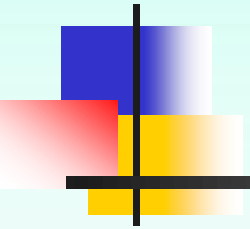
CRYPTOGRAPHY

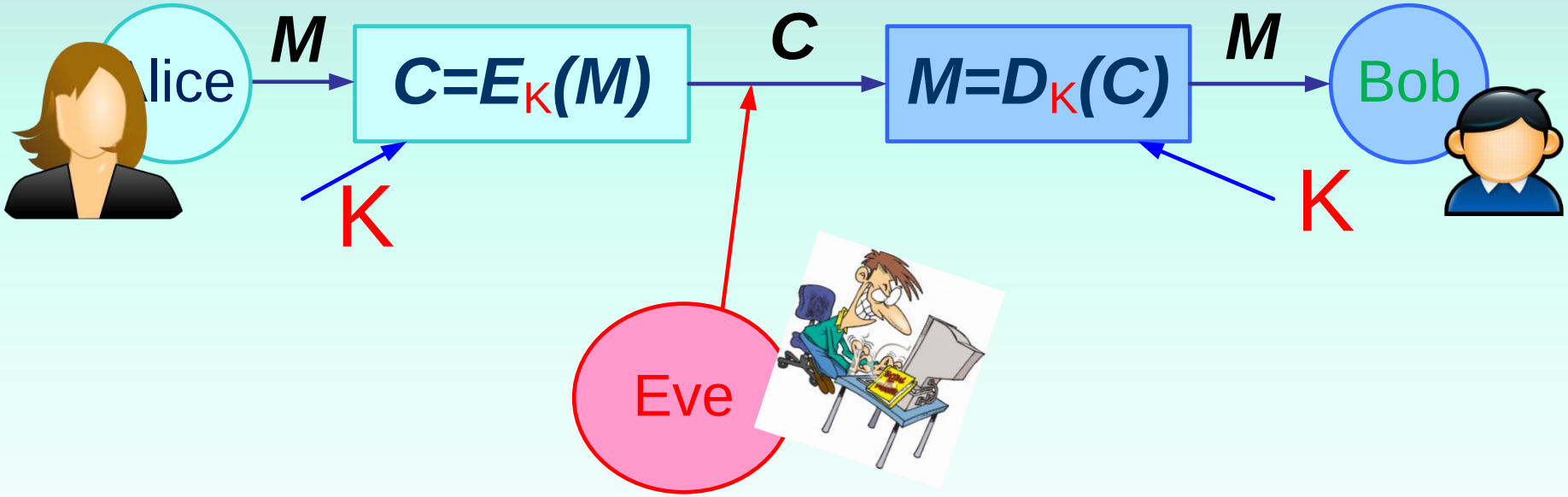


МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Лек. 10 2022 КІБ-19

СТАНДАРТ AES

Advanced Encryption Standard



СИММЕТРИЧНЫЙ АЛГОРИТМ БЛОЧНОГО ШИФРОВАНИЯ

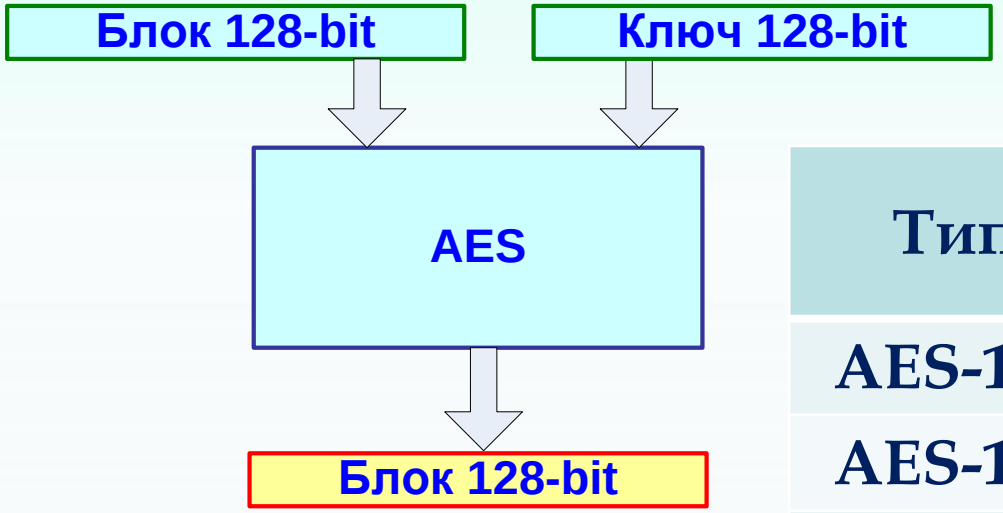
→ ОДИН СЕКРЕТНЫЙ КЛЮЧ

как для шифрования, так и дешифрования

Принят NIST (USA) в 2001 году

Advanced Encryption Standard

AES – блочный шифр *не-Фейстеля*: использует только обратимые операции - замены, перестановок и гаммирования (сложение по модулю 2).
Относится к подстановочно – перестановочным сетям (SP-сеть).



