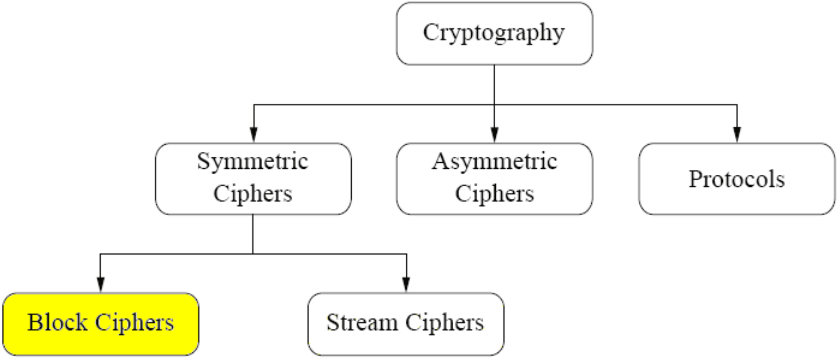
Introdução à Criptografia

Cifras de Bloco
AES

Prof. Rodrigo Minetto
rminetto@dainf.ct.utfpr.edu.br
Universidade Tecnológica Federal do Paraná
Baseado em: Understanding Cryptography by Paar e Pelzl

Sumário

Algoritmos para criptografia



Introdução

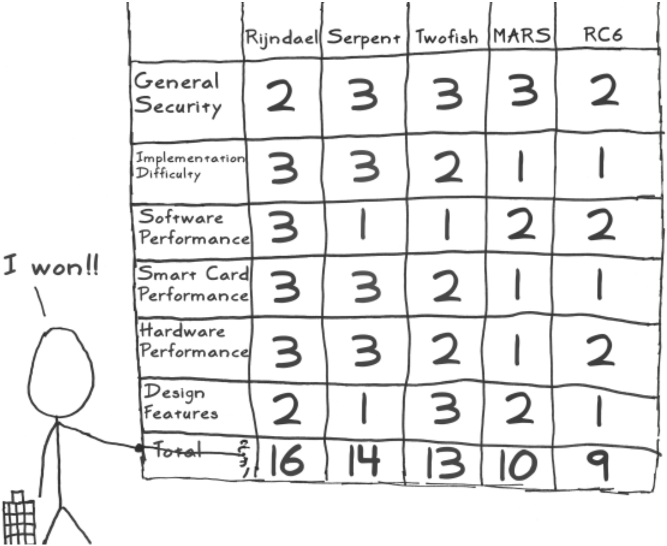
Em 1997, o governo americano, representado pelo NIST (National Institute of Standards and Technology), promoveu uma seleção para a adoção de um novo algoritmo de chave privada simétrica para proteger informações do governo federal americano. Ao algoritmo vencedor foi atribuído o nome de **AES** (**Advanced Encryption Standard**). O algoritmo AES tornou-se um padrão efetivo em 26 de Maio de 2002 e rapidamente substitui o DES em muitas aplicações. Em 2006, o AES já era considerado um dos algoritmos mais populares usados para criptografia de chave simétrica no mundo.

Introdução

Requisitos para participar da competição:

- Divulgação pública.
- Livre de direitos autorais.
- Operar em blocos de 128 bits.
- Permitir chaves de 128, 192 e 256 bits.
- Eficiente em hardware e software.
- Segurança (esforço requerido para criptoanálise).
- Eficiência computacional e de memória.
- Simplicidade e facilidade de implementação.

The Advanced Encryption Standard (AES)

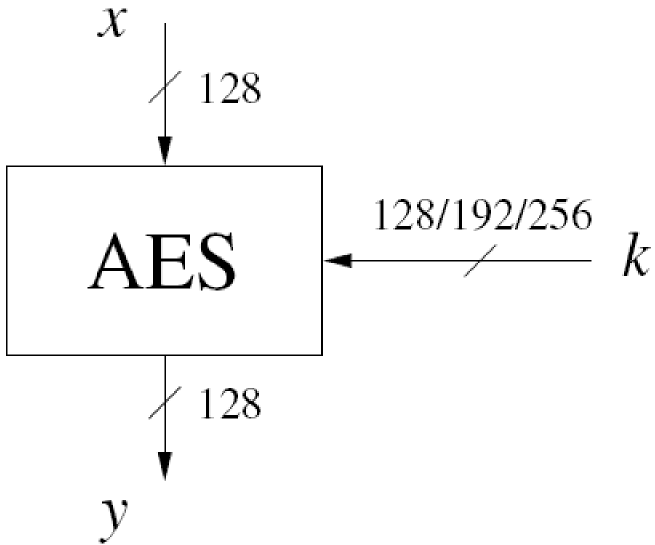


https://www.techbliss.org/threads/history-of-aes.35/

Introdução

Curiosidade: em 2003 a NSA (National Security Agency) anunciou a permissão para utilizar o AES para cifrar documentos da categoria **SECRET** para qualquer tamanho de chave, e documentos da categoria **TOP SECRET** para chaves de 192 e 256 bits. Até aquele momento, somente algoritmos de domínio não-público eram utilizados para cifrar documentos secretos.

The Advanced Encryption Standard (AES)



The Advanced Encryption Standard (AES)

O algoritmo AES cifra todos os 128 bits a cada iteração (NÃO utiliza uma rede de Feistel)

Tamanho da chave	Número de rodadas
128 bits	10
192 bits	12
256 bits	14

O DES utiliza 16 rodadas para uma chave de 56 bits (cifra metade dos bits por iteração).

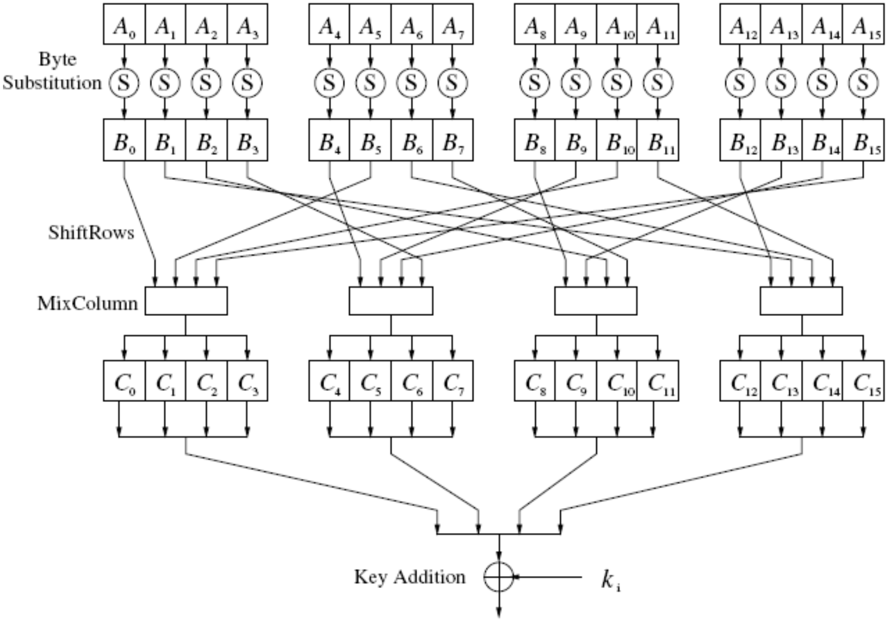
Introdução

No AES os módulos são chamados de **layers**. Cada layer manipula 128 bits de dados. Existem três tipos diferentes de layers no AES:

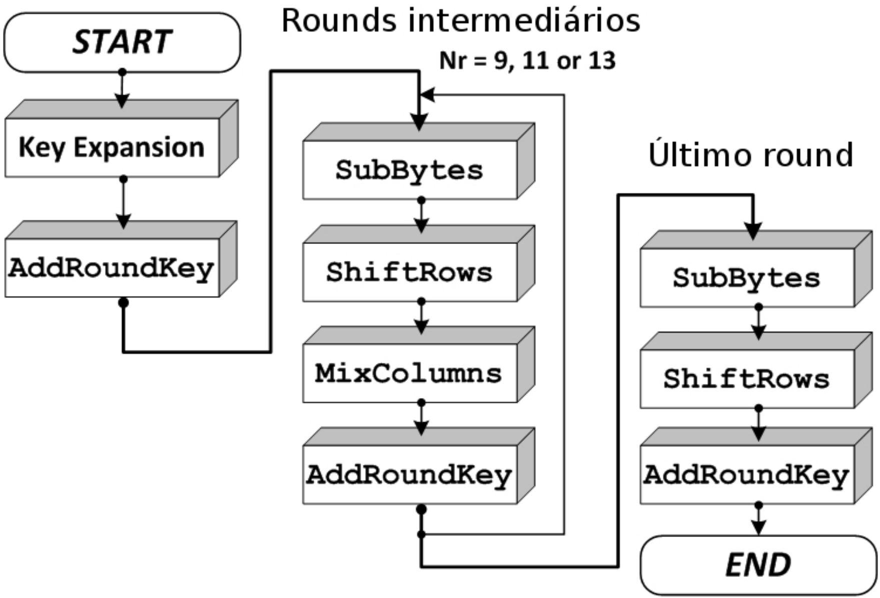
- **Key Addition layer**: escalonador de sub-chaves.
- **Byte Substitution layer (S-Box)**: operação não-linear (confusão).
- **Diffusion layer**: operações lineares (difusão)
  - **ShiftRows**: permutação de bytes.
  - **MixColumn**: permutação de blocos.

