Criptografia FIB

Advanced Encryption Standard

Anna Rio

Departament de Matemàtica Aplicada II • Universitat Politècnica de Catalunya

AES: Advanced Encryption Standard

El 12 de setembre de 1997 NIST fa una crida pública per a la presentació d'algoritmes candidatas a convertir-se en el *Advanced Encryption Standard*

Requisits mínims

1. L'algoritme ha d'ésser de clau secreta (simètric) i de xifratge en bloc
2. L'algoritme ha de poder suportar les combinacions clau-bloc dels tamanys 128-128, 192-128 i 256-128

AES: Criteris d'avaluació

- Seguretat: és el factor més important en l'avaluació dels candidats
- Cost: l'algoritme ha de
  - ser accesible per a tothom i de lliure distribució
  - ser computacionalment eficient, en *hardware* i en *software*
  - utilitzar la menor quantitat de memòria possible, en *hardware* i en *software*
- Característiques d'implemetació de l'algoritme:
  - Fàcilment implementable en diferents plataformes, en *hardware* i en *software*
  - Adaptable a diferents combinacions clau-bloc, a més de les mínimes requerides
  - De disseny simple

`http://csrc.nist.gov/CryptoToolkit/aes/pre-round1/aes_9709.htm`

CANDIDATS AL AES

Agost de 1998: Primera fase de selecció (15 candidats)

`http://csrc.nist.gov/CryptoToolkit/aes/round1/round1.htm`

- **CAST-256**, Entrust Technologies, Inc. (C. Adams)
- **CRYPTON**, Future Systems, Inc. (Chae Hoon Lim)
- **DEAL**, L. Knudsen, R. Outerbridge
- **DFC**, CNRS-Ecole Normale Superiere (S. Vaudenay)
- **E2**, NTT *Nippon Telegraph and Telephone Corporation* (M. Kanda)
- **FROG**, TecApro International S.A. (D. Georgoudis, Leroux, Chaves)
- **HPC**, R. Schoeppel
- **LOKI97**, L. Brown, J. Pieprzyk, J.Seberry
- **MAGENTA**, Deutshe Telekom AG (K. Huber)

Candidats al AES

- **MARS***, IBM (N. Zunic)
- **RC6***, RSA Laboratories (R. Rivest, M. Robshaw, Sidney, Yin)
- **RIJNDAEL***, J. Daemen, V. Rijmen
- **SAFER+**, Cylink Corporation (L. Chen)
- **SERPENT***, R. Anderson, E. Biham, L. Knudsen
- **TWOFISH***, B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson

Agost de 1999: segona fase de selecció (5 candidats)

`http://csrc.nist.gov/CryptoToolkit/aes/round2/round2.htm`

Octubre de 2000: L'escollit és Rijndael

Novembre de 2001: Es publica el FIPS-197

AES: Advanced Encryption Standard

L'any 2001, l'algoritme RIJNDAEL, dissenyat per Joan Daemen (1965) i Vincent Rijmen (1970)


de la Universitat Catòlica de Leuven (Bèlgica), es converteix en el nou estàndard

AES: Advanced Encryption Standard

- Algoritme simètric de bloc de 128 bits i clau de 128, 192 o 256 bits
- Les transformacions es fan sobre la matriu d'estat, una matriu 4×4, els coeficients de la qual són bytes
- Realitza operacions al cos finit $GF(2^8)$ i a l'espai vectorial de dimensió 4 sobre aquest cos

RIJNDAEL-AES

http://csrc.nist.gov/CryptoToolkit/aes/

Algoritme simètric de bloc de 128 bits i clau de 128, 192 o 256 bits. (AES-128, AES-192, AES-256)

L'algoritme realitza operacions amb bytes i amb vectors de 4 bytes. En el conjunt dels bytes (de 256 elements) tenim

- una operació suma: xor bit a bit o suma de vectors binaris
- una operació producte: interpretem un byte com a polinomi binari

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

i multipliquem polinomis reduïnt mòdul $x^8 + x^4 + x^3 + x + 1$

Estructura de cos: GF(2^8)

PRODUCTE AL COS GF(2^8)

Producte de polinomis mòdul $x^8 + x^4 + x^3 + x + 1$

$$(x^7 + x^6 + x^4 + x + 1)(x^5 + x^2 + x) = x^{12} + x^{11} + x^7 + x^3 + x$$

$$\text{mod } x^8 + x^4 + x^3 + x + 1 = x^7 + x^6 + x^5 + x^4 + x^3 + 1$$

$$(x^7 + x^6 + x^4 + x + 1) \bullet (x^5 + x^2 + x) = x^7 + x^6 + x^5 + x^4 + x^3 + 1$$

$$11010011 \bullet 00100110 = 11111001$$

$$0\text{x}d3 \bullet 0\text{x}26 = 0\text{x}f9$$

PRODUCTE AL COS GF(2^8)

Producte de polinomis mòdul $x^8 + x^4 + x^3 + x + 1$

$$(x^7 + x^6 + x^4 + x + 1)(x^5 + x^2 + x) = x^{12} + x^{11} + x^7 + x^3 + x$$

$$\text{mod } x^8 + x^4 + x^3 + x + 1 = x^7 + x^6 + x^5 + x^4 + x^3 + 1$$

$$\begin{aligned} (x^7 + x^6 + x^4 + x + 1) \bullet (x^5 + x^2 + x) &= x^7 + x^6 + x^5 + x^4 + x^3 + 1 \\ 11010011 \bullet 00100110 &= 11111001 \\ 0\text{x}d3 \bullet 0\text{x}26 &= 0\text{x}f9 \end{aligned}$$

$0\text{x}03 = 00000011 = x + 1$ és un generador

$$
\begin{array}{lll}
(x+1)^2 & = x^2 + 1 & = 00000101 \quad = 0\text{x}05 \\
(x+1)^3 & = x^3 + x^2 + x + 1 & = 00001111 \quad = 0\text{x}0f \\
(x+1)^4 & = x^4 + 1 & = 00010001 \quad = 0\text{x}11 \\
\ldots & & \\
(x+1)^7 & = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & = 11111111 \quad = 0\text{x}ff \\
(x+1)^8 & = x^4 + x^3 + x & = 00011010 \quad = 0\text{x}1a \\
\ldots & & \\
\ldots & & \\
(x+1)^{255} & = 1 & = 00000001 \quad = 0\text{x}01
\end{array}
$$

GF(256) GENERAT PER $0x03 = x + 1$

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

Producte i inversos a GF(2^8)

Producte

$$\begin{aligned} 00111000 = 38 &= \text{element } 18 \\ 11100100 = e4 &= \text{element } 35 \\ 0\text{x}38 \bullet 0\text{x}e4 &= \text{element } 18 + 35 = 0\text{x}3c \end{aligned}$$

