 32 битные подблоки X_n^0, X_n^1, …, X_n^{31}.

7) В выходном преобразовании раундовые ключи K_{32n}, K_{32n+1}, ..., K_{32n+31} умножаются и суммируются с соответствующими подблоками, т.е., $X_{n+1}^0 = X_n^0 + K_{32n}$, $X_{n+1}^{31} = X_n^{31} + K_{32n+31}$, $X_{n+1}^j = X_n^{31-j} \cdot K_{32n+j}$, при j=1, 3, 5, 7, 9, 11, 13, 15, 16, 18, 20, 22, 24, 26, 28, 30 и $X_{n+1}^j = X_n^{31-j} + K_{32n+j}$, при j=2, 4, 6, 8, 10, 12, 14, 17, 19, 21, 23, 25, 27, 29.

8) Подблоки X_{n+1}^0, X_{n+1}^1, …, X_{n+1}^{31} суммируются по XOR с соответствующими раундовыми ключами K_{32n+64}, K_{32n+65}, ..., K_{32n+95}: $X_{n+1}^j = X_{n+1}^j \oplus K_{32n+64+j}$, $j = \overline{0...31}$. В качестве шифртекста открытого текста X принимается объединение 32 битных подблоков $X_{n+1}^0 \| X_{n+1}^1 \| ... \| X_{n+1}^{31}$.

Генерация ключей алгоритма шифрования AES–RFWKIDEA32–4

В n–раундовом алгоритме шифрования AES–RFWKIDEA32–4 в каждом раунде применяются 32 раундовые ключи длиной 32 бита и в выходном преобразовании 32 раундовые ключи длиной 32 бита. Кроме этого, до первого раунда и после выходного преобразования применяются 32 раундовые ключи длиной 32 бита. Общее число 32 битных раундовых ключей равно 32n+95. При зашифровании на Рис.6 вместо K_i используются раундовые ключи зашифрования K_i^c, при расшифровании раундовые ключи расшифрования K_i^d.

Ключ алгоритма шифрования K длиной l ($256 \le l \le 1024$) бит разбивается на 32 битовых

раундовых ключа K_0^c, K_1^c,..., $K_{Lenght-1}^c$, $Lenght = l/32$, здесь $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^c = \{k_0, k_1, ..., k_{31}\}$, $K_1^c = \{k_{32}, k_{33}, ..., k_{63}\}$,..., $K_{Lenght-1}^c = \{k_{l-32}, k_{l-31}, ..., k_{l-1}\}$ и $K = K_0^c \| K_1^c \| ... \| K_{Lenght-1}^c$. После чего вычисляется $K_L = K_0^c \oplus K_1^c \oplus ... \oplus K_{Lenght-1}^c$. Если $K_L = 0$ тогда в качестве K_L выбирается 0xC5C31537, т.е. $K_L = 0$xC5C31537. Если выполняются условия $i \bmod 3 = 1$, тогда раундовые ключи вычисляются как $K_i^c = SubBytes32(K_{i-Lenght+1}^c) \oplus SubBytes32(RotWord32(K_{i-Lenght}^c)) \oplus Rcon[i \bmod 32] \wedge K_L$, иначе $K_i^c = SubBytes32(K_{i-Lenght}^c) \oplus SubBytes32(K_{i-Lenght+1}^c) \wedge K_L$. После каждой генерации раундовых ключей значение K_L циклически сдвигается влево на 1 бит.

Раундовые ключи расшифрования вычисляются на основе раундовых ключей зашифрования и ключи расшифрования выходного преобразования связаны с ключами зашифрования следующим образом:

$(K_{32n}^d, K_{32n+1}^d, K_{32n+2}^d, K_{32n+3}^d, K_{32n+4}^d, K_{32n+5}^d, K_{32n+6}^d, K_{32n+7}^d, K_{32n+8}^d,$
$K_{32n+9}^d, K_{32n+10}^d, K_{32n+11}^d, K_{32n+12}^d, K_{32n+13}^d, K_{32n+14}^d, K_{32n+15}^d, K_{32n+16}^d,$
$K_{32n+17}^d, K_{32n+18}^d, K_{32n+19}^d, K_{32n+20}^d, K_{32n+21}^d, K_{32n+22}^d, K_{32n+23}^d, K_{32n+24}^d,$
$K_{32n+25}^d, K_{32n+26}^d, K_{32n+27}^d, K_{32n+28}^d, K_{32n+29}^d, K_{32n+30}^d, K_{32n+31}^d) = (-K_0^c,$
$(K_1^c)^{-1}, -K_2^c, (K_3^c)^{-1}, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1}, -K_8^c, (K_9^c)^{-1},$
$-K_{10}^c, (K_{11}^c)^{-1}, -K_{12}^c, (K_{13}^c)^{-1}, -K_{14}^c, (K_{15}^c)^{-1}, (K_{16}^c)^{-1}, -K_{17}^c, (K_{18}^c)^{-1},$
$-K_{19}^c, (K_{20}^c)^{-1}, -K_{21}^c, (K_{22}^c)^{-1}, -K_{23}^c, (K_{24}^c)^{-1}, -K_{25}^c, (K_{26}^c)^{-1}, -K_{27}^c,$
$(K_{28}^c)^{-1}, -K_{29}^c, (K_{30}^c)^{-1}, -K_{31}^c).$

Таким же образом, ключи расшифрования второго, третьего и *n*–раунда связаны с ключами зашифрования следующим образом:

$(K_{32(i-1)}^d, K_{32(i-1)+1}^d, K_{32(i-1)+2}^d, K_{32(i-1)+3}^d, K_{32(i-1)+4}^d, K_{32(i-1)+5}^d, K_{32(i-1)+6}^d,$
$K_{32(i-1)+7}^d, K_{32(i-1)+8}^d, K_{32(i-1)+9}^d, K_{32(i-1)+10}^d, K_{32(i-1)+11}^d, K_{32(i-1)+12}^d,$
$K_{32(i-1)+13}^d, K_{32(i-1)+14}^d, K_{32(i-1)+15}^d, K_{32(i-1)+16}^d, K_{32(i-1)+17}^d, K_{32(i-1)+18}^d,$
$K_{32(i-1)+19}^d, K_{32(i-1)+20}^d, K_{32(i-1)+21}^d, K_{32(i-1)+22}^d, K_{32(i-1)+23}^d, K_{32(i-1)+24}^d,$
$K_{32(i-1)+25}^d, K_{32(i-1)+26}^d, K_{32(i-1)+27}^d, K_{32(i-1)+28}^d, K_{32(i-1)+29}^d, K_{32(i-1)+30}^d,$
$K_{32(i-1)+31}^d) = (-K_{32(n-i+1)}^c, (K_{32(n-i+1)+30}^c)^{-1}, -K_{32(n-i+1)+29}^c,$
$(K_{32(n-i+1)+28}^c)^{-1}, -K_{32(n-i+1)+27}^c, (K_{32(n-i+1)+26}^c)^{-1}, -K_{32(n-i+1)+25}^c,$
$(K_{32(n-i+1)+24}^c)^{-1}, -K_{32(n-i+1)+23}^c, (K_{32(n-i+1)+22}^c)^{-1}, -K_{32(n-i+1)+21}^c,$
$(K_{32(n-i+1)+20}^c)^{-1}, -K_{32(n-i+1)+19}^c, (K_{32(n-i+1)+18}^c)^{-1}, -K_{32(n-i+1)+17}^c,$
$(K_{32(n-i+1)+16}^c)^{-1}, (K_{32(n-i+1)+15}^c)^{-1}, -K_{32(n-i+1)+14}^c, (K_{32(n-i+1)+13}^c)^{-1},$
$-K_{32(n-i+1)+12}^c, (K_{32(n-i+1)+11}^c)^{-1}, -K_{32(n-i+1)+10}^c, (K_{32(n-i+1)+9}^c)^{-1},$
$-K_{32(n-i+1)+8}^c, (K_{32(n-i+1)+7}^c)^{-1}, -K_{32(n-i+1)+6}^c, (K_{32(n-i+1)+5}^c)^{-1},$
$-K_{32(n-i+1)+4}^c, (K_{32(n-i+1)+3}^c)^{-1}, -K_{32(n-i+1)+2}^c, (K_{32(n-i+1)+1}^c)^{-1},$
$-K_{32(n-i+1)+31}^c), i = \overline{2...n}.$

Раундовые ключи расшифрования первого раунда связаны к раундовым ключам зашифрования следующим образом:

$(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d, K_6^d, K_7^d, K_8^d, K_9^d, K_{10}^d, K_{11}^d, K_{12}^d, K_{13}^d,$
$K_{14}^d, K_{15}^d, K_{16}^d, K_{17}^d, K_{18}^d, K_{191}^d, K_{20}^d, K_{21}^d, K_{22}^d, K_{23}^d, K_{24}^d, K_{25}^d, K_{26}^d,$
$K_{27}^d, K_{28}^d, K_{28}^d, K_{29}^d, K_{30}^d, K_{31}^d) = (-K_{32n}^c, (K_{32n+1}^c)^{-1}, -K_{32n+2}^c,$
$(K_{32n+3}^c)^{-1}, -K_{32n+4}^c, (K_{32n+5}^c)^{-1}, -K_{32n+6}^c, (K_{32n+7}^c)^{-1}, -K_{32n+8}^c,$
$(K_{32n+9}^c)^{-1}, -K_{32n+10}^c, (K_{32n+11}^c)^{-1}, -K_{32n+12}^c, (K_{32n+13}^c)^{-1}, -K_{32n+14}^c,$
$(K_{32n+15}^c)^{-1}, (K_{32n+16}^c)^{-1}, -K_{32n+17}^c, (K_{32n+18}^c)^{-1}, -K_{32n+19}^c, (K_{32n+20}^c)^{-1},$
$-K_{32n+21}^c, (K_{32n+22}^c)^{-1}, -K_{32n+23}^c, (K_{32n+24}^c)^{-1}, -K_{32n+25}^c, (K_{32n+26}^c)^{-1},$
$-K_{32n+27}^c, (K_{32n+28}^c)^{-1}, -K_{32n+29}^c, (K_{32n+30}^c)^{-1}, -K_{32n+31}^c).$

Раундовые ключи расшифрования, примененные до первого раунда и после выходного преобразования связаны с ключами зашифрования следующим образом: $K_{32n+32+j}^d = K_{32n+64+j}^c$, $K_{32n+64+j}^d = K_{32n+16+j}^c$, $j = \overline{0...15}$

Полученные результаты

С использованием преобразования алгоритма шифрования AES в качестве раундового преобразования сети IDEA32–4 и RFWKIDEA32–4 разработан алгоритм блочного шифрования AES–IDEA32–4 и AES–RFWKIDEA32–4. В алгоритме шифрования количество раундов и длина ключа являются переменными, и пользователь может выбрать количество раундов и длину ключа в зависимости степени секретности информации и скорости шифрования. Чем больше количество раундов и длина ключей, тем больше степень защищенности информации, но тем меньше скорость шифрования.

Как в алгоритмах шифрования на основе сети Фейстеля, основными преимуществами алгоритмов шифрования AES–IDEA32–4 и AES–RFWKIDEA32–4 являются то, что при зашифровании и расшифровании используется один и тот же алгоритм и в качестве раундовой функций можно использовать любые преобразования, в том числе односторонние функции. При расшифровании алгоритмов шифрования раундовые ключи зашифрования применяются в обратном порядке, при этом на основе операции необходимо вычислять инверсию. Например, если раундовый ключ умножен на подблок, при расшифровании необходимо вычислять мультипликативную инверсию, если суммировано, то необходимо вычислять аддитивную инверсию.

Известно, что стойкость алгоритма шифрования AES тесно связана со стойкостью S–блока, примененного в алгоритме. В S–блоке алгоритма шифрования AES алгебраическая степень нелинейности $\deg = 7$, нелинейность $NL = 112$, стойкость к линейному криптоанализу $\lambda = 32/256$, стойкость к дифференциальному криптоанализу $\delta = 4/256$, критерии строгого лавинного эффекта SAC=8, критерии независимости выходных битов BIC=8.

В алгоритмах шифрования AES–IDEA32–4 и AES–RFWKIDEA32–4 стойкость S–блоков равна стойкости S блока алгоритма шифрования AES, т.е., $\deg = 7$, $NL = 112$, $\lambda = 32/256$, $\delta = 4/256$, SAC= BIC=8.

Исследования показывают что, скорость шифрования алгоритмы шифрования AES–IDEA32–4 и AES–RFWKIDEA32–4 выше, чем AES. Алгоритм шифрования AES–IDEA32–4 на 1.18 раз и алгоритм шифрования AES–RFWKIDEA32–4 1.25 раз быстрее шифрует чем AES.