O AES é orientado a **byte**, ao contrário do DES que é orientado a **bit**.

The Advanced Encryption Standard (AES)

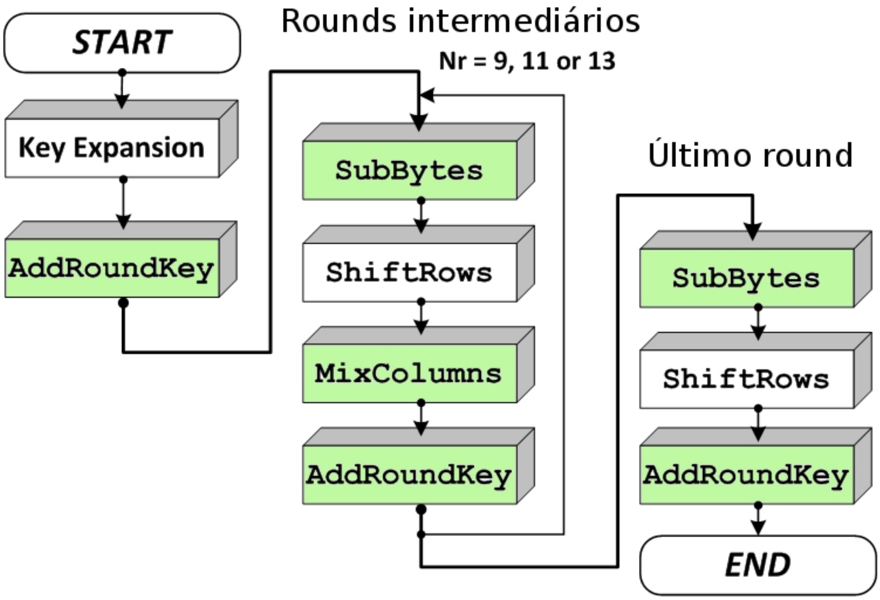


The Advanced Encryption Standard (AES)



Sumário

Os módulos em verde usam a teoria de Galois



Galois Field

O algoritmo AES é baseado na teoria de **corpos finitos de Galois**. Os elementos de um corpo primo $GF(p)$ são os inteiros que pertecem ao conjunto $\{0, 1, 2, \ldots, p-1\}$. As operações de adição e multiplicação em $GF(p)$ são operações modulares.

Galois Field

Um corpo de extensão de Galois é representado por $GF(2^n)$, observe que 2^n pode não produzir um número primo. Analogamente ao corpo $GF(p)$, uma redução polinomial de grau n é utilizada para construir $GF(2^n)$. A adição no corpo de extensão $GF(2^n)$ é realizada em módulo 2 nos coeficientes dos dois polinômios. Já para a multiplicação necessitamos de um **polinômio irredutível**, pois o resultado da multiplicação pode produzir resultados com grau maior que n. Um polinômio é irredutível se ele não pode ser representado como a multiplicação de outros dois polinômios de menor grau.

Galois Field

As operações no algoritmo AES são realizadas no campo finito $GF(2^8)$. Esse campo foi escolhido para permitir a representação de cada elemento por um único byte (8 bits). A notação $GF(2^8)$ considera um conjunto de 2^8 polinômios possíveis com a seguinte representação

$$f(x) = a_7x^7 + \cdots + a_1x + a_0, \quad a_i \in GF(2) = \{0, 1\}.$$

Observe que cada polinômio pode ser representado na forma digital pelo seguinte vetor de 8-bits

$$f = (a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0)$$

Exemplos:

$$x^0 = (00000001)_2 = (01)_{\mathrm{hex}}$$
$$x^1 = (00000010)_2 = (02)_{\mathrm{hex}}$$
$$x^2 = (00000100)_2 = (04)_{\mathrm{hex}}$$
$$x^3 = (00001000)_2 = (08)_{\mathrm{hex}}$$
$$x^3 + x^2 + x^1 + x^0 = (00001111)_2 = (0F)_{\mathrm{hex}}$$
$$x^7 + x^6 + x = (11000010)_2 = (C2)_{\mathrm{hex}}$$
$$x^5 + x^3 + x^2 + x + 1 = (00101111)_2 = (2F)_{\mathrm{hex}}$$
$$x^7 + x^6 + x^5 + x^4 + x = (11110010)_2 = (F2)_{\mathrm{hex}}$$

Adição em $GF(2^m)$

A soma de $F(x)$ e $G(x) \in GF(2^m)$ é definida por

$$H(x) = F(x) + G(x) = \sum_{i=0}^{m-1} c_i x^i, \; c_i \equiv f_i + g_i \bmod 2$$

$$\begin{array}{rcccccccccc}
F(x) & = & x^7 & + & x^6 & + & x^4 & + & & & 1 \\
G(x) & = & & & & & x^4 & + & x^2 & + & 1 \\
\hline
H(x) & = & x^7 & + & x^6 & + & & & x^2 & &
\end{array}$$

Multiplicação em $GF(2^m)$

Seja $F(x)$ e $G(x) \in GF(2^m)$ e seja também

$$P(x) \equiv \sum_{i=0}^{m} p_i x^i, \; p_i \in GF(2)$$

um **polinômio irredutível**. A multiplicação é então definida por

$$H(x) \equiv F(x) \cdot G(x) \mod P(x)$$

No AES $P(x) = x^8 + x^4 + x^3 + x + 1$.

Multiplicação no $GF(2^8)$

$$F(x) = x^6 + x^4 + x^2 + x + 1 = (01010111)_2$$

$$G(x) = x^4 + x + 1 = (00010011)_2$$

$$P(x) = x^8 + x^4 + x^3 + x + 1 = (100011011)_2$$

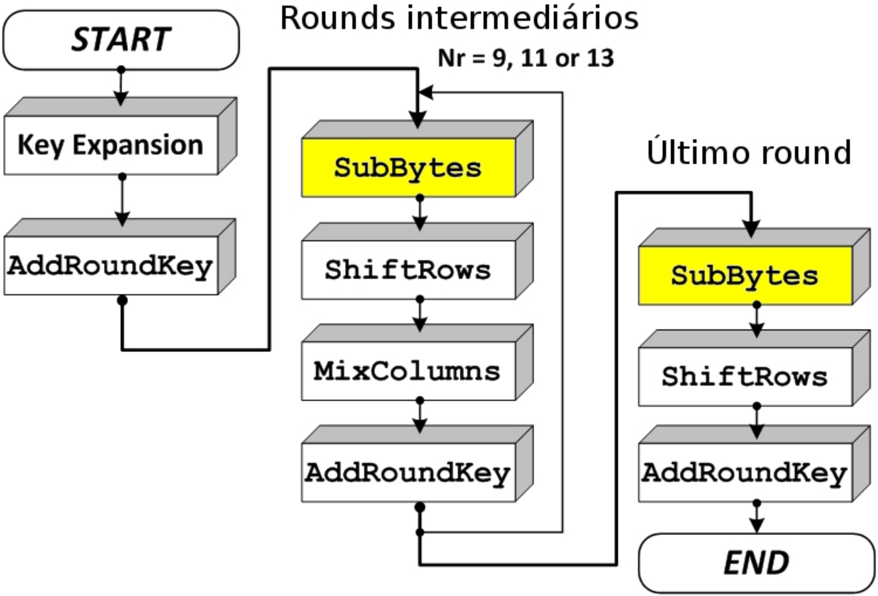
$$\begin{array}{lcccc}
F(x) = & x^6 + & x^4 + & x^2 + & x + 1 \times \\
G(x) = & & x^4 + & & x + 1 \\
\hline
\multicolumn{5}{l}{H(x) = x^{10} + x^8 + x^7 + x^3 + 1}
\end{array}$$

Redução modular por P: $H(x) \bmod P(x)$

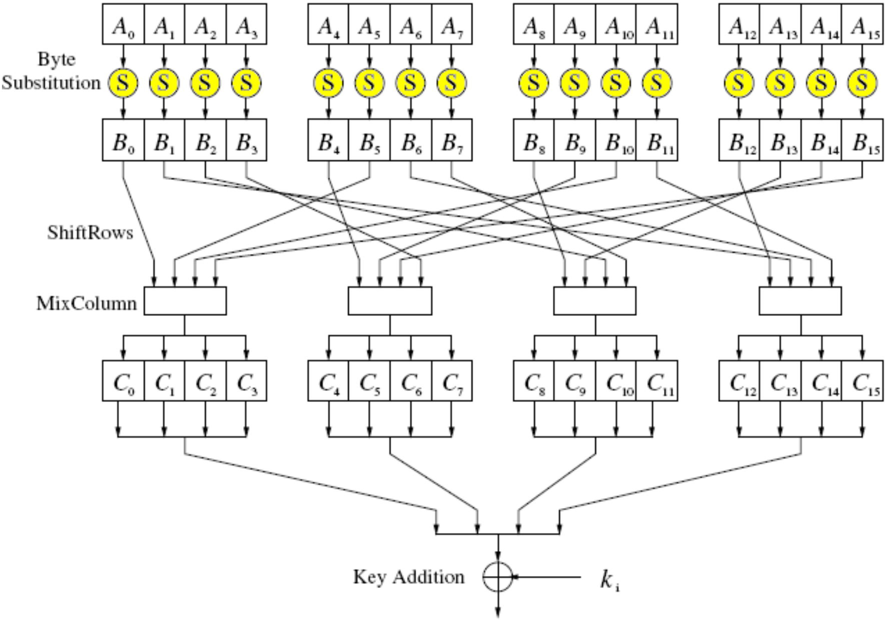
Resp: $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x = 11111110 = FE_{hex}$.