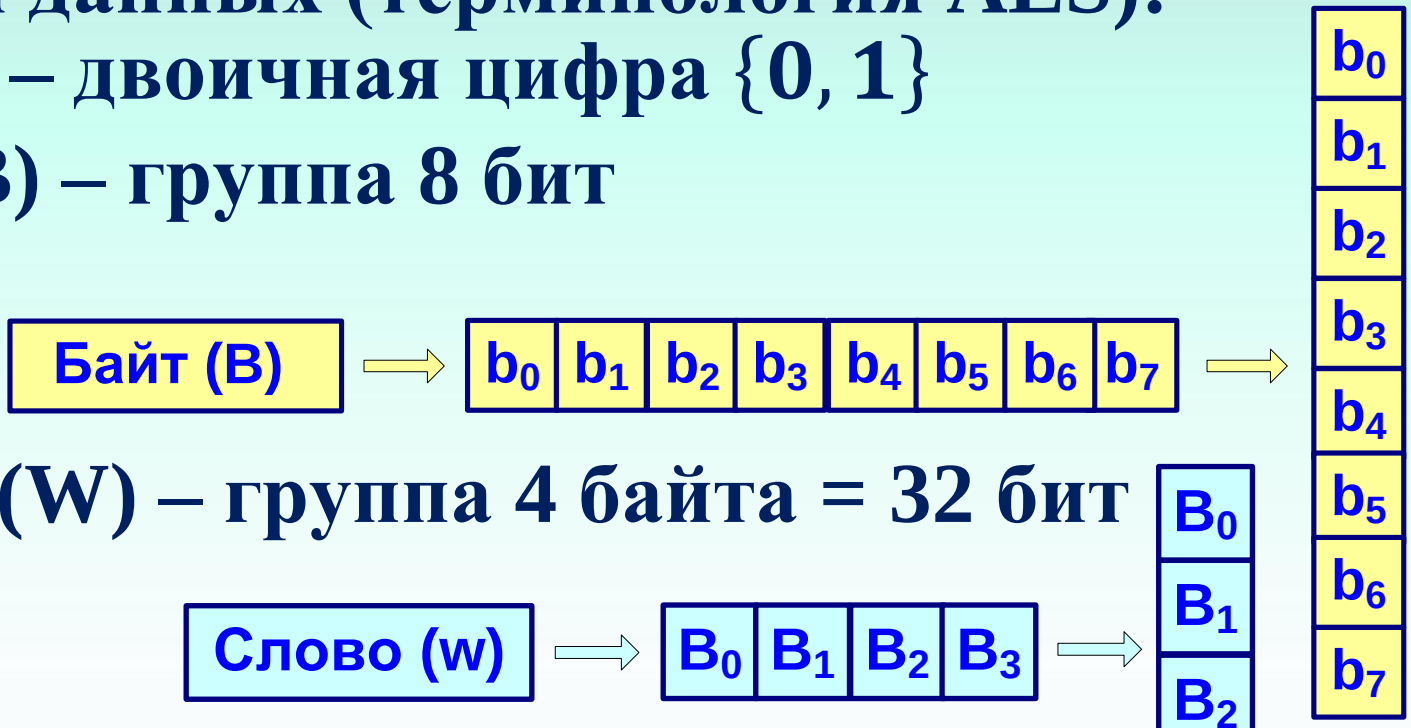
Тип	Ключ (бит)	Раундов
AES-128	128	10
AES-192	192	12
AES-256	256	14

Блок – 128 бит.

Advanced Encryption Standard

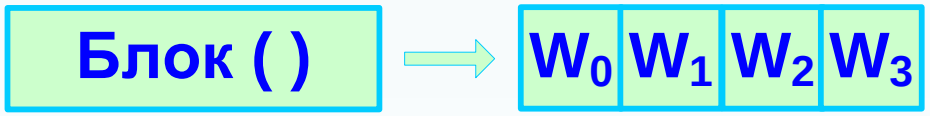
Единицы данных (терминология AES):

- **Бит (b) – двоичная цифра {0, 1}**
- **Байт (B) – группа 8 бит**



- **Слово (W) – группа 4 байта = 32 бит**

- **Блок – группа 4 слова = 16 байт = 128 бит**



Advanced Encryption Standard

Единицы данных (терминология AES):

- **Матрица состояний (S, state) – 16 байт**

$S_{r,c}$, здесь $r \in \{0, 1, 2, 3\}$ номер строки,
$c \in \{0, 1, 2, 3\}$ номер столбца
N_b - число столбцов (32-бит слов), $N_b = 4$

Базовая структура AES

Шифрование

N_r - число раундов, $N_r = 10$

Раунды $i \in \{0, 1, 2, \ldots, N_r\}$

K_i - ключ i-го раунда

K – секретный ключ (cipher key)