Inversos

$0\text{x}05$ està a la posició 2 $\Rightarrow$ el seu invers el trobem a la posició 255-2

$$0\text{x}05^{-1} = 0\text{x}52$$

No depèn del generador

Si prenem com a generador $x^2 + 1 = 0\text{x}05$

05	11	55	1a	72	a1	13	5f	38	d8	95	f7	06	1e	66	e5
5c	37	eb	6a	d9	90	e6	53	04	14	44	4f	68	d3	b2	4c
67	e0	4d	62	f1	18	78	83	b9	6b	dc	81	b3	49	76	b5
57	10	50	0b	27	bb	61	fe	2b	87	ad	2f	93	e9	60	fb
3a	d2	b7	5d	32	fa	3f	c3	e2	47	40	5b	2c	9c	da	9f
d5	ac	2a	82	bc	7a	89	9b	c1	e8	65	ea	6f	c8	c5	fc
21	a5	07	1b	77	b0	46	45	4a	79	86	a8	3e	c6	f3	12
5a	29	8d	8f	85	a7	0d	39	dd	84	a2	1c	6c	c7	f6	03
0f	33	ff	2e	96	f8	35	e1	48	73	a4	02	0a	22	aa	34
e4	59	26	be	70	ab	31	f5	0c	3c	cc	d1	b8	6e	cd	d4
a9	3b	d7	a6	08	28	88	9e	d0	bd	7f	98	ce	db	9a	c4
f9	30	f0	1d	69	d6	a3	19	7d	92	ec	71	ae	20	a0	16
4e	6d	c2	e7	56	15	41	5e	3d	c9	c0	ed	74	bf	75	ba
64	ef	7e	9d	df	8e	80	b6	58	23	af	25	b1	43	54	1f
63	f4	09	2d	99	cb	ca	cf	de	8b	91	e3	42	51	e	36
ee	7b	8c	8a	94	f2	17	4b	7c	97	fd	24	b4	52	01	

Producte i inversos

Producte

$$\begin{aligned} 00111000 = 38 &= \text{element } 9 \\ 11100100 = e4 &= \text{element } 145 \\ 0x38 \bullet 0xe4 &= \text{element } 145 + 9 = 0x3c \end{aligned}$$

Inversos

$0x05$ està a la posició 1 $\Rightarrow$ el seu invers el trobem a la posició 255-1

$$0x05^{-1} = 0x52$$

Sí depèn del mòdul $x^8 + x^4 + x^3 + x + 1$

Si treballem mòdul $x^8 + x^4 + x^3 + x^2 + 1$
podem prendre $x = 0\text{x}02$ com a generador

02	04	08	10	20	40	80	1d	3a	74	e8	cd	87	13	26	4c
98	2d	5a	b4	75	ea	c9	8f	03	06	0c	18	30	60	c0	9d
27	4e	9c	25	4a	94	35	6a	d4	b5	77	ee	c1	9f	23	46
8c	05	0a	14	28	50	a0	5d	ba	69	d2	b9	6f	de	a1	5f
be	61	c2	99	2f	5e	bc	65	ca	89	0f	1e	3c	78	f0	fd
e7	d3	bb	6b	d6	b1	7f	fe	e1	df	a3	5b	b6	71	e2	d9
af	43	86	11	22	44	88	0d	1a	34	68	d0	bd	67	ce	81
1f	3e	7c	f8	ed	c7	93	3b	76	ec	c5	97	33	66	cc	85
17	2e	5c	b8	6d	da	a9	4f	9e	21	42	84	15	2a	54	a8
4d	9a	29	52	a4	55	aa	49	92	39	72	e4	d5	b7	73	e6
d1	bf	63	c6	91	3f	7e	fc	e5	d7	b3	7b	f6	f1	ff	e3
db	ab	4b	96	31	62	c4	95	37	6e	dc	a5	57	ae	41	82
19	32	64	c8	8d	07	0e	1c	38	70	e0	dd	a7	53	a6	51
a2	59	b2	79	f2	f9	ef	c3	9b	2b	56	ac	45	8a	09	12
24	48	90	3d	7a	f4	f5	f7	f3	fb	eb	cb	8b	0b	16	2c
58	b0	7d	fa	e9	cf	83	1b	36	6c	d8	ad	47	8e	01	

Producte i inversos

Producte

$$\begin{aligned} 00111000 = 38 &= \text{element } 201 \\ 11100100 = e4 &= \text{element } 156 \\ 0\text{x}38 \bullet 0\text{x}e4 &= \text{element } 357 - 255 = \text{element } 102 = 0\text{x}44 \end{aligned}$$

Inversos

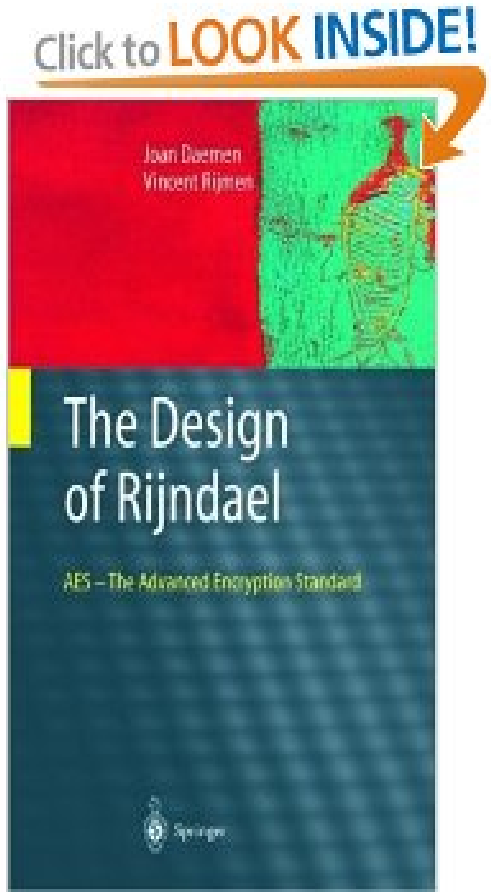
$0\text{x}05$ està a la posició 50 $\Rightarrow$ el seu invers el trobem a la posició 255-50

$$0\text{x}05^{-1} = 0\text{x}a7$$

AES especifica el mòdul

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

Podem usar la primera o la segona ordenació però no la tercera!



RIJNDAEL-AES: Paràmetres i tipus de dades

- N_k és el nombre de bits de la clau dividit por 32
- El nombre de voltes, N_r, depèn de la longitud de la clau:

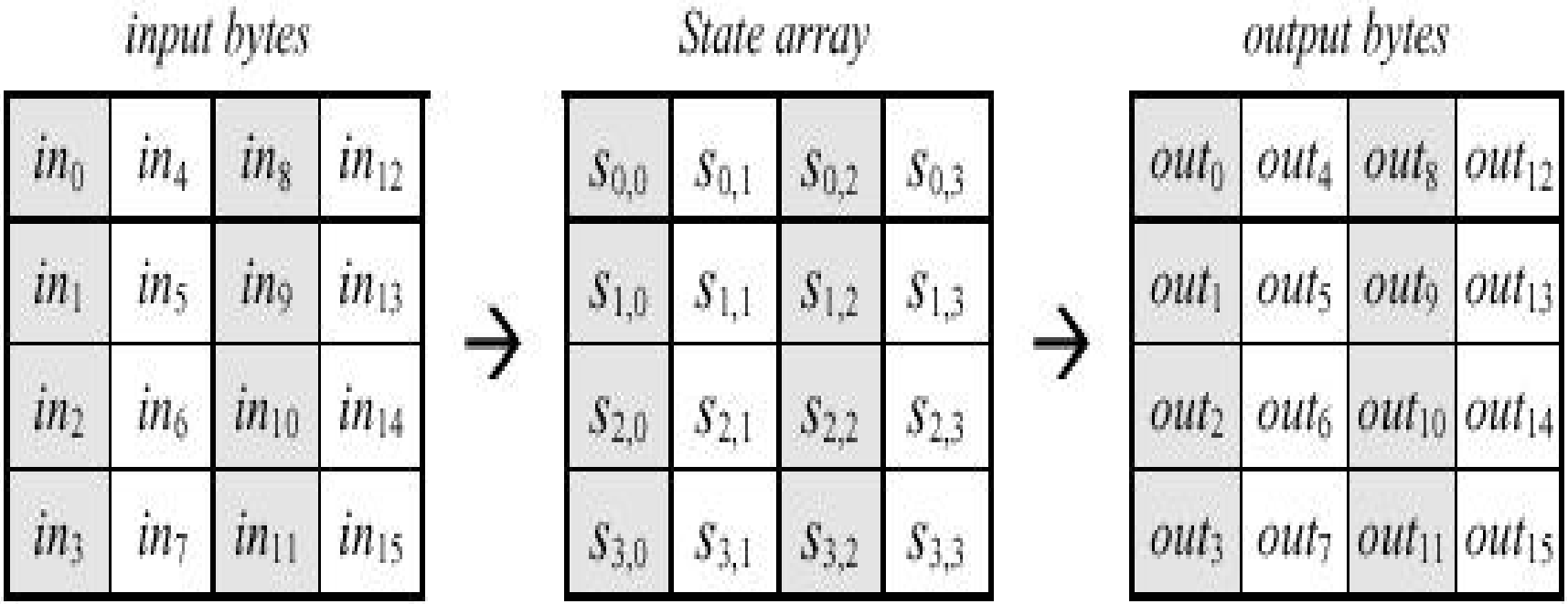
$$N_k = \begin{cases} 128/32 = 4 \Rightarrow N_r = 10 \\ 192/32 = 6 \Rightarrow N_r = 12 \\ 256/32 = 8 \Rightarrow N_r = 14 \end{cases}$$

Les diferents transformacions es fan sobre la matriu d'estat

$m_{0,0}$	$m_{0,1}$	$m_{0,2}$	$m_{0,3}$
$m_{1,0}$	$m_{1,1}$	$m_{1,2}$	$m_{1,3}$
$m_{2,0}$	$m_{2,1}$	$m_{2,2}$	$m_{2,3}$
$m_{3,0}$	$m_{3,1}$	$m_{3,2}$	$m_{3,3}$

que s'inicialitza amb el bytes del bloc: $m_{0,0}\, m_{1,0}\, m_{2,0} \ldots m_{3,3} = B$

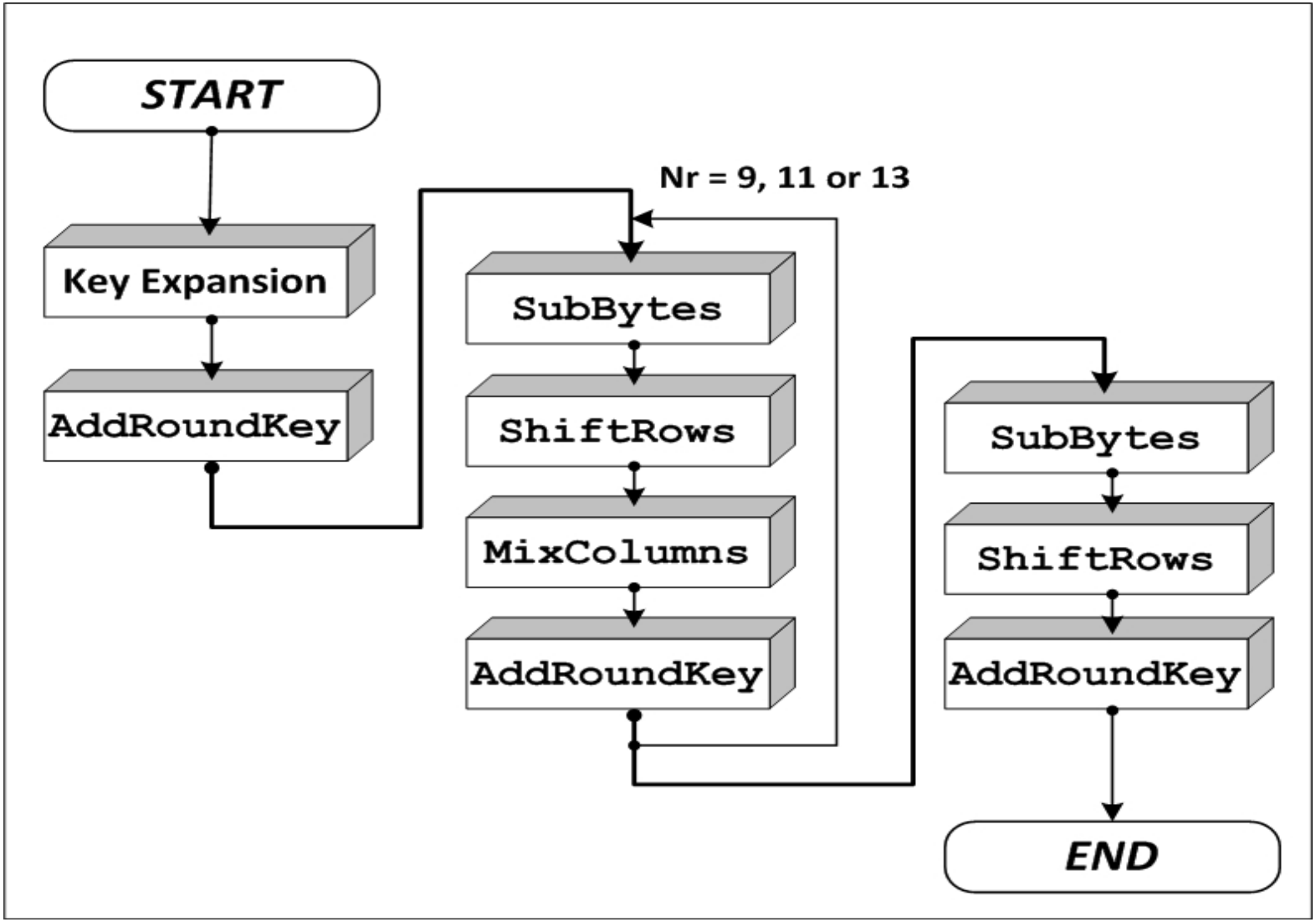
RIJNDAEL-AES: Paràmetres i tipus de dades