Sumário

The Advanced Encryption Standard (AES)

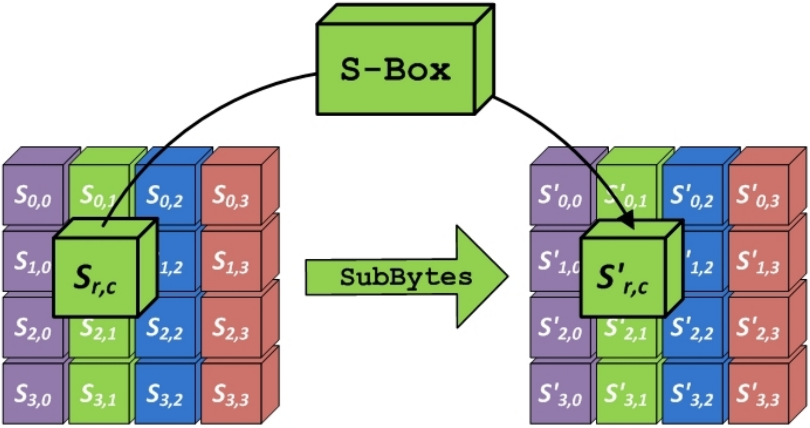


The Advanced Encryption Standard (AES)



The Advanced Encryption Standard (AES)

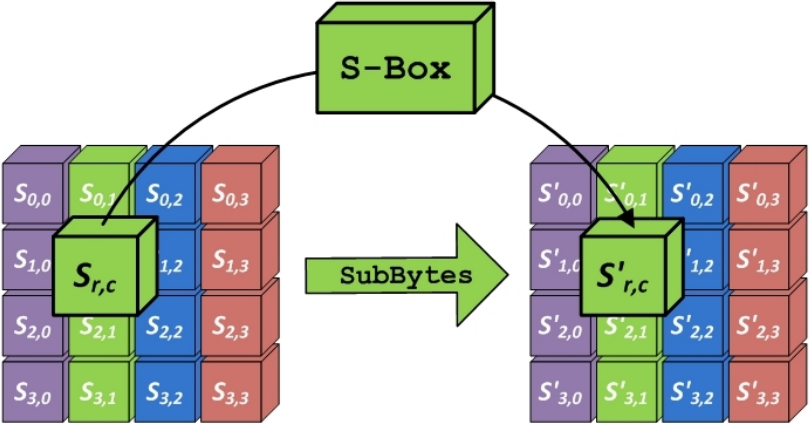
No AES as 16 **S-boxes** são idênticas (note que no DES todas eram diferentes).



The Advanced Encryption Standard (AES)

A **S-box** é indexada por 1 byte (8 bits) e produz como saída 1 byte (A_i e B_i são bytes!).

$$S(A_i) = B_i$$



The Advanced Encryption Standard (AES)

O elemento **S-box** é a única operação **não-linear** no AES, assim

$$\text{ByteSub}(A)+\text{ByteSub}(B) \neq \text{ByteSub}(A+B)$$

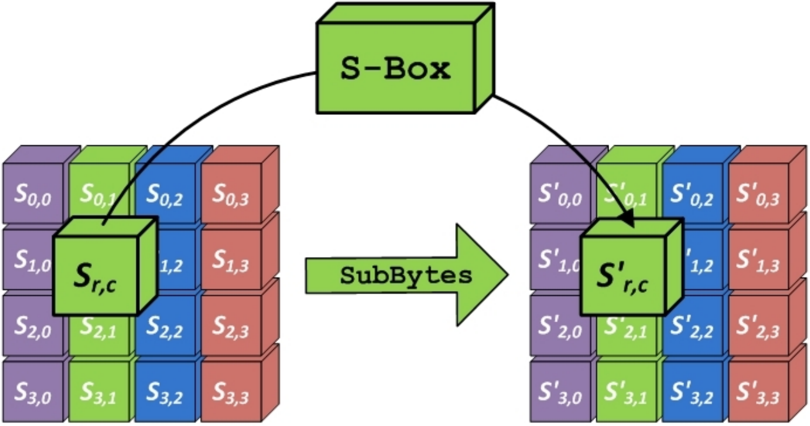


Tabela de substituição **S-box** para o AES!

	y: 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
x 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

$S(11000010)$?   (indexado por 1 byte!)

x \ y	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

$S(11000010) = S(C2)$

		y															
		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
x	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

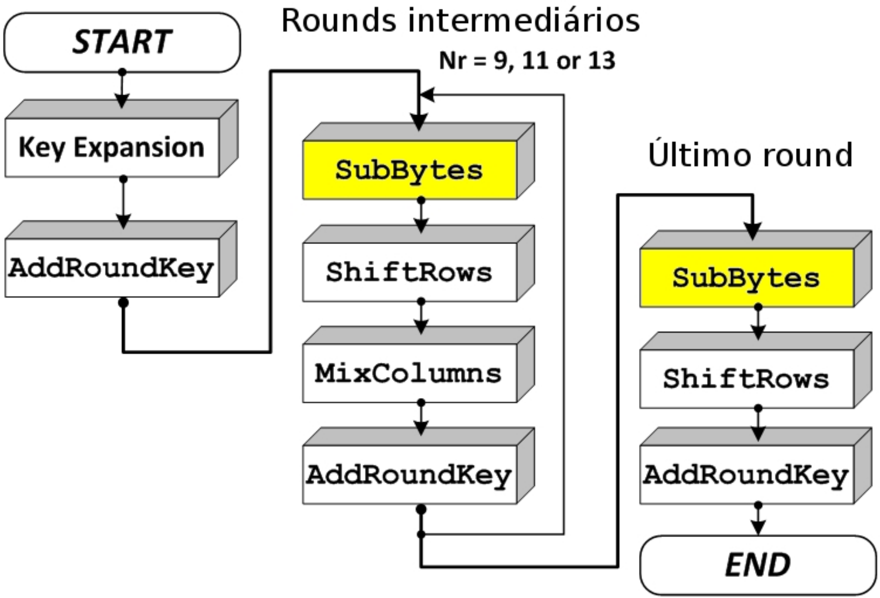
$S(11000010) = S(C2)$

		y															
		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
x	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

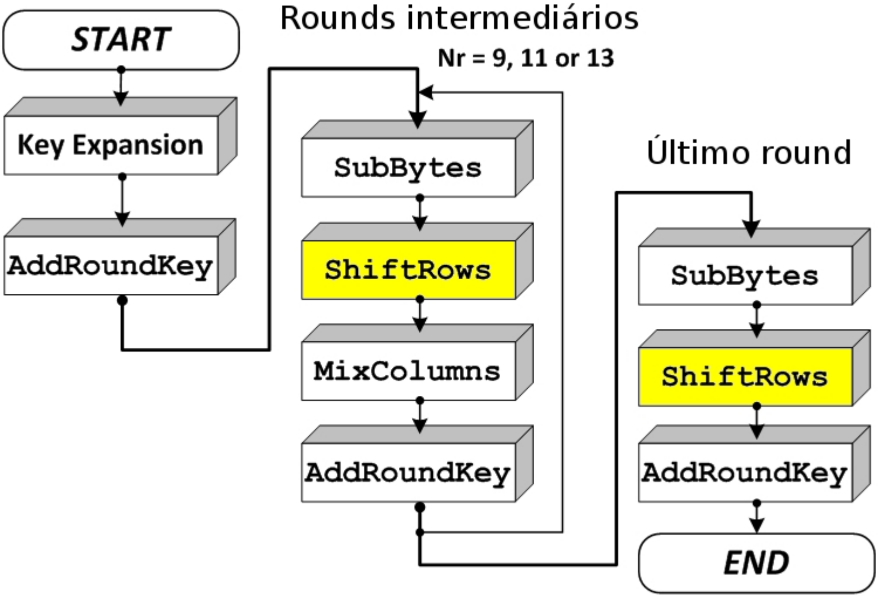
$S(C2) = 25 = 00100101.$

									y							
	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
x 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

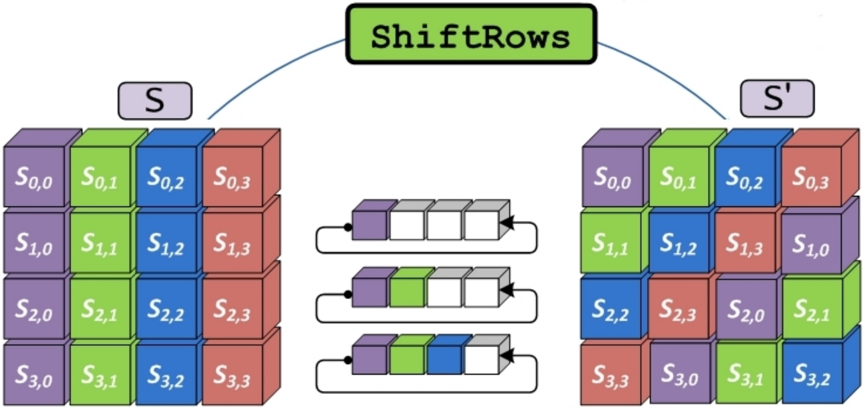
The Advanced Encryption Standard (AES)