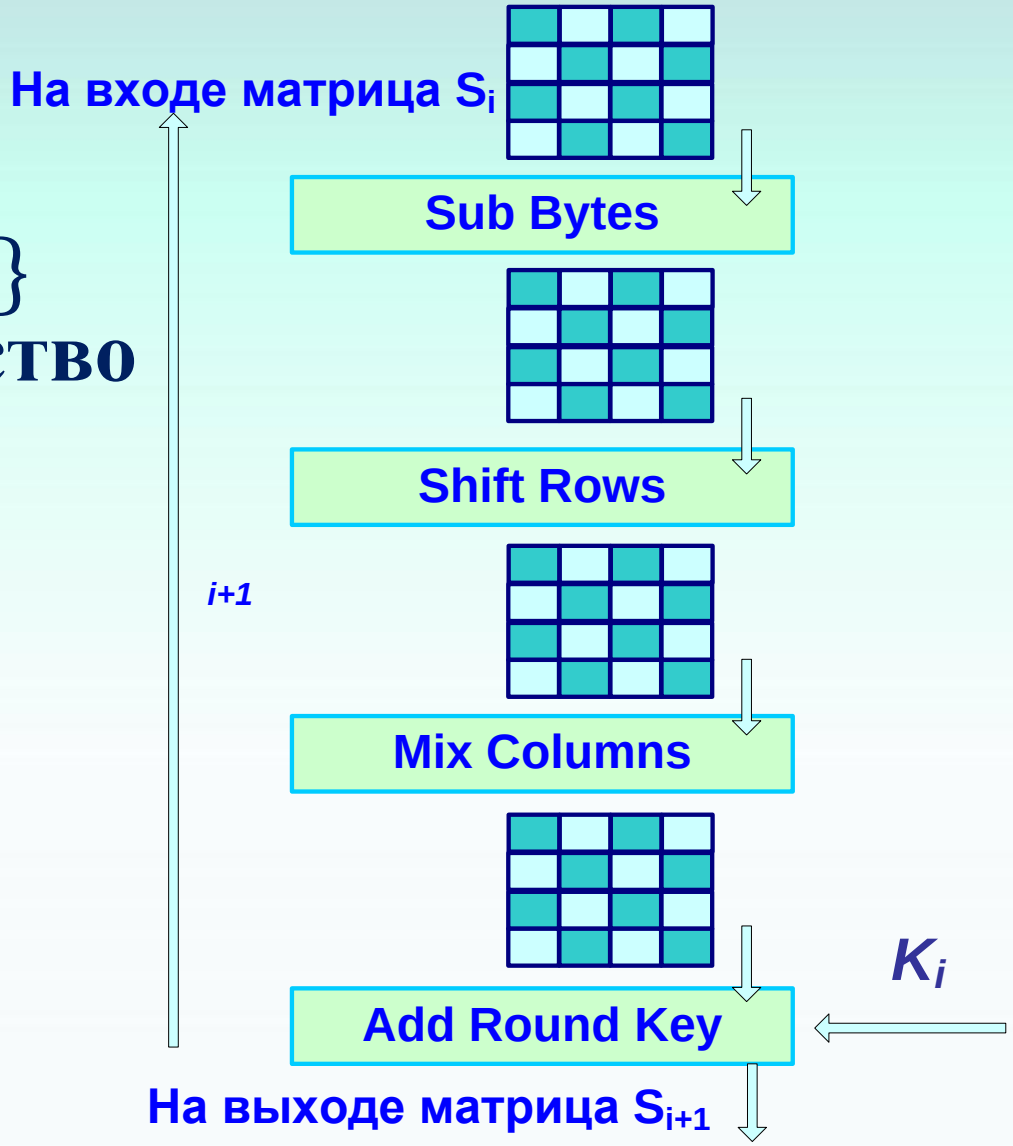
N_k - число слов в ключе, $N_k = 4$

AES раунд

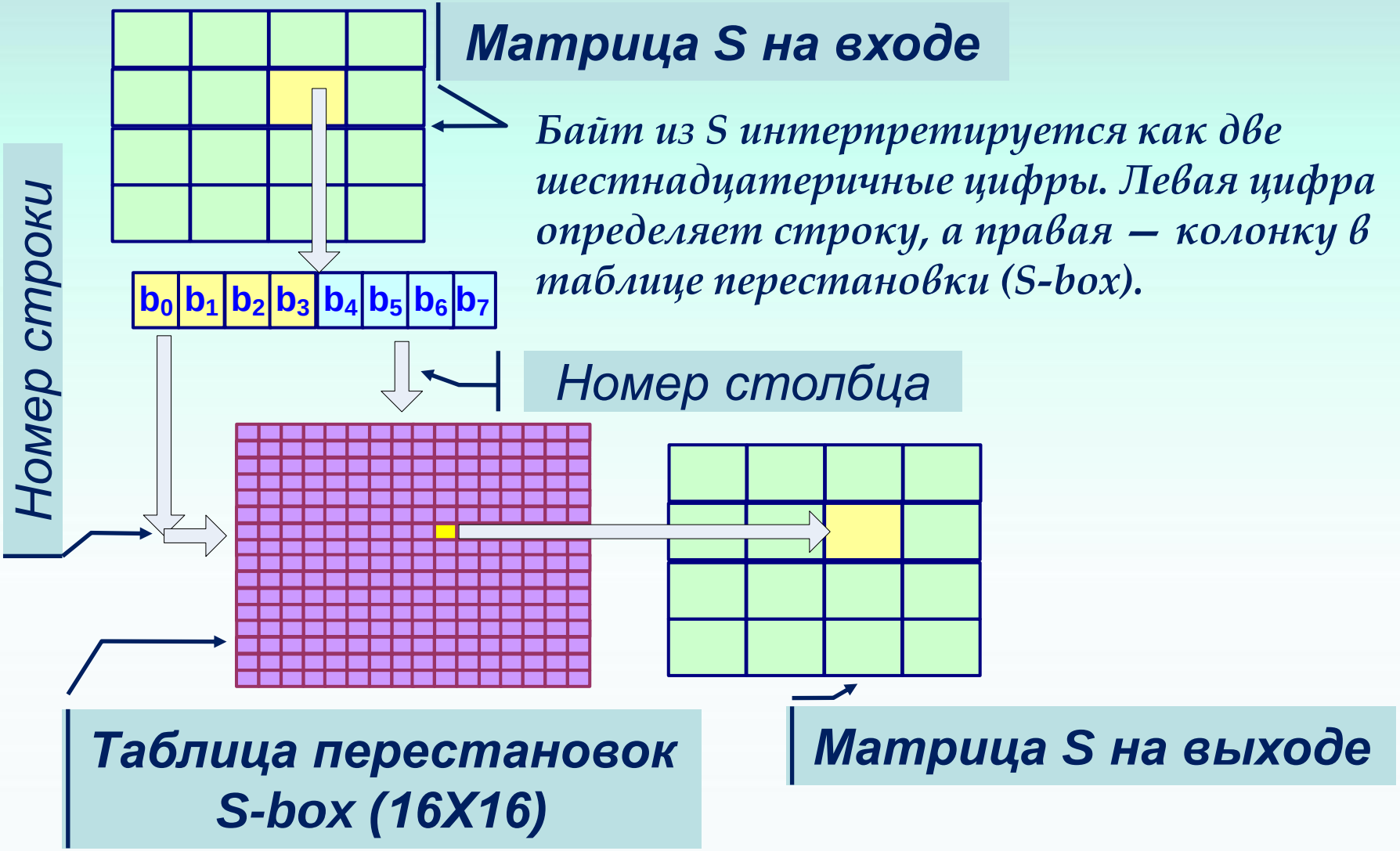
Раунды
$i \in \{0, 1, 2, \ldots, N_r\}$
N_r - количество раундов

Раунд 0 – только *Add Round Key*

Раунд N_r – без *Mix Columns*



AES преобразование SubBytes()



На пересечении строки и колонки, обозначенных этими цифрами, находится подстановочный байт.

AES преобразование SubBytes()

	_0	_1	_2	_3	_4	_5	_6	_7	_8	_9	_A	_B	_C	_D	_E	_F
0_	63	7C	77	7B	F2	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	6E	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	19	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	4B	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