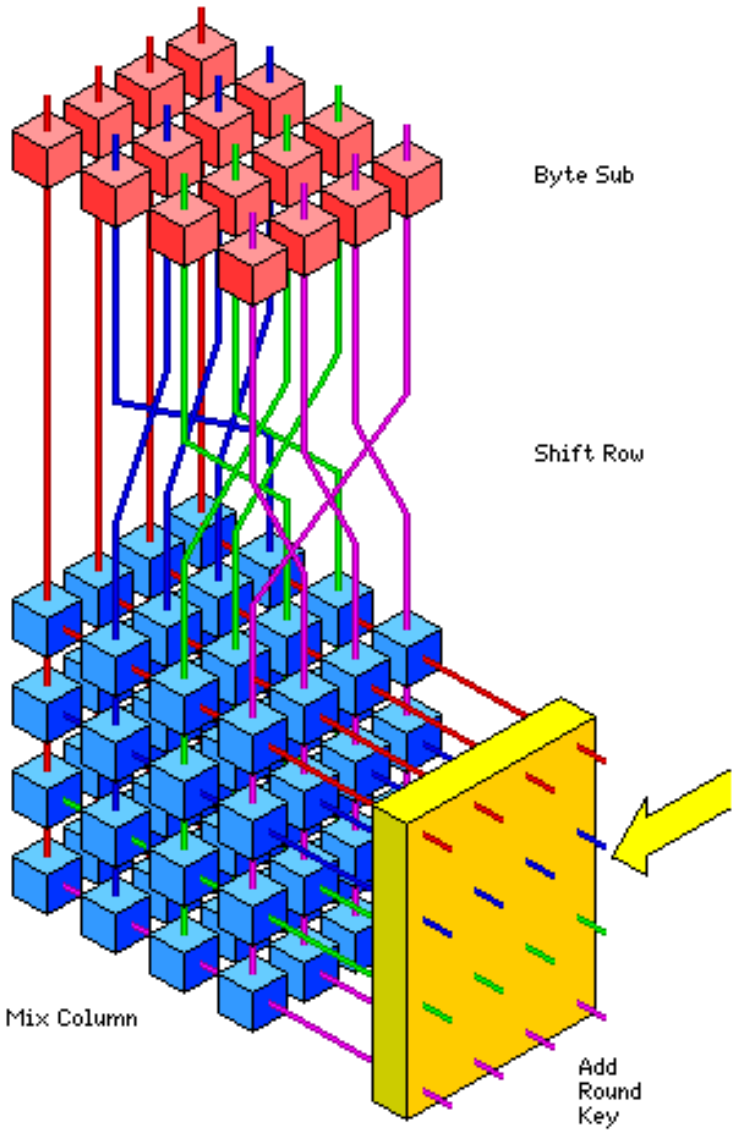
RIJNDAEL-AES: Descripció de l'algoritme de xifratge

1. AddRoundKey(State, RoundKey_0)
2. Round(State, RoundKey_i), $i = 1, \ldots, N_r - 1$:
   1. ByteSub(State)
   2. ShiftRow(State)
   3. MixColumn(State)
   4. AddRoundKey(State, RoundKey_i)
3. FinalRound(State, RoundKey_{N_r}):
   1. ByteSub(State)
   2. ShiftRow(State)
   3. AddRoundKey(State, RoundKey_{N_r})

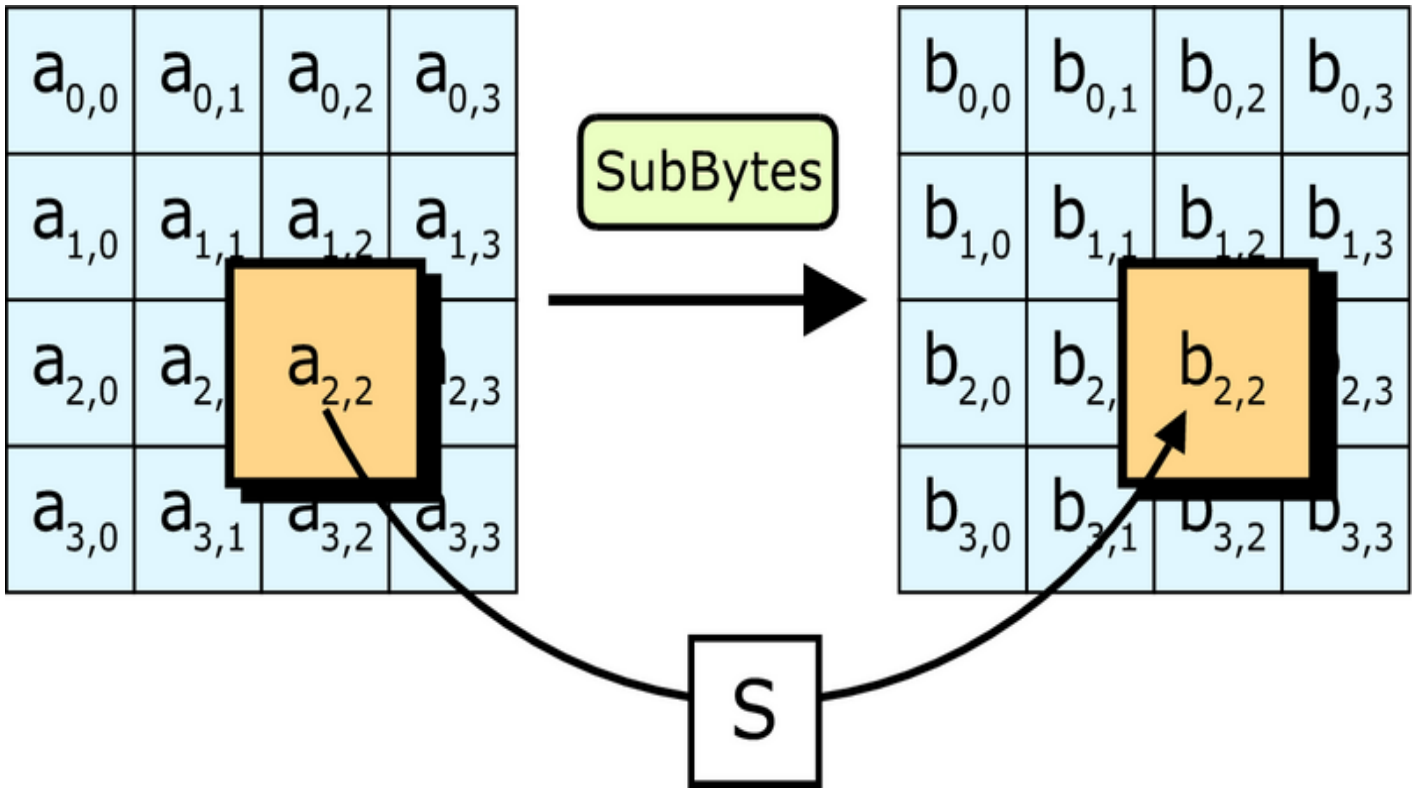
RIJNDAEL-AES: Descripció de l'algoritme de xifratge