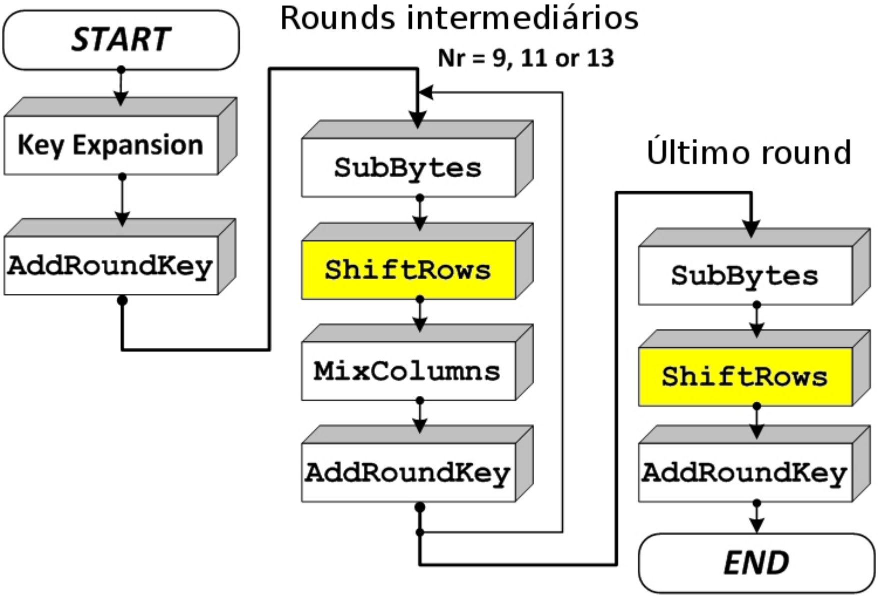
The Advanced Encryption Standard (AES)



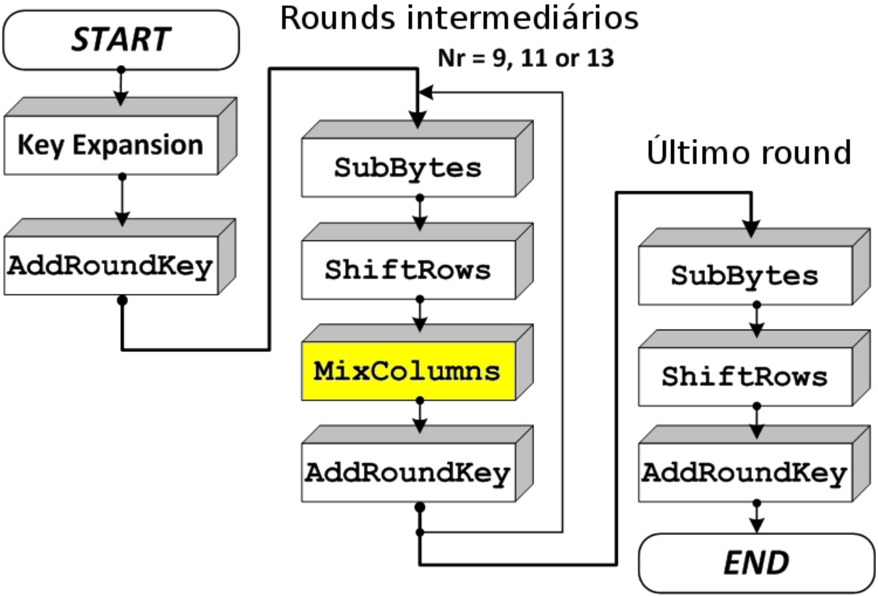
Elemento de Difusão



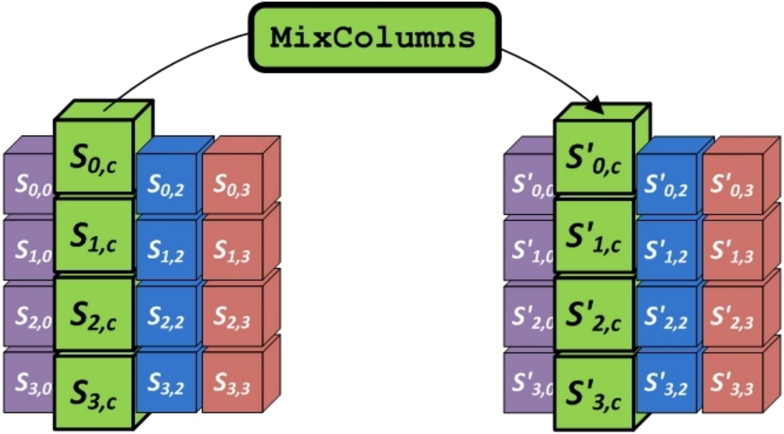
The Advanced Encryption Standard (AES)



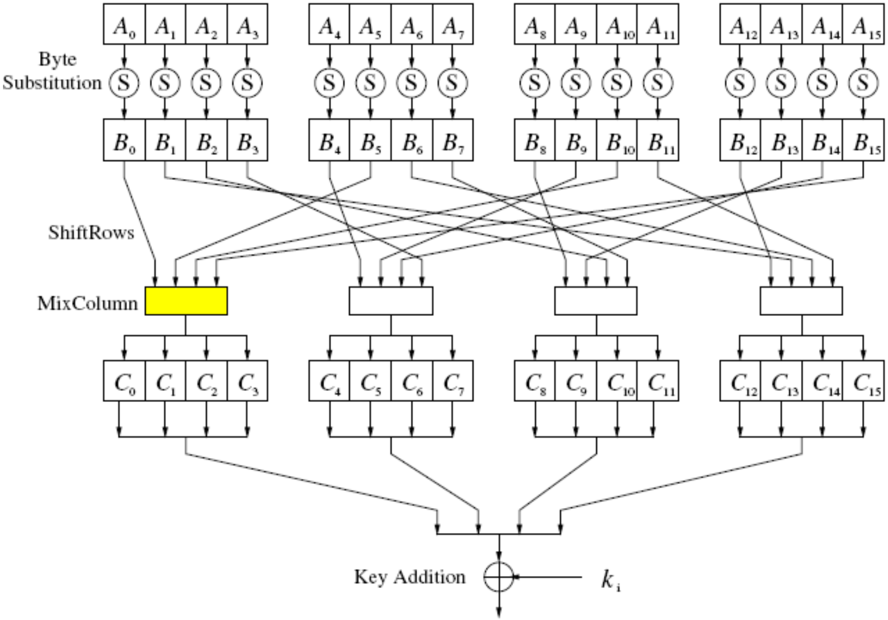
The Advanced Encryption Standard (AES)



The Advanced Encryption Standard (AES)



The Advanced Encryption Standard (AES)



Operação **MixColumn**

$$\begin{matrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{matrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{matrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{matrix}$$

Multiplicação no $GF(2^8)$

$$\begin{matrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{matrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{matrix} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{matrix}$$

Exemplo: multiplicação por um bloco de 25's.

$$\begin{array}{c} C_0 \\ C_1 \\ C_2 \\ C_3 \end{array} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{array}{c} B_0 \\ B_5 \\ B_{10} \\ B_{15} \end{array}$$

The Advanced Encryption Standard (AES)

Exemplo: multiplicação por um bloco de 25's.

$$\begin{matrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{matrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{matrix} 25 \\ 25 \\ 25 \\ 25 \end{matrix}$$

Exemplo: multiplicação por um bloco de 25's.

$$\begin{array}{c} C_0 \\ C_1 \\ C_2 \\ C_3 \end{array} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{array}{c} 25 \\ 25 \\ 25 \\ 25 \end{array}$$

$$\begin{aligned} 02 \cdot 25 &= x \cdot (x^5 + x^2 + 1) = x^6 + x^3 + x \\ 03 \cdot 25 &= (x+1) \cdot (x^5 + x^2 + 1) \\ &= (x^6 + x^3 + x) + (x^5 + x^2 + 1) \\ &= x^6 + x^5 + x^3 + x^2 + x + 1 \end{aligned}$$