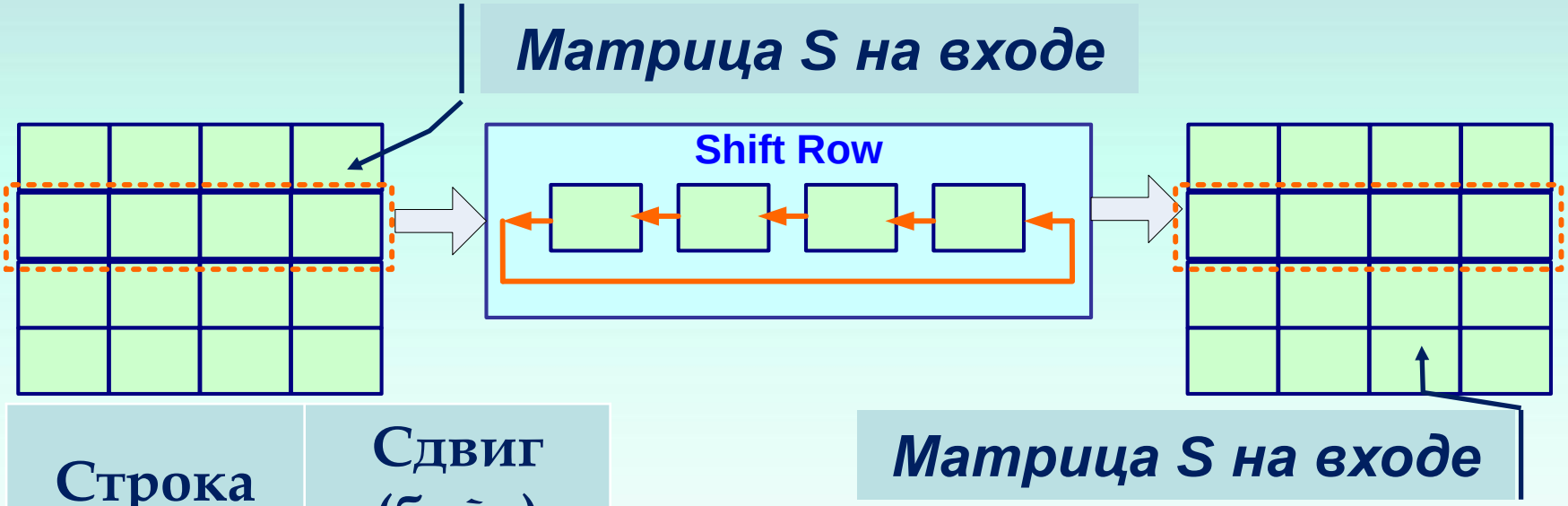
Direct S-box

Invers S-box

	_0	_1	_2	_3	_4	_5	_6	_7	_8	_9	_A	_B	_C	_D	_E	_F
0_	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1_	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2_	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3_	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4_	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5_	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6_	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7_	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8_	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9_	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A_	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B_	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C_	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D_	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E_	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F_	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

SubBytes()← → InvSubBytes()

AES преобразование ShiftRows()



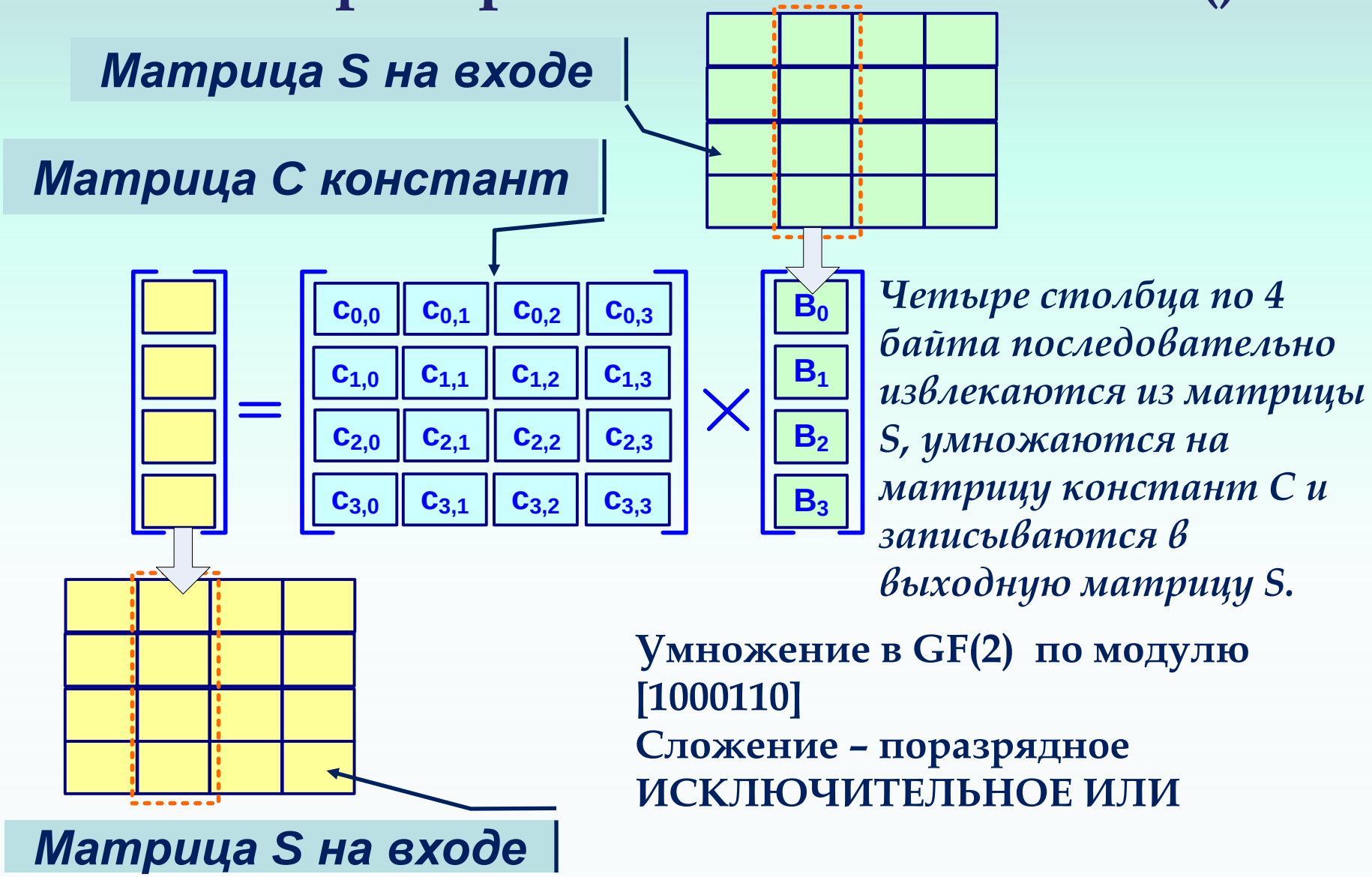
Строка	Сдвиг (байт)
0	0
1	1
2	2
3	3

Четыре строки по 4 байта каждая последовательно извлекаются из матрицы S, циклически сдвигаются на X байт влево и записываются в матрицу S. Число сдвигов численно равно номеру строки.