RIJNDAEL-AES: Descripció d'un tomb



RIJNDAEL-AES: ByteSuB



RIJNDAEL-AES: ByteSuB

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

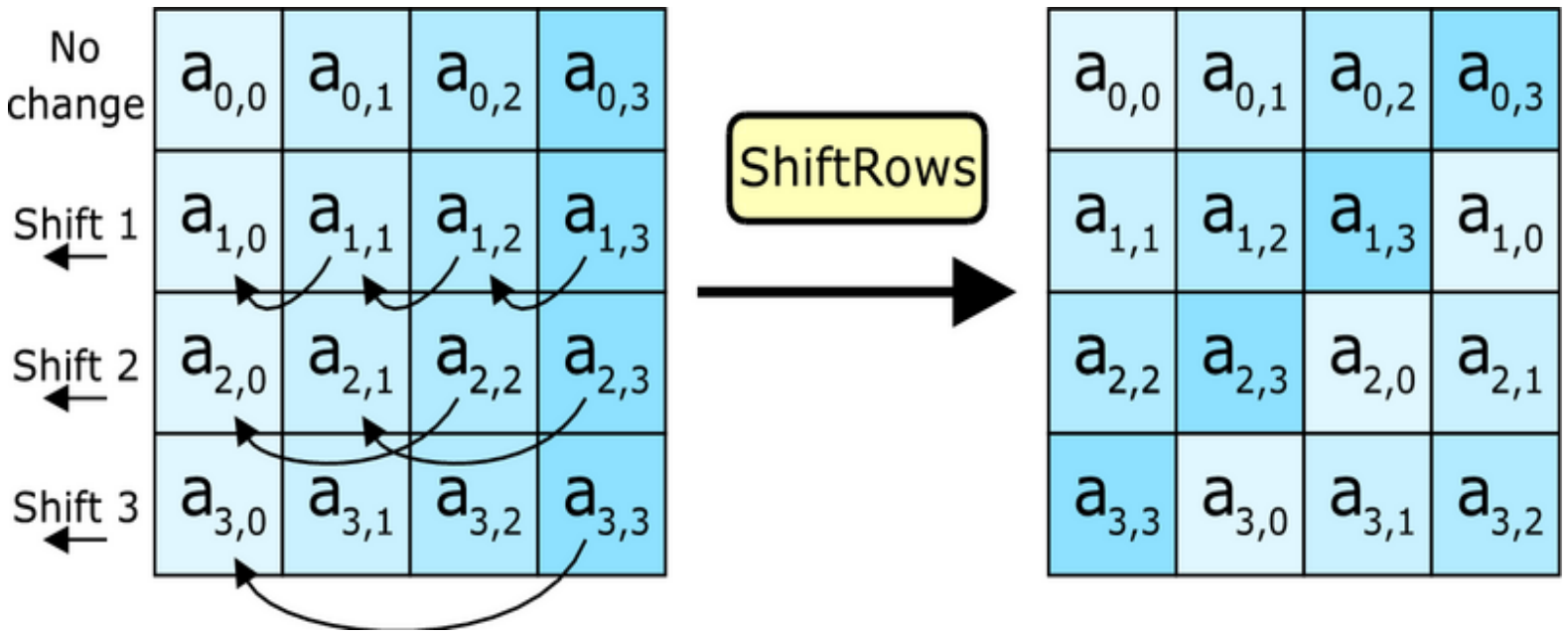
Transformació no lineal de substitució de bytes (S-box)

1. Pren l'invers a GF(2^8)
2. Aplica la transformació afí

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

RIJNDAEL-AES: ShiftRow

Les files de State es desplacen cíclicament cap a l'esquerra: la primera no es toca, la segona es desplaça 1 posició, la tercera 2 posicions i la quarta 3

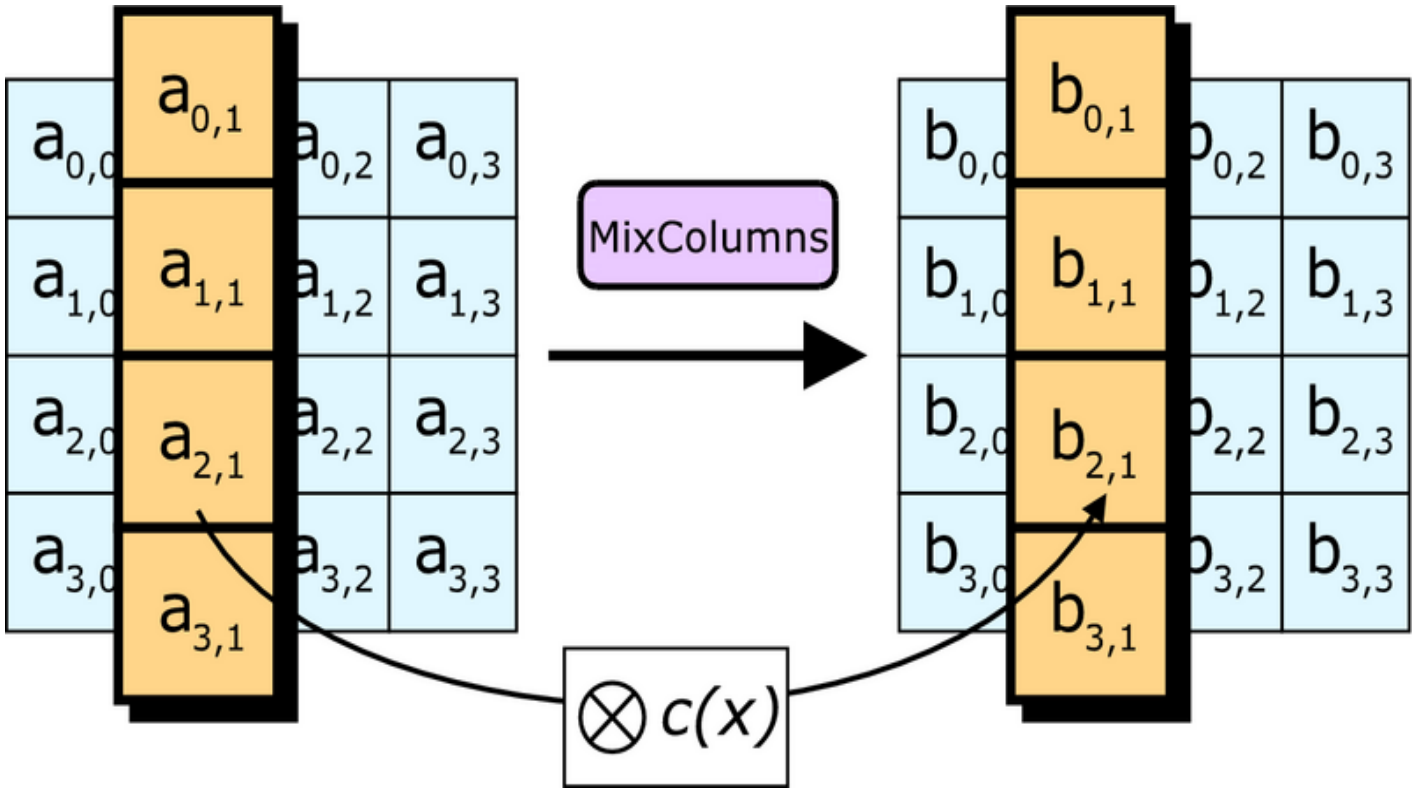


Canvia cada columna a_0, a_1, a_2, a_3 de la matriu d'estat

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 0x02 & 0x03 & 0x01 & 0x01 \\ 0x01 & 0x02 & 0x03 & 0x01 \\ 0x01 & 0x01 & 0x02 & 0x03 \\ 0x03 & 0x01 & 0x01 & 0x02 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

$$\begin{aligned} b_0 &= 0x02 \bullet a_0 + 0x03 \bullet a_1 + 0x01 \bullet a_2 + 0x01 \bullet a_3 \\ b_1 &= 0x01 \bullet a_0 + 0x02 \bullet a_1 + 0x03 \bullet a_2 + 0x01 \bullet a_3 \\ &\dots \end{aligned}$$