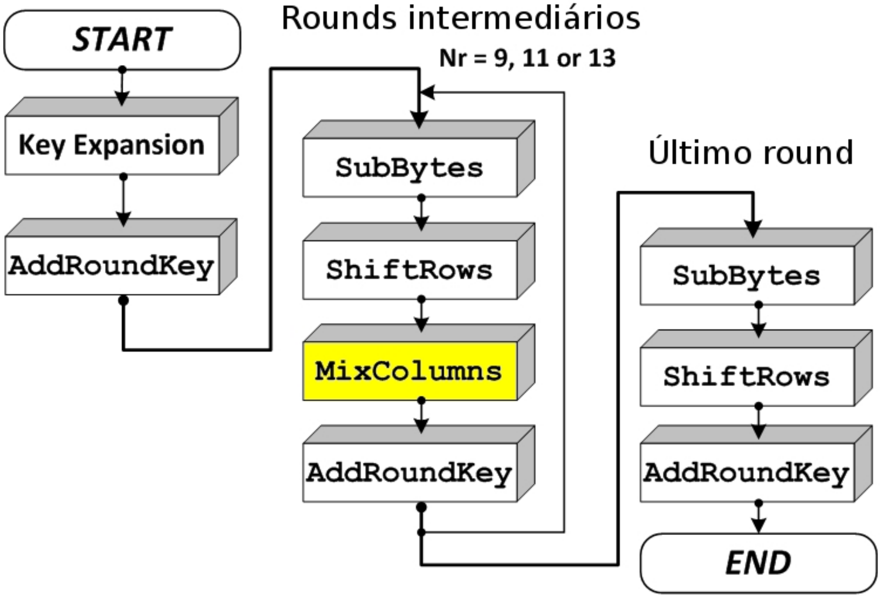
Suponha um bloco $B = (25, 25, \ldots, 25)$

$$
\begin{array}{rcrrrrrr}
01 \cdot 25 & = & & x^5 + & & x^2 + & & 1 \\
01 \cdot 25 & = & & x^5 + & & x^2 + & & 1 \\
02 \cdot 25 & = & x^6 + & & x^3 + & & x & \\
03 \cdot 25 & = & x^6 + & x^5 + & x^3 + & x^2 + & x + & 1 \\
\hline
C_i & = & & x^5 + & & x^2 + & & 1
\end{array}
$$

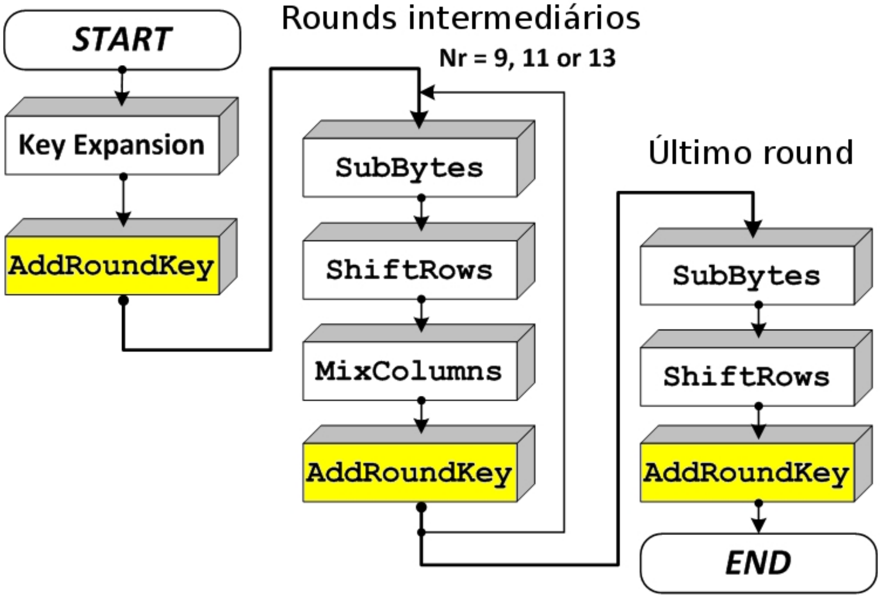
Resultado: $x^5 + x^2 + 1 = (25)_2$ para todo C_i.

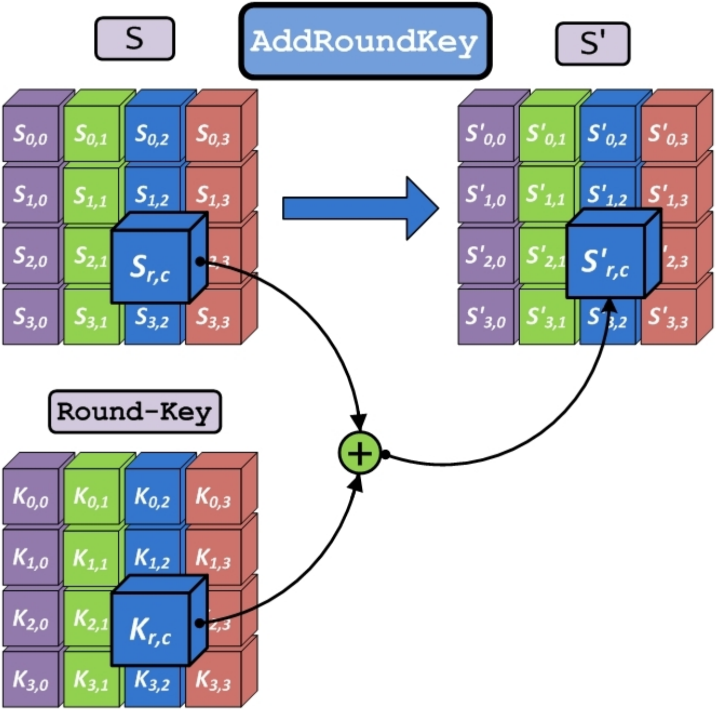
Se necessário, devemos usar redução modular por $P(x) = x^8 + x^4 + x^3 + x + 1$.

The Advanced Encryption Standard (AES)



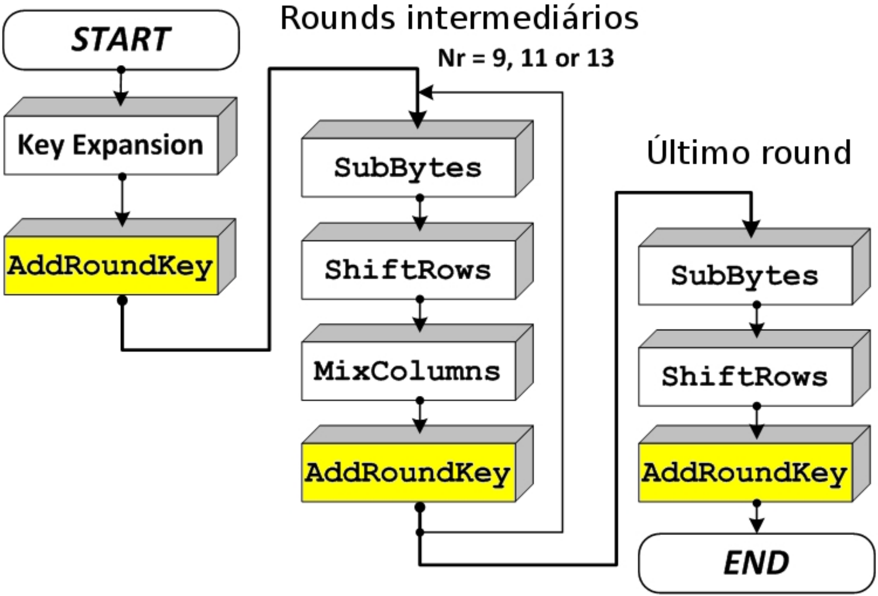
The Advanced Encryption Standard (AES)



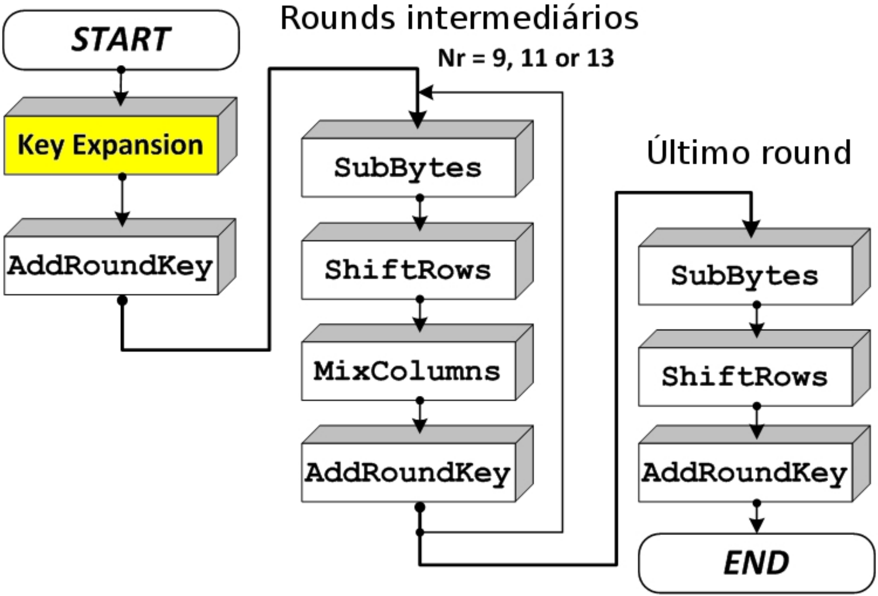

S
AddRoundKey
S'
$S_{0,0}$ $S_{0,1}$ $S_{0,2}$ $S_{0,3}$
$S_{1,0}$ $S_{1,1}$ $S_{1,2}$ $S_{1,3}$
$S_{2,0}$ $S_{2,1}$
$S_{3,0}$ $S_{3,1}$ $S_{3,2}$ $S_{3,3}$
$S_{r,c}$
$S'_{0,0}$ $S'_{0,1}$ $S'_{0,2}$ $S'_{0,3}$
$S'_{1,0}$ $S'_{1,1}$ $S'_{1,2}$ $S'_{1,3}$
$S'_{2,0}$ $S'_{2,1}$
$S'_{3,0}$ $S'_{3,1}$ $S'_{3,3}$
$S'_{r,c}$
Round-Key
$K_{0,0}$ $K_{0,1}$ $K_{0,2}$ $K_{0,3}$
$K_{1,0}$ $K_{1,1}$ $K_{1,2}$ $K_{1,3}$
$K_{2,0}$ $K_{2,1}$
$K_{3,0}$ $K_{3,1}$ $K_{3,2}$ $K_{3,3}$
$K_{r,c}$

Sumário

Key scheduling



Key scheduling



Key scheduling

O módulo **key schedule (expansion)** recebe uma chave do usuário de 128, 192 ou 256 bits e deriva **sub-chaves** de 128 bits para cada um dos **rounds**. O número de sub-chaves é igual ao número de rounds mais um, pois a primeira sub-chave não é manipulada (chave original do usuário). As chaves no AES são armazenadas e manipuladas na unidade de medida **word** (32 bits).