ShiftRows() ← → InvShiftRows()

При дешифровании аналогично, но сдвиги вправо.

AES преобразование MixColumns()



Четыре столбца по 4 байта последовательно извлекаются из матрицы S, умножаются на матрицу констант C и записываются в выходную матрицу S.

Умножение в GF(2) по модулю [1000110]
Сложение – поразрядное ИСКЛЮЧИТЕЛЬНОЕ ИЛИ

AES преобразование MixColumns()

Direct C

02	03	01	01
01	02	03	01
01	01	02	03
01	01	01	02

Invers C

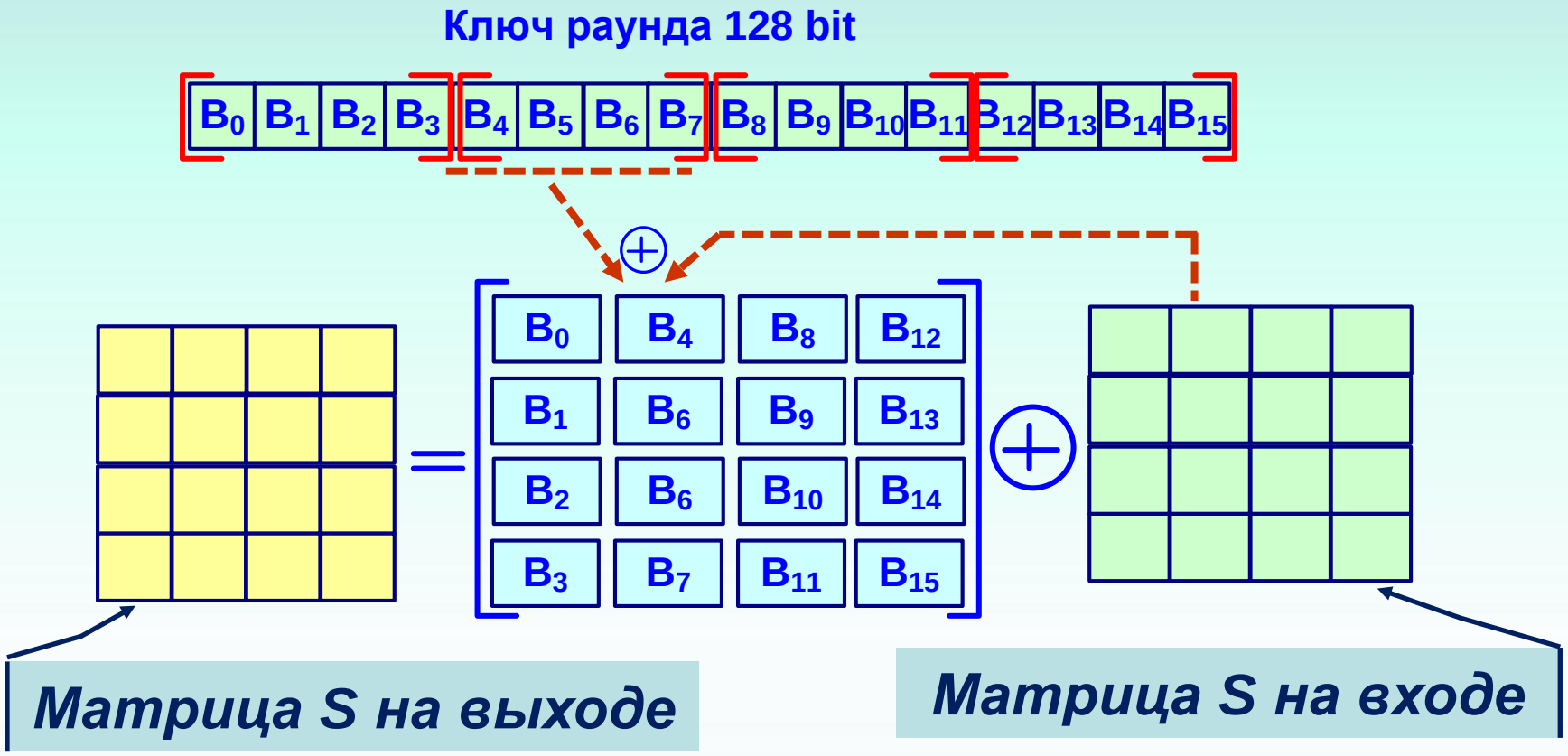
0E	0B	0D	09
09	0E	0B	0C
0D	09	0E	0B
0B	0D	09	0E

Например, первый байт результата (строка X столбец)

$$b_0 = (02 \odot S_{0,c}) \oplus (03 \odot S_{1,c}) \oplus S_{2,c} \oplus S_{3,c}$$