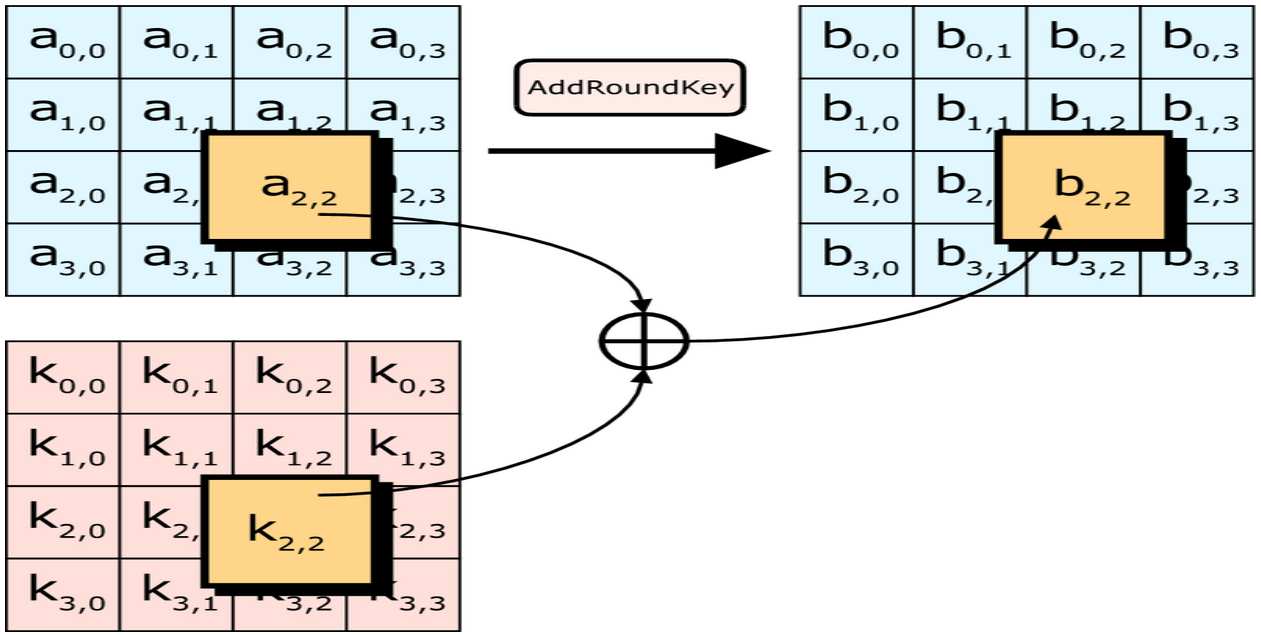
RIJNDAEL-AES: MixColumn



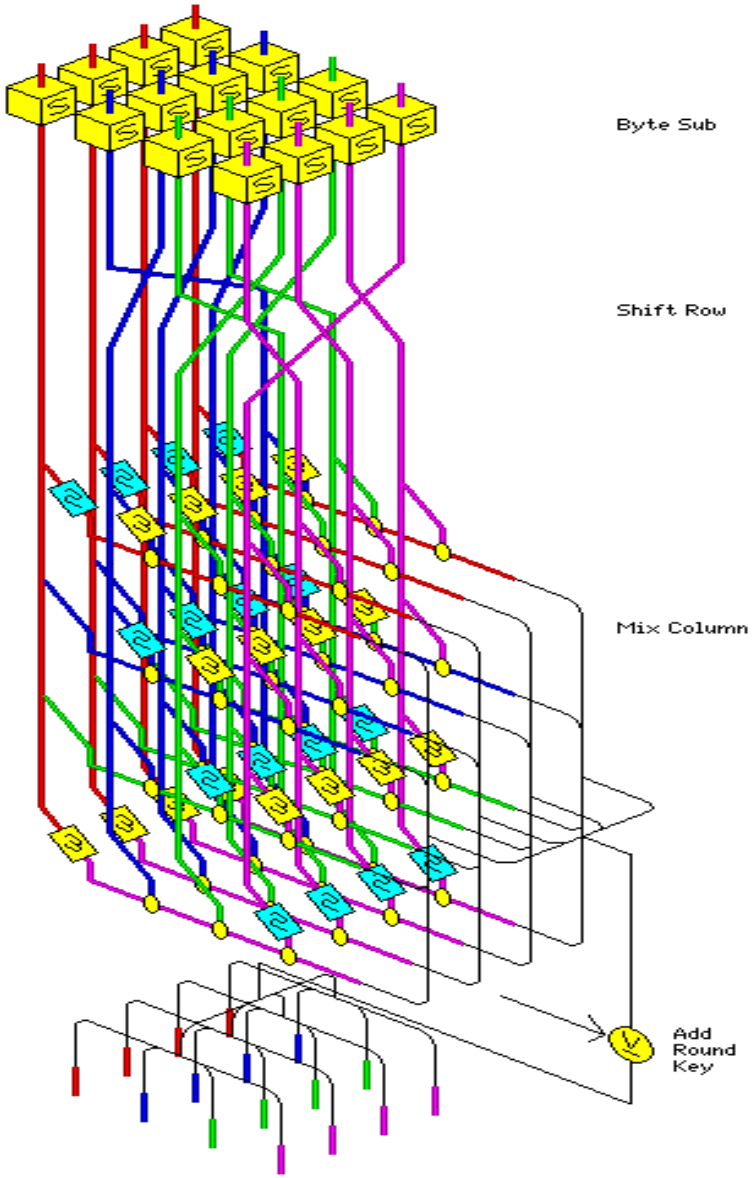
RIJNDAEL-AES: AddRoundKey

És un XOR (byte a byte) entre State i RoundKey:

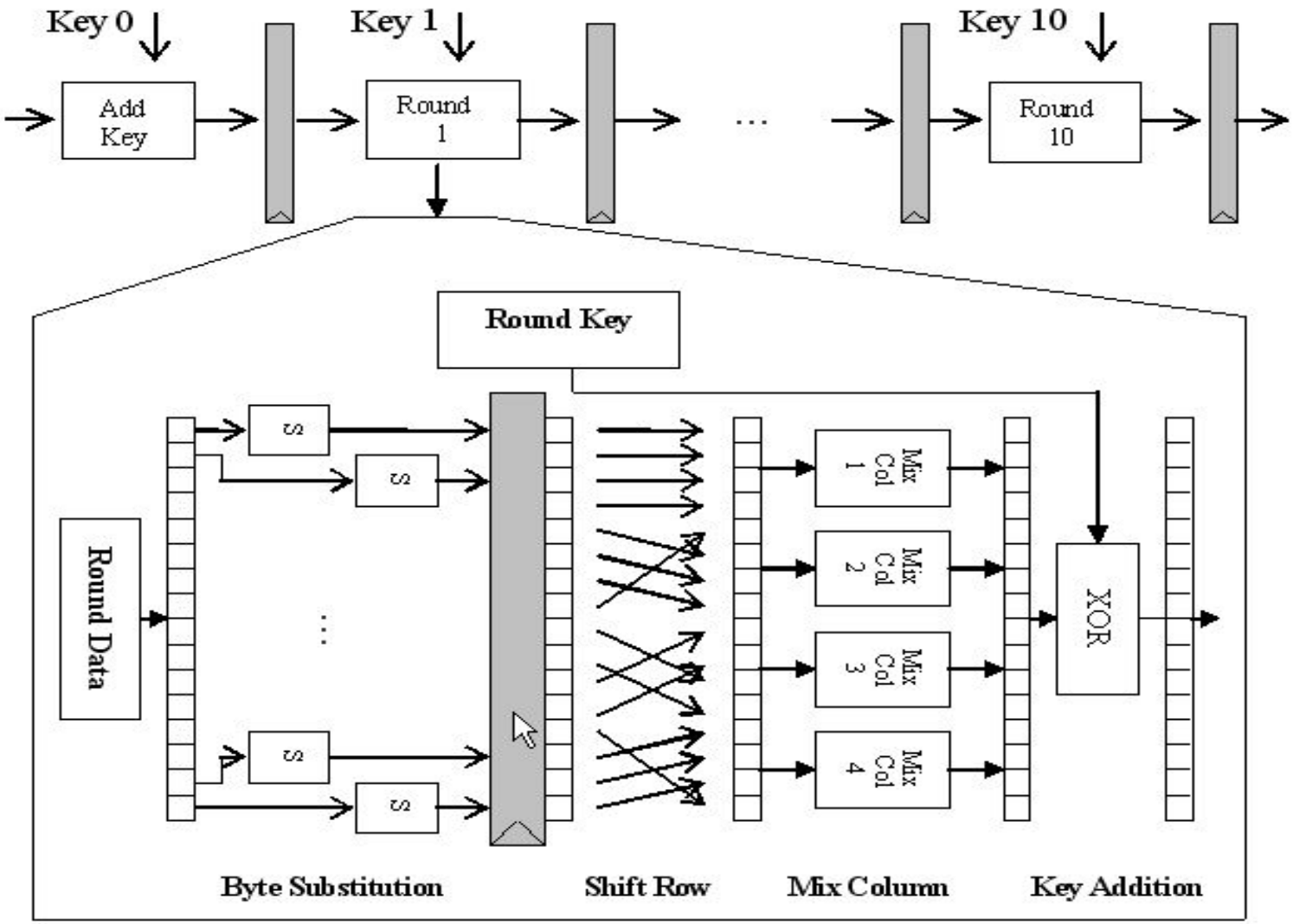
$$\texttt{State} \oplus \texttt{RoundKey}$$



RIJNDAEL-AES: Descripció d'un tomb

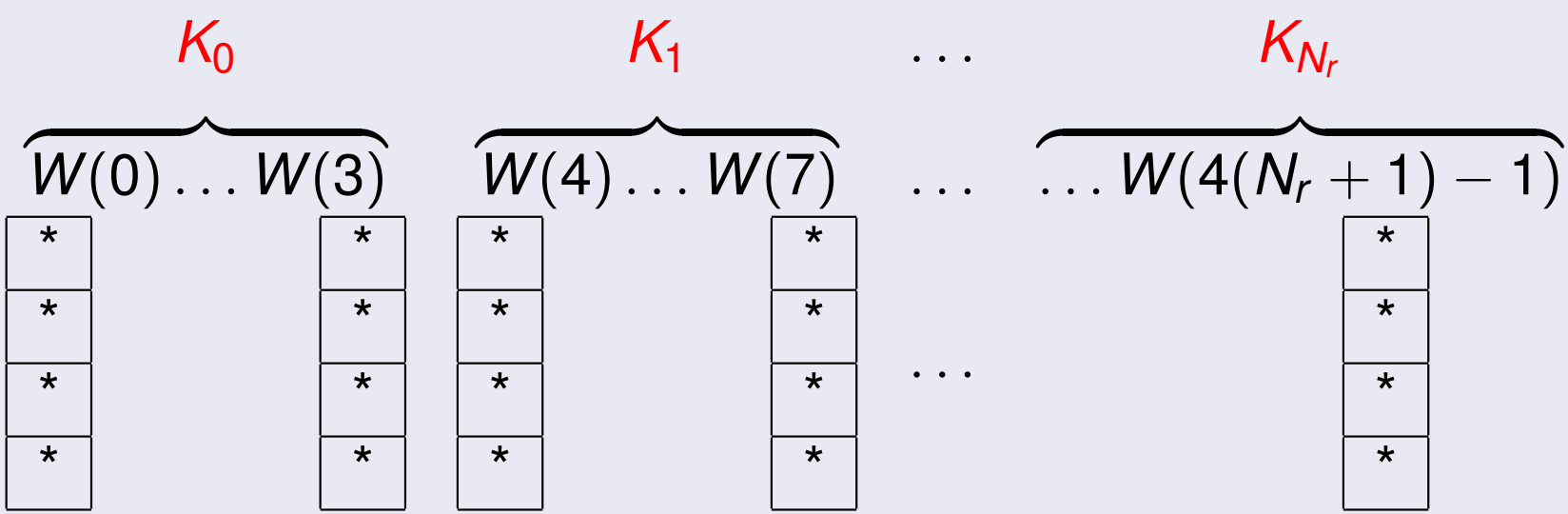


RIJNDAEL-AES



RIJNDAEL-AES: Expansió de clau

Es generen $N_r + 1$ subclaus. Cadascuna és una matriu 4×4 de bytes. S'emmagatzemen en una matriu W, de 4 files i $4(N_r + 1)$ columnes



Les primeres N_k columnes són les de la clau K La resta es defineixen recursivament utilitzant la funció `ByteSub`, desplaçaments cíclics i $\oplus$. La recurrència depèn de la longitud de la clau

RIJNDAEL-AES: Expansió de clau

$N_k \leq 6$

```
KeyExpansion(byte Key[4*Nk] word W[Nb*(Nr+1)]) {
for(i = 0; i < Nk; i++)
W[i] = (Key[4*i],Key[4*i+1],Key[4*i+2],Key[4*i+3]);
for(i = Nk; i < Nb * (Nr + 1); i++)
{
temp = W[i - 1];
if (i % Nk == 0)
temp = SubByte(RotByte(temp)) ⊕ Rcon[i / Nk];
W[i] = W[i - Nk] ⊕ temp;
}
```

RIJNDAEL-AES: Expansió de clau

$N_k = 8$

```
KeyExpansion(byte Key[4*Nk] word W[Nb*(Nr+1)]) {
for(i = 0; i < Nk; i++)
W[i] = (key[4*i],key[4*i+1],key[4*i+2],key[4*i+3]);
for(i = Nk; i < Nb * (Nr + 1); i++)
{
temp = W[i - 1];
if (i % Nk == 0)
temp = SubByte(RotByte(temp)) ⊕ Rcon[i / Nk];
else if (i % Nk == 4)
temp = SubByte(temp);
W[i] = W[i - Nk] ⊕ temp;
}
}
```

RIJNDAEL-AES: Expansió de clau

$$W(i) = W(i - N_k) \oplus \texttt{temp}$$

$$\texttt{temp} = \texttt{ByteSub}(\texttt{RotByte}(\texttt{temp})) \oplus \texttt{Rcon}(\texttt{i}/\texttt{N}_\texttt{k})$$

o bé

$$\texttt{ByteSub}(\texttt{RotByte}(\texttt{temp})) \qquad (\texttt{N}_\texttt{k} = 8)$$

- $\texttt{RotByte}$ és un desplaçament cíclic d'una posició a l'esquerra
- $\texttt{Rcon[i]} = (\texttt{RC[i]}, \texttt{0x00}, \texttt{0x00}, \texttt{0x00})$, essent $\texttt{RC[i]}$ un element de GF(2^8) definit per la recurrència

$$\texttt{RC[1]} = \texttt{0x01}, \qquad \texttt{RC[i]} = \texttt{0x02} \bullet \texttt{RC[i} - 1\texttt{]}$$