Key scheduling

A chave original é armazenada na posição $W[0], \ldots, W[3]$ do array (cada W com 32 bits)!

- **Array para chaves 128 bits**: $W[0], \ldots W[43]$
- **Array para chaves 192 bits**: $W[0], \ldots W[51]$
- **Array para chaves 256 bits**: $W[0], \ldots W[59]$

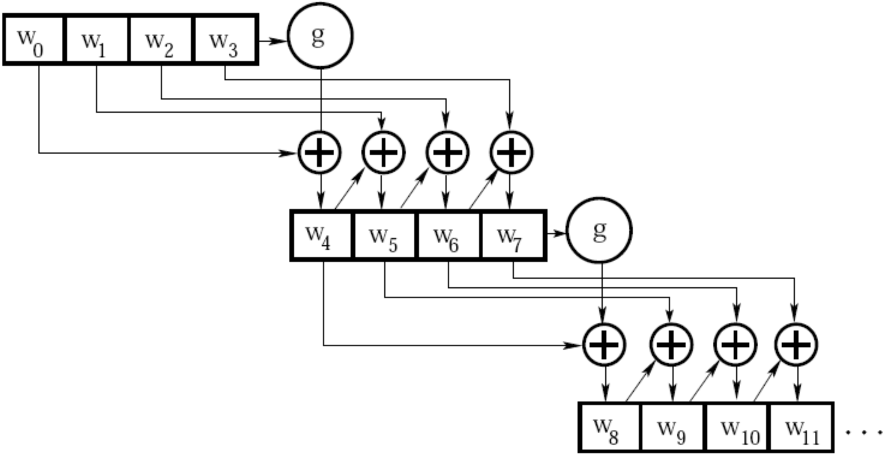
Key scheduling

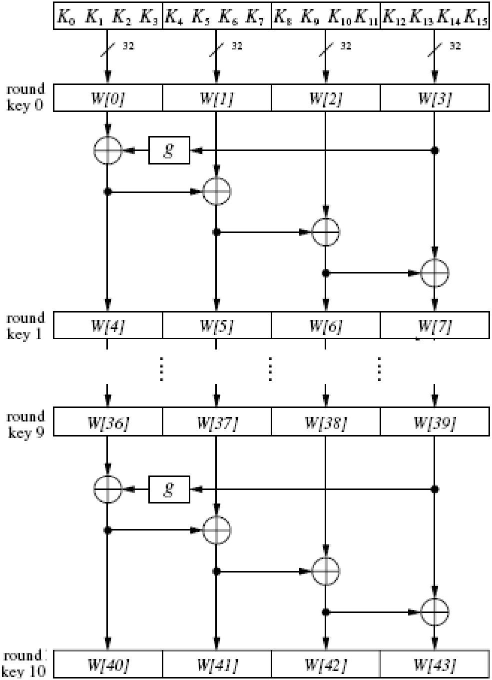
Questão: como obter as demais sub-chaves ($W[4], \ldots, W[43]$ ou $W[51]$ ou $W[59]$)?

- **Array para chaves 128 bits**: $W[0], \ldots W[43]$
- **Array para chaves 192 bits**: $W[0], \ldots W[51]$
- **Array para chaves 256 bits**: $W[0], \ldots W[59]$

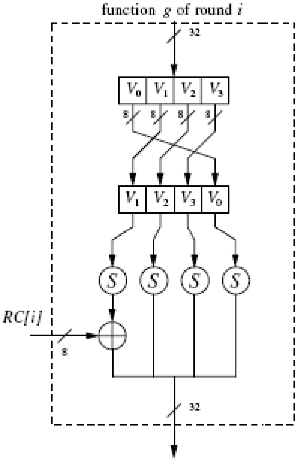
Key scheduling

Observe que as sub-chaves são calculadas recursivamente, para derivar k_i é necessário calcular k_{i-1}.



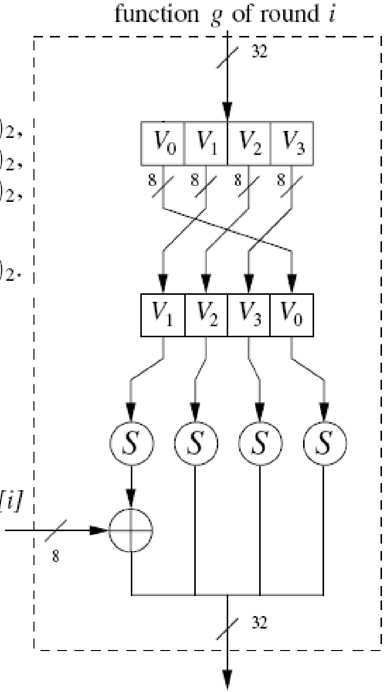


K0 K1 K2 K3 K4 K5 K6 K7 K8 K9 K10 K11 K12 K13 K14 K15
32
round key 0
W[0] W[1] W[2] W[3]
g
round key 1
W[4] W[5] W[6] W[7]
round key 9
W[36] W[37] W[38] W[39]
round key 10
W[40] W[41] W[42] W[43]



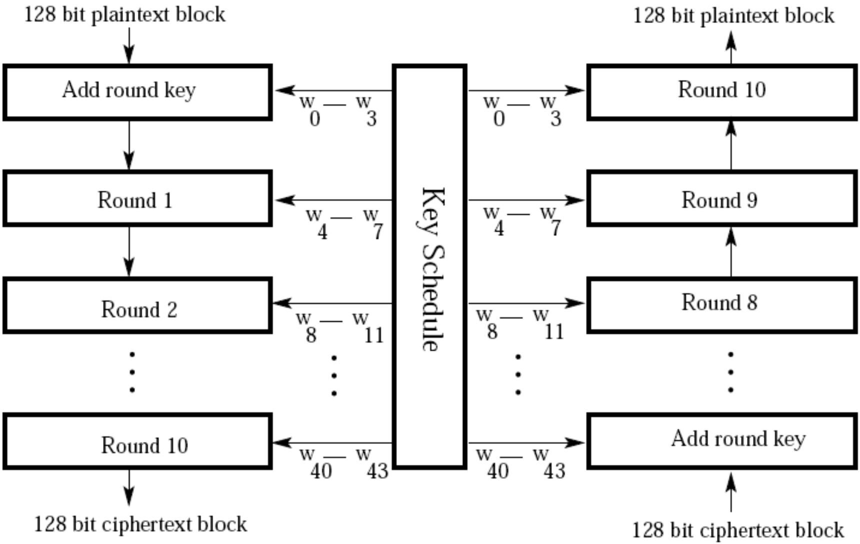
function g of round i
32
V0 V1 V2 V3
8
V1 V2 V3 V0
S
RC[i]

$$
\begin{aligned}
RC[1] &= x^0 = (0000\,0001)_2,\\
RC[2] &= x^1 = (0000\,0010)_2,\\
RC[3] &= x^2 = (0000\,0100)_2,\\
&\ \ \vdots\\
RC[10] &= x^9 = (0011\,0110)_2.
\end{aligned}
$$

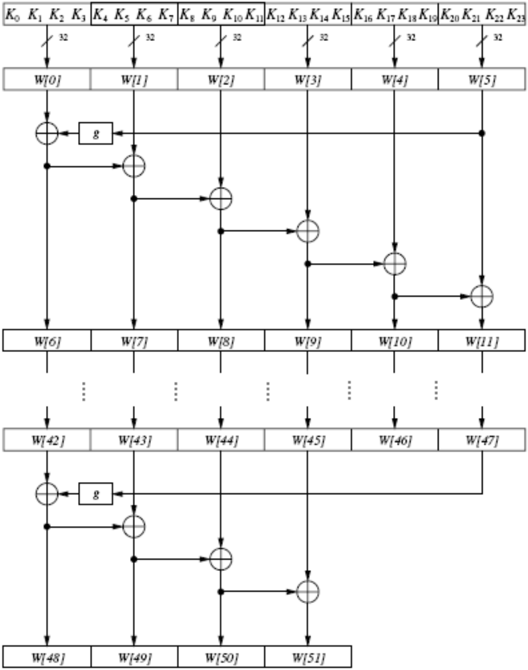


Key scheduling

$w[0] - w[3] = 128$ bits (4 palavras de 4 bytes).