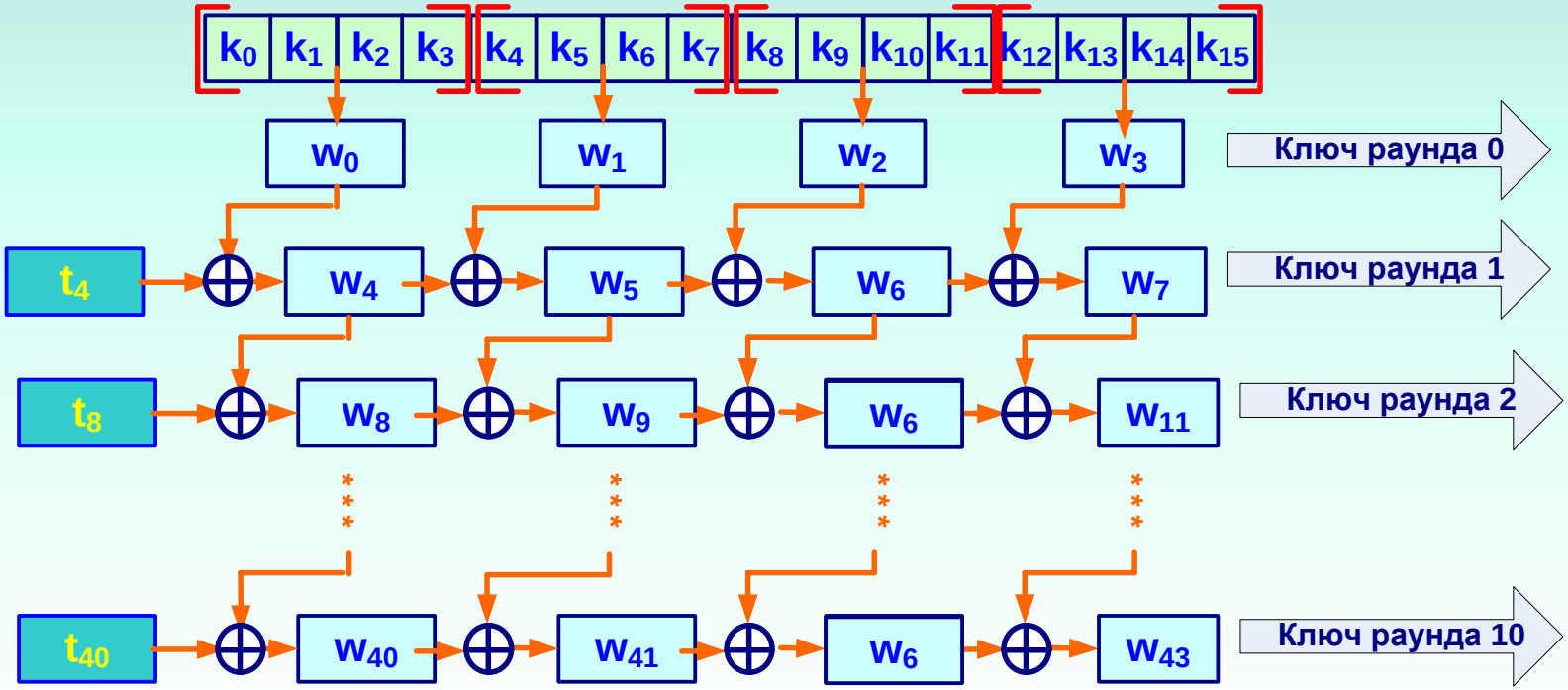
MixColumns() ← → InvMixColumns()

AES преобразование AddRoundKey()



Четыре столбца по 4 байта последовательно извлекаются из матрицы S, суммируются по модулю 2 на соответствующее слово ключа раунда записываются в выходную матрицу S.

AES Расширение ключей



Ключ раунда 0 – первые четыре слова ключа шифра.

Ключ i-го раунда:

if $(i \bmod 4) \neq 0$:

$$w_i = w_{i-1} \oplus w_{i-4}$$

if $(i \bmod 4) = 0$:

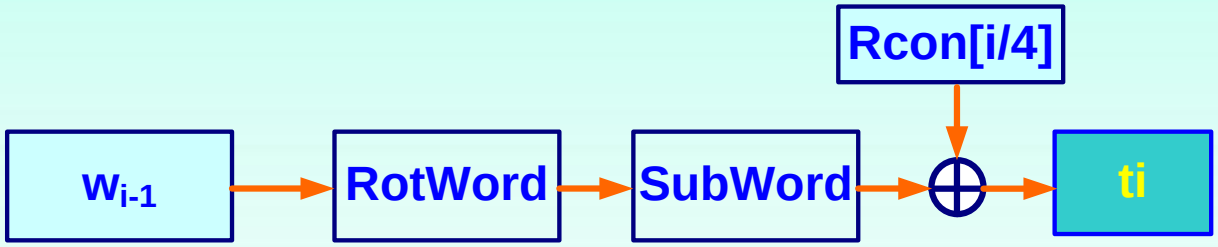
$$w_i = t \oplus w_{i-4}$$

Раунд	Слова ключа раунда			
0	W_0	W_1	W_2	W_3
1	W_4	W_5	W_6	W_7
2	W_8	W_9	W_{10}	W_{11}
...	...	...	...	...
10	W_{40}	W_{41}	W_{42}	W_{43}