Выводы

Известно, что как у алгоритмов на основе сети Фейстеля, стойкость алгоритма на основе сети IDEA32–4 и RFWKIDEA32–4 тесно связана со стойкостью раундовой функции. Поэтому, выбирая преобразования стойкого алгоритма шифрования AES на основе раундовой функции сети IDEA32–4 и RFWKIDEA32–4.

Литература

[1] Арипов М.М., Туйчиев Г.Н. Сеть IDEA4–2, состоящая из двух раундовых функций // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент. – 2012. – №4 (24). – С. 55–59.

[2] ГОСТ 28147–89. Государственный Стандарт СССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

[3] Туйчиев Г.Н. О сетях IDEA32–8, IDEA32–4, IDEA32–2, IDEA32–1, созданных на основе сети IDEA32–16 // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент. – 2014. – №2 (30). – С. 45–50.

[4] Tuychiev G.N. To the networks RFWKIDEA32–16, RFWKIDEA32–8, RFWKIDEA32–4, RFWKIDEA32–2 and RFWKIDEA32–1, based on the network IDEA32–16 // International Journal on Cryptography and Information Security (IJCIS), Vol. 5, No. 1, March 2015, pp. 9-20.

[5] Туйчиев Г.Н. Сети RFWKIDEA4–2, IDEA4–1 и RFWKIDEA4–1 // Вестник Туринского политехнического университета в городе Ташкента. – 2013. – №3. – С. 71-77.

[6] Туйчиев Г.Н. О сетях PES4–1 и RFWKPES4–2, RFWKPES4–1, разработанных на основе сети PES4–2 // Узбекский журнал проблемы информатики и энергетики. – Ташкент. – 2015. – №1. – С. 97–103.

[7] Туйчиев Г.Н. Создание блочного алгоритма шифрования на основе сети IDEA4–2, с использованием раундовой функции алгоритма шифрования ГОСТ 28147–89 // Инфокоммуникации: Сети–Технологии–Решения. – Ташкент. – 2014. – №4 (32). – С. 49–54.

[8] Туйчиев Г.Н. О сетях IDEA8–2, IDEA8–1 и RFWKIDEA8–4, RFWKIDEA8–2, RFWKIDEA8–1, разработанные на основе сети IDEA8–4 // Узбекский математический журнал. – Ташкент. – 2014. – №3. – С. 104–118.

[9] Туйчиев Г.Н. О сетях PES8–2 и PES8–1, разработанные на основе сети PES8–4 // Труды международной конференции «Актуальные проблемы прикладной математики и информационных технологий–Аль–Хорезми 2014», Том 2. – Самарканд. – 2014. – С. 28–32.

[10] Туйчиев Г.Н. О сетях RFWKPES8–4, RFWKPES8–2, RFWKPES8–1, разработанные на основе сети PES8–4 // Труды междунар. конференции «Актуальные проблемы прикладной математики и информационных технологий–Аль–Хорезми 2014». – Том 2. – Самарканд. – 2014. – С. 32–36.

[11] Туйчиев Г.Н. О сетях IDEA16–4, IDEA16–2, IDEA16–1, созданных на основе сети IDEA16–8 // Сборник тезисов и докладов республиканского семинара «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения». –Ташкент, 2014 г.

[12] Туйчиев Г.Н. О сетях PES32–8, PES32–4, PES32–2 и PES32–1, созданных на основе сети PES32–16 // Безопасность информации, –Киев, 2014. Том 20, №2, с. 164–168.

[13] Туйчиев Г.Н. О сетях RFWKPES32–8, RFWKPES32–4, RFWKPES32–2 и RFWKPES32–1, созданных на основе сети PES32–16 // Сборник тезисов и докладов республиканского семинара «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения». – Ташкент. – 2014.

[14] Daeman J., Rijmen V. AES Proposal: Rijndael // NIST AES Proposal, 1998, http://csrc.nist.gov / Daeman J., Rijmen V. The Block Cipher Rijndael // Third Smart CardResearch and Advanced Applications Conference Proceedings, 1998.