Escalonamento para chaves de 192 bits (12 rounds)



Key scheduling

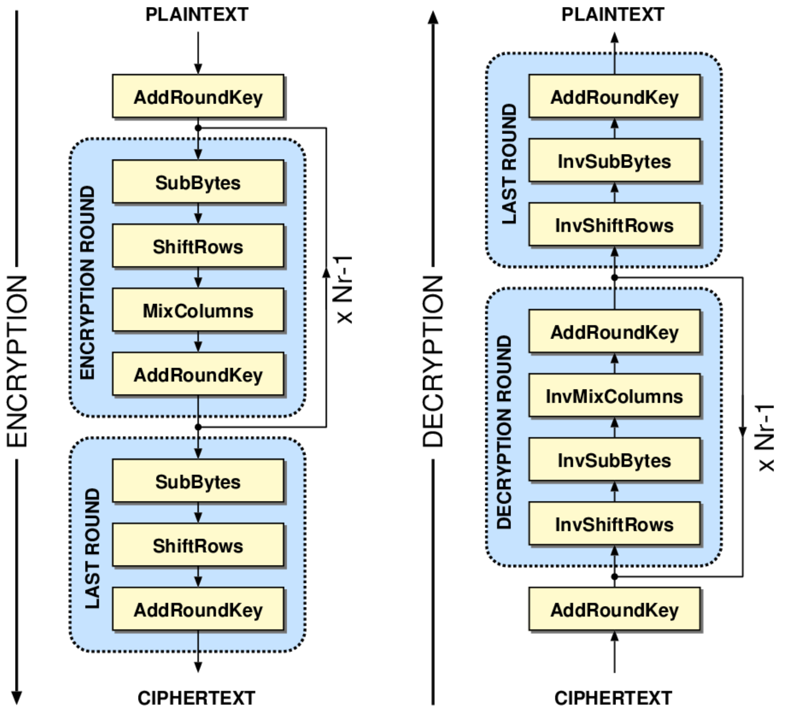
Cada sub-chave é composta por 4 palavras $W[i], W[i+1], W[i+2], W[i+3]$ diferentes.

- Chave de 128 bits:
  - $W[0] \dots W[3]$ no round inicial.
  - $W[4] \dots W[43]$ nos 10 rounds seguintes.
- Chave de 192 bits:
  - $W[0] \dots W[3]$ no round inicial.
  - $W[4] \dots W[51]$ nos 12 rounds seguintes.
- Chave de 256 bits:
  - $W[0] \dots W[3]$ no round inicial.
  - $W[4] \dots W[59]$ nos 14 rounds seguintes.

Sumário

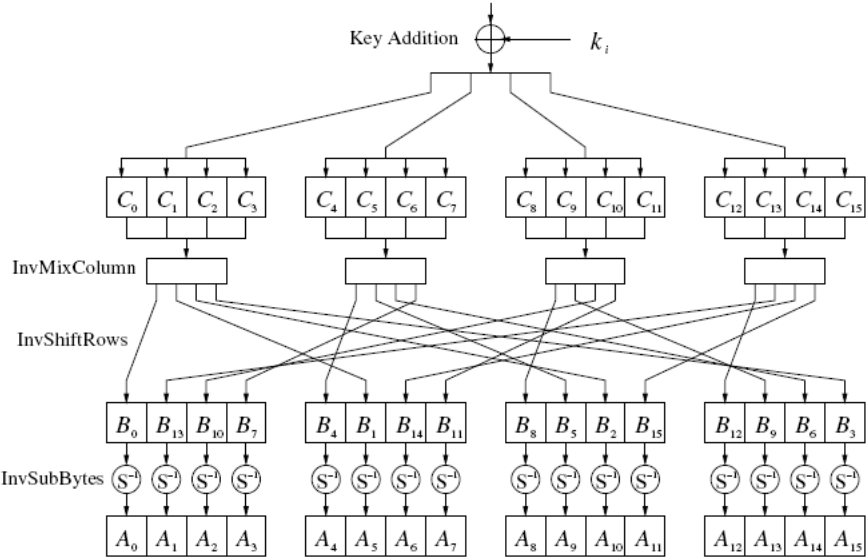
Key scheduling

A algoritmo AES NÃO utiliza um rede de Feistel, desta forma, para a decifragem todos os layers necessitam ser **invertidos**!

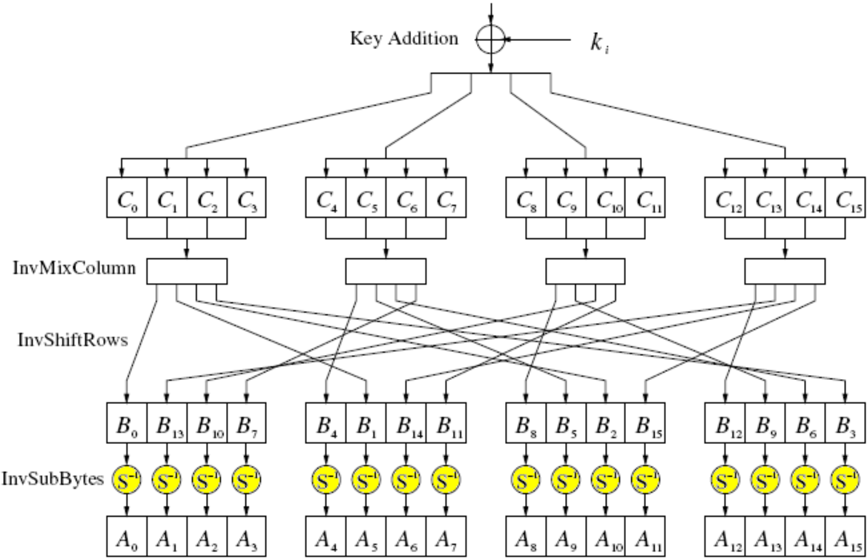


ENCRYPTION
PLAINTEXT
AddRoundKey
ENCRYPTION ROUND
SubBytes
ShiftRows
MixColumns
AddRoundKey
x Nr-1
LAST ROUND
SubBytes
ShiftRows
AddRoundKey
CIPHERTEXT
DECRYPTION
PLAINTEXT
LAST ROUND
AddRoundKey
InvSubBytes
InvShiftRows
DECRYPTION ROUND
AddRoundKey
InvMixColumns
InvSubBytes
InvShiftRows
x Nr-1
AddRoundKey
CIPHERTEXT

The Advanced Encryption Standard (AES)



The Advanced Encryption Standard (AES)

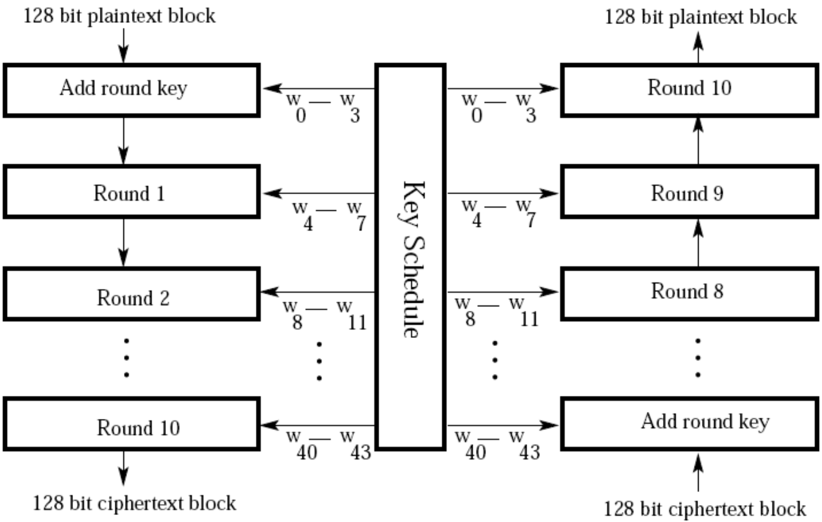


The Advanced Encryption Standard (AES)

								y								
		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
x	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

The Advanced Encryption Standard (AES)

As sub-chaves são utilizadas em ordem inversa no deciframento:



The Advanced Encryption Standard (AES)

Na prática, todas as sub-chaves são calculadas da mesma maneira que no ciframento, armazenadas em um array e utilizadas na ordem inversa. Esse processo produz uma pequena latência no deciframento que não existe no ciframento.

Sumário

Porque o valor **53** resulta em **ED** na Sbox?

									y								
		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
x	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

$\mathbf{53} = 01010011 = x^6 + x^4 + x + 1$

x \ y	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

The Advanced Encryption Standard (AES)

Qual o inverso multiplicativo de $x^6 + x^4 + x + 1$?

$x^6 + x^4 + x + 1$		

The Advanced Encryption Standard (AES)

No AES o polinômio irredutível é $x^8+x^4+x^3+x+1$.

x^6+x^4+x+1		

The Advanced Encryption Standard (AES)

No AES o polinômio irredutível é $x^8 + x^4 + x^3 + x + 1$.