AES Расширение ключей

Формирование t (временное слово)

$$t = SubWord(\, RotWord(w_{i-1})) \oplus RCon_{i/4}$$



Раунд	RCon (Hex)
1	01 00 00 00
2	02 00 00 00
3	04 00 00 00
4	08 00 00 00
5	10 00 00 00
6	20 00 00 00
7	40 00 00 00
8	80 00 00 00
9	1B 00 00 00
10	36 00 00 00

RotWord – аналог ShiftRow , но применяется только к одной строке. Циклический сдвиг влево на один байт.

SubWord – аналог SubByte , но применяется только к одной строке. Принимает байт в слове и заменяет его другим (используя S-box).

AES. Cipher

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
      byte state[4,Nb]
      state = in
      AddRoundKey(state, w[0, Nb-1])
      for round = 1 step 1 to Nr-1
            SubBytes(state)
            ShiftRows(state)
            MixColumns(state)
            AddRoundKey(state, w[round*Nb,
                                 (round+1)*Nb-1])
      end for
      SubBytes(state)
      ShiftRows(state)
      AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
      out = state
end
```

AES. Inverse Cipher

```
InvCipher(byte in[4 * Nb], byte out[4 * Nb], word w[Nb *
(Nr+1)])
begin
      byte state[4, Nb]
      state = in
      AddRoundKey(state, w[Nr * Nb, Nb * (Nr+1) - 1])
      for round = Nr - 1 step -1 downto 1
            InvShiftRows(state)
            InvSubBytes(state)
            AddRoundKey(state,w[Nb*round,Nb*
                                    (round+1)-1])
            InvMixColumns(state)
      end for
      InvShiftRows(state)
      InvSubBytes(state)
      AddRoundKey(state, w[0, Nb - 1])
      out = state
end
```

AES. Key Expansion

```
KeyExpansion(byte key[4 * Nk], word w[Nb * (Nr+1)], Nk)
Begin
    word temp
    i = 0;
    while(i < Nk)
         w[i]=word(key[4*i],key[4*i+1], key[4*i+2],
                                              key[4*i+3])
       i = i + 1
    end while
    i = Nk
    while(i < Nb * (Nr+1))
        temp = w[i - 1]
        if (i mod Nk = 0)
            temp=SubWordRotWord(temp)) xor Rcon[i/Nk]
        else if(Nk>6 and i modNk = 4)
                temp = SubWord(temp)
        end if
        w[i] = w[i - Nk] xor temp
        i = i + 1
    end while
end
```

AES. Криптостойкость

2003 Агентство национальной безопасности США
SECRET →AES 128
TOP SECRET →AES 192 | AES 256

Атака грубой силы неосуществима:
Если предположить, что можно построить машину, которая может восстановить ключ DES в секунду (попробовать 2^55 ключей в секунду), то этой машине потребуется примерно 149 тысяч миллиардов (149 триллионов) лет чтобы взломать 128-битный ключ AES. Считается , что возраст Вселенной составляет менее 20 миллиардов лет.

Сообщений о взломе AES нет.

Вопросы:

- Охарактеризуйте ,базовую структуру и организацию процесса шифрования/дешифрования в стандарте **AES**.
- Определите функцию AES преобразования **SubBytes().**
- Определите функцию AES преобразования **ShiftRows().**
- Определите функцию AES преобразования **MixColumns().**
- Определите функцию AES преобразования **AddRoundKey().**

Вопросы:

- Поясните организацию и функционирование генератора раундовых ключей (функция **KeyExpancion().**
- Охарактеризуйте криптостойкость стандарта **AES**.

ЛИТЕРАТУРА

FIPS-197
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

ЛИТЕРАТУРА

Нечаев В.И. Элементы криптографии (Основы теории защиты информации).- Учеб. пособие. – М.:, ВШ., 1999.- 109 с.

Введение в криптографию. **Под общ. ред. В.В.Ященко.** – 4-е изд., доп. М.: МЦНМО, 2012 – 348 с. ISBN 978-5-4439-0026-1

ЛИТЕРАТУРА

Венбо Мао. Современная криптография: теория и практика.—М.: Издательский дом «Вильямс», 2005.—768 с.: ил. ISSN 5-8459-0847-7 (рус.)

Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на Си. – Москва: Вильямс, 2016. 1024 с.

ЛИТЕРАТУРА

Francisco Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc.

Cryptographic Algorithms on Reconfigurable Hardware. - Springer, 2006.

A. Menezes, P. van Oorschot, S. Vanstone.

Handbook of Applied Cryptography.- CRC Press, 1996.

END # 10