[15] Tuychiev G. Creating a encryption algorithm based on network RFWKIDEA4–2 with the use the round function of the GOST 28147-89 // International Conference on Emerging Trends in Technology, Science and Upcoming Research in Computer Science (ICDAVIM-2015) printed in International Journal of Advanced Technology in Engineering and Science, 2015, vol. 3, №1, pp. 427-432.

[16] Tuychiev G. Creating a encryption algorithm based on network RFWKPES4–2 with the use the round function of the GOST 28147–89 // International Journal of Multidisciplinary in Cryptology and Information Security, 2015, vol.4., №2, pp. 14-17.

[17] Tuychiev G. New encryption algorithm based on network IDEA8-1 using of the transformation of the encryption algorithm AES // IPASJ International Journal of Computer Science, 2015, Volume 3, Issue 1, pp. 1-6.

[18] Tuychiev G. New encryption algorithm based on network RFWKIDEA8-1 using transformation of AES encryption algorithm // International Journal of Computer Networks and Communications Security, 2015, Vol. 3, №. 2, pp. 43–47.

[19] Tuychiev G. New encryption algorithm based on network PES8-1 using of the transformations of the encryption algorithm AES // International Journal of Multidisciplinary in Cryptology and Information Security, 2015, vol.4., №1, pp. 1-5.

[20] Tuychiev G. New encryption algorithm based on network RFWKPES8-1 using of the transformations of the encryption algorithm AES // International Journal of Multidisciplinary in Cryptology and Information Security, 2014, vol.3., №6, pp. 31-34.

[21] Tuychiev G. New encryption algorithm based on network IDEA16-1 using of the transformation of the encryption algorithm AES // IPASJ International

Journal of Information Technology, 2015, vol. 3, Issue 1, pp. 6-12.

[22] Туйчиев Г.Н. Создание блочного алгоритма шифрования на основе сетей PES32–1 и RFWKPES32–1 с использованием преобразования алгоритма шифрования AES // Сборник научных работы научно-практической конференции «Актуальные вопросы обеспечения кибернетической безопасности и защиты информации- CICSIS-2015», Киев, 25-28 февраля 2015. – С. 101-112.

УДК 003.056.55 (045)

Туйчієв Г.Н. Створення блочного алгоритму шифрування на основі мереж IDEA32-4 і RFWKIDEA32-4 з використанням перетворення алгоритму шифрування AES

Анотація. *На сьогодні одним з найбільш ефективних симетричних блокових шифрів є AES. У статті розроблені алгоритми блокового шифрування AES-IDEA32-4 і AES-RFWKIDEA32-4 на основі мережі IDEA32-4 і RFWKIDEA32-4. В алгоритмі шифрування AES-IDEA32-4 у якості раундової функції обрані перетворення SubBytes(), ShiftRows(), MixColumns(), AddRoundKey(), а в алгоритмі шифрування AES-RFWKIDEA32-4 у якості раундової функції обрані перетворення SubBytes(), ShiftRows(), MixColumns(). Довжина блоку алгоритмів шифрування дорівнює 512 бітам, кількість раундів дорівнює 10, 12, 14 і довжина ключа змінюється від 256 біт до 1024 біт з кроком 128 біт.*

Ключові слова: *криптографія, симетричний алгоритм, перетворення, раунд, раундова функція, ключ, зашифрування, розшифрування.*

Tuychiev G. The development of block encryption algorithm based on IDEA32-4 and RFWKIDEA32-4 networks using transformation of the encryption algorithm AES

Abstract. *Today one of the most effective symmetric block ciphers is AES. In the paper block encryption algorithms AES-IDEA32-4 and AES-RFWKIDEA32-4 on the basis of networks IDEA32-4 and RFWKIDEA32-4 were developed. In the encryption algorithm AES-IDEA32-4 as a round function were selected transformation SubBytes(), ShiftRows(), MixColumns(), AddRoundKey(), and in the encryption algorithm AES-RFWKIDEA32-4 as a round function were selected transformation SubBytes(), ShiftRows(), MixColumns(). The block length of encryption algorithm is 512 bits, the number of rounds is 10, 12, 14 and key length changes from 256 bits to 1024 bits with a step of 128 bits.*

Key words: *cryptography, symmetric algorithm, transformation, round, round function, key, encryption, decryption.*

Отримано *27 травня 2015 року*, затверджено редколегією *12 червня 2015 року*