$x^8 + x^4 + x^3 + x + 1$ $x^6 + x^4 + x + 1$		

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		
$x^6 + x^4 + x + 1$		
	$x^2 + 1$	

The Advanced Encryption Standard (AES)

$$
\begin{array}{l|c|l}
x^8 + x^4 + x^3 + x + 1 & & \\
{\color{blue} x^6 + x^4 + x + 1} & & \\
\hline
 & {\color{blue} x^2 + 1} & \\
 & & \\
\end{array}
$$

$$
\begin{aligned}
&= (x^6 + x^4 + x + 1) \times (x^2 + 1) \\
&= x^8 + x^6 + x^6 + x^4 + x^3 + x + x^2 + 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$ $x^6 + x^4 + x + 1$		
	$x^2 + 1$	

$$
\begin{aligned}
&= (x^6 + x^4 + x + 1) \times (x^2 + 1) \\
&= x^8 + x^4 + x^3 + x + x^2 + 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$$
\begin{array}{l|l|l}
x^8 + x^4 + x^3 + x + 1 & & \\
x^6 + x^4 + x + 1 & & \\
\hline
 & x^2 + 1 & \\
 & & \\
\end{array}
$$

$$
\begin{aligned}
&= (x^6 + x^4 + x + 1) \times (x^2 + 1) \\
&= x^8 + x^4 + x^3 + x + x^2 + 1 \\
&= x^8 + x^4 + x^3 + x + 1 \\
\hline
&= x^2
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		
$x^6 + x^4 + x + 1$		
x^2	$x^2 + 1$	

$$
\begin{aligned}
&= (x^6 + x^4 + x + 1) \times (x^2 + 1) \\
&= x^8 + x^4 + x^3 + x + x^2 + 1 \\
&= x^8 + x^4 + x^3 + x + 1 \\
\hline
&= x^2
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		
$x^6 + x^4 + x + 1$		
x^2	$x^2 + 1$	
	$x^4 + x^2$	

$$
\begin{array}{l|l|l}
x^8 + x^4 + x^3 + x + 1 & & \\
x^6 + x^4 + x + 1 & & \\
\hline
\color{blue}{x^2} & x^2 + 1 & \\
 & \color{blue}{x^4 + x^2} & \\
 & & \\
\end{array}
$$

$$
\begin{aligned}
&= (x^2) \times (x^4 + x^2) \\
&= x^6 + x^4
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$ $x^6 + x^4 + x + 1$		
x^2	$x^2 + 1$ $x^4 + x^2$	

$$
\begin{aligned}
&= (x^2) \times (x^4 + x^2) \\
&= x^6 + x^4 \\
&= x^6 + x^4 + x + 1 \\
\hline
&= x + 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		
$x^6 + x^4 + x + 1$		
x^2	$x^2 + 1$	
$x + 1$	$x^4 + x^2$	

$$
\begin{aligned}
&= (x^2) \times (x^4 + x^2) \\
&= x^6 + x^4 \\
&= x^6 + x^4 + x + 1 \\
\hline
&= x + 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		
$x^6 + x^4 + x + 1$		
x^2	$x^2 + 1$	
$x + 1$	$x^4 + x^2$	
	$x + 1$	

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		
$x^6 + x^4 + x + 1$		
x^2	$x^2 + 1$	
$x + 1$	$x^4 + x^2$	
	$x + 1$	

$$
\begin{aligned}
&= (x+1) \times (x+1) \\
&= x^2 + x + x + 1
\end{aligned}
$$

$x^8 + x^4 + x^3 + x + 1$		
$x^6 + x^4 + x + 1$		
x^2	$x^2 + 1$	
$x + 1$	$x^4 + x^2$	
	$x + 1$	

$$\begin{aligned} &= (x+1) \times (x+1) \\ &= x^2 + 1 \end{aligned}$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		
$x^6 + x^4 + x + 1$		
x^2	$x^2 + 1$	
$x + 1$	$x^4 + x^2$	
	$x + 1$	

$$
\begin{aligned}
&= (x+1) \times (x+1) \\
&= x^2 + 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		
$x^6 + x^4 + x + 1$		
x^2	$x^2 + 1$	
$x + 1$	$x^4 + x^2$	
	$x + 1$	

$$
\begin{aligned}
&= (x+1) \times (x+1) \\
&= x^2 + 1 \\
&= x^2 \\
&= 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		
$x^6 + x^4 + x + 1$		
x^2	$x^2 + 1$	
$x + 1$	$x^4 + x^2$	
1	$x + 1$	

$$
\begin{aligned}
&= (x+1) \times (x+1) \\
&= x^2 + 1 \\
&= x^2 \\
&= 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$$
\begin{array}{l|l|l}
x^8 + x^4 + x^3 + x + 1 & & 0 \\
x^6 + x^4 + x + 1 & & 1 \\
\hline
x^2 & x^2 + 1 & \\
x + 1 & x^4 + x^2 & \\
1 & x + 1 &
\end{array}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	
$x + 1$	$x^4 + x^2$	
1	$x + 1$	

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	
$x + 1$	$x^4 + x^2$	
1	$x + 1$	

$$
\begin{aligned}
&= (x^2 + 1) \times 1 + 0 \\
&= x^2 + 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	$x^2 + 1$
$x + 1$	$x^4 + x^2$	
1	$x + 1$	

$$
\begin{aligned}
&= (x^2 + 1) \times 1 + 0 \\
&= x^2 + 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	$x^2 + 1$
$x + 1$	$x^4 + x^2$	
1	$x + 1$	

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	$x^2 + 1$
$x + 1$	$x^4 + x^2$	
1	$x + 1$	

$$
\begin{aligned}
&= (x^4 + x^2) \times (x^2 + 1) + 1 \\
&= x^6 + x^4 + x^4 + x^2 + 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8+x^4+x^3+x+1$		0
x^6+x^4+x+1		1
x^2	x^2+1	x^2+1
$x+1$	x^4+x^2	
1	$x+1$	

$$
\begin{aligned}
&= (x^4+x^2)\times(x^2+1)+1 \\
&= x^6+x^2+1
\end{aligned}
$$

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	$x^2 + 1$
$x + 1$	$x^4 + x^2$	$x^6 + x^2 + 1$
1	$x + 1$	

$$\begin{aligned} &= (x^4 + x^2) \times (x^2 + 1) + 1 \\ &= x^6 + x^2 + 1 \end{aligned}$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	$x^2 + 1$
$x + 1$	$x^4 + x^2$	$x^6 + x^2 + 1$
1	$x + 1$	

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	$x^2 + 1$
$x + 1$	$x^4 + x^2$	$x^6 + x^2 + 1$
1	$x + 1$	

$$
\begin{aligned}
&= (x+1) \times (x^6 + x^2 + 1) + x^2 + 1 \\
&= x^7 + x^3 + x + x^6 + x^2 + 1 + x^2 + 1
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	$x^2 + 1$
$x + 1$	$x^4 + x^2$	$x^6 + x^2 + 1$
1	$x + 1$	

$$
\begin{aligned}
&= (x+1) \times (x^6 + x^2 + 1) + x^2 + 1 \\
&= x^7 + x^3 + x^6 + x
\end{aligned}
$$

The Advanced Encryption Standard (AES)

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	$x^2 + 1$
$x + 1$	$x^4 + x^2$	$x^6 + x^2 + 1$
1	$x + 1$	$x^7 + x^6 + x^3 + x$

$$
\begin{aligned}
&= (x+1) \times (x^6 + x^2 + 1) + x^2 + 1 \\
&= x^7 + x^3 + x^6 + x
\end{aligned}
$$

The Advanced Encryption Standard (AES)

O inverso multiplicativo é $x^7 + x^6 + x^3 + x$.

$x^8 + x^4 + x^3 + x + 1$		0
$x^6 + x^4 + x + 1$		1
x^2	$x^2 + 1$	$x^2 + 1$
$x + 1$	$x^4 + x^2$	$x^6 + x^2 + 1$
1	$x + 1$	$x^7 + x^6 + x^3 + x$

The Advanced Encryption Standard (AES)

$$x^7 + x^6 + x^3 + x = 11001010$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \bmod 2$$

The Advanced Encryption Standard (AES)

$$x^7 + x^6 + x^3 + x = 11001010$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \bmod 2$$

The Advanced Encryption Standard (AES)

$$x^7 + x^6 + x^3 + x = 11001010$$

$$\begin{pmatrix} 2 \\ 3 \\ 3 \\ 3 \\ 2 \\ 2 \\ 2 \\ 3 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \mathrm{mod} 2$$

The Advanced Encryption Standard (AES)

$$x^7 + x^6 + x^3 + x = 11001010$$

$$\begin{pmatrix} 3 \\ 4 \\ 3 \\ 3 \\ 2 \\ 3 \\ 3 \\ 3 \end{pmatrix} \mathrm{mod} 2$$

The Advanced Encryption Standard (AES)

$$x^7 + x^6 + x^3 + x = 11001010$$

$$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Inverso de:

$x^6 + x^4 + x + 1 = 01010011\ (0 \times 53)$

Resultado: $11101101\ (0 \times \mathrm{ED})$

$$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

The Advanced Encryption Standard (AES)

										y							
		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
x	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

Considerações

O algoritmo AES não se baseia em nenhum problema matemático de difícil solução. A substituição é uma transformação não linear que introduz o conceito de confusão na cifra. A transformação não linear, essencial em toda cifra moderna, é provada ser uma primitiva criptográfica forte contra a criptoanálise linear e diferencial. A substituição no AES está presente na S-Box (Substitution Box).

Xuanping Zhang, Zhongmeng Zhao e Jiayin Wang. **Chaotic image encryption based on circular substitution box and key stream buffer**, Elsevier. 2014.