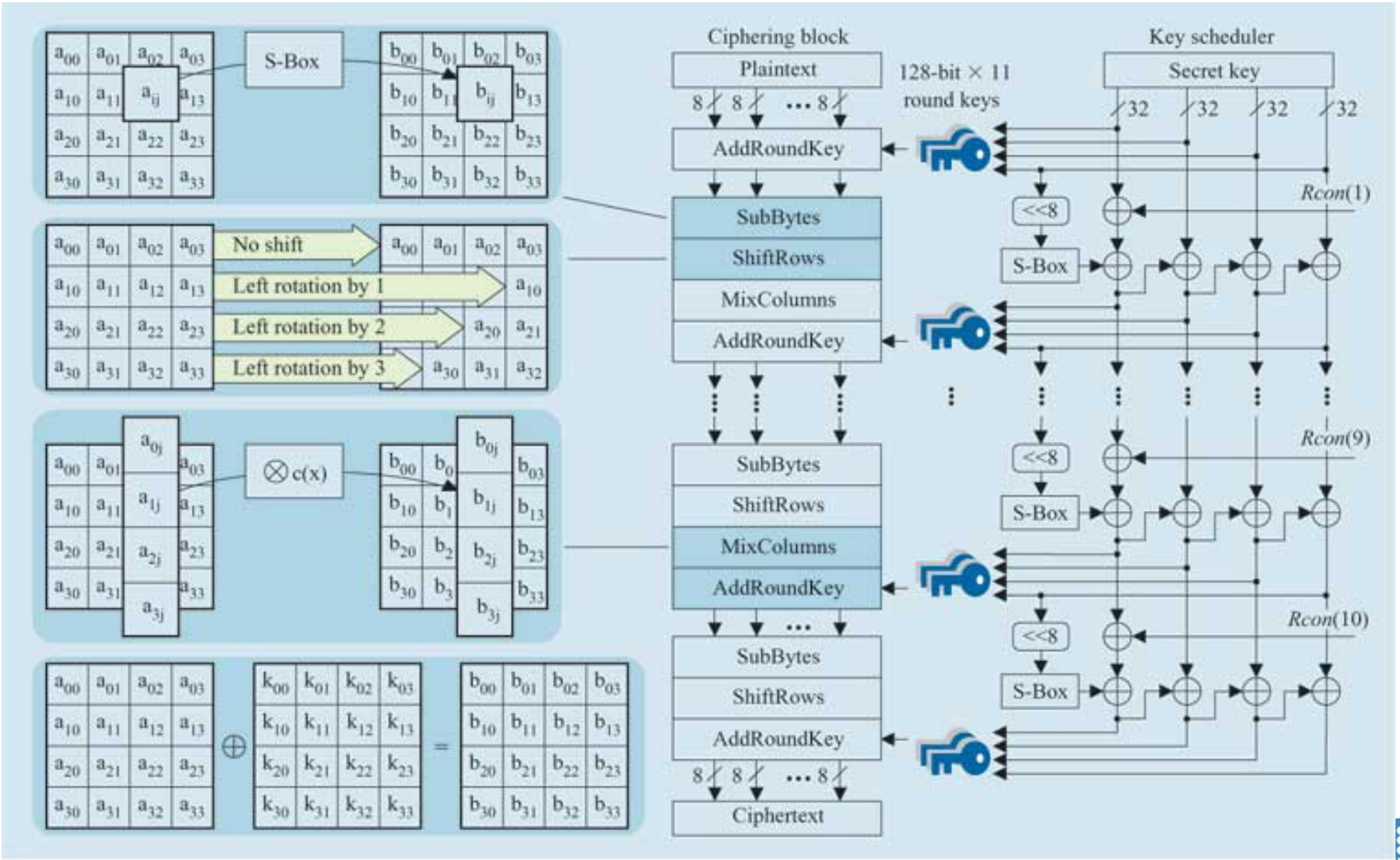
RIJNDAEL-AES: Expansió de clau

Nk	Nb	Nr	Nb(Nr+1)
4	4	10	44
6	4	12	52
8	4	14	60

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Rcon

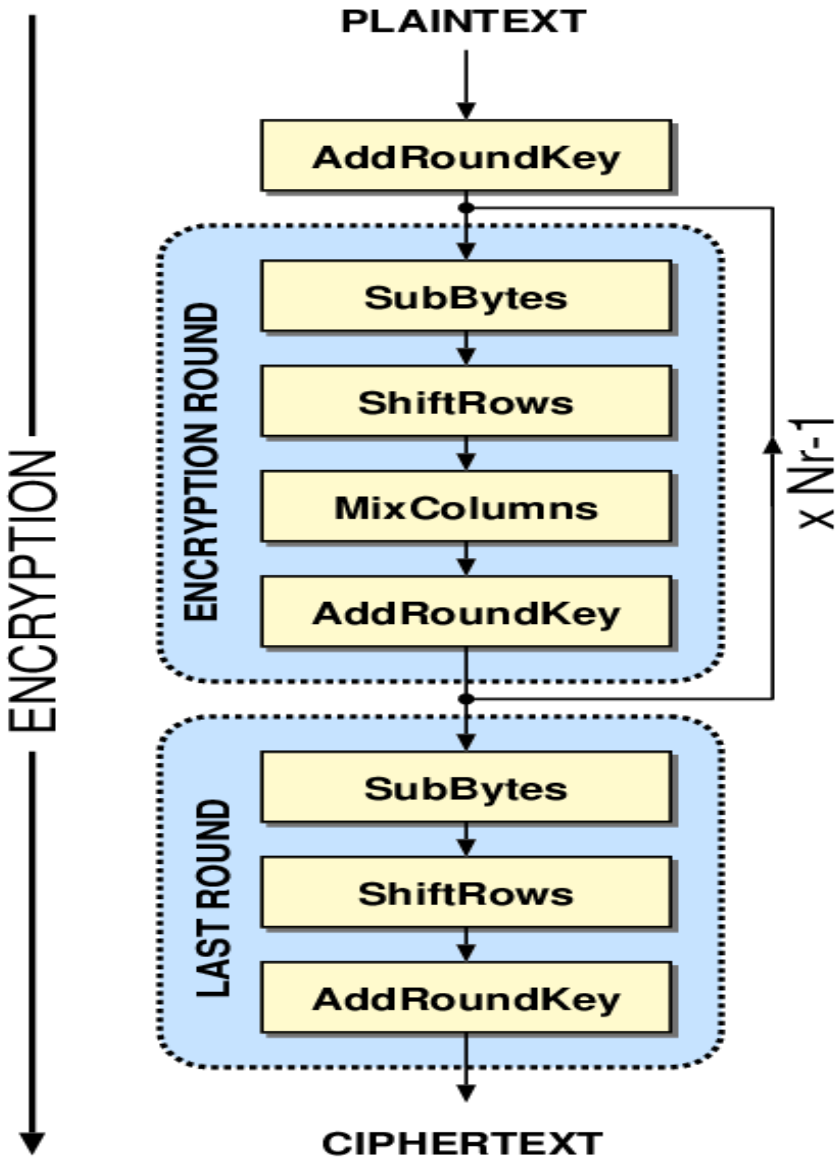
RIJNDAEL-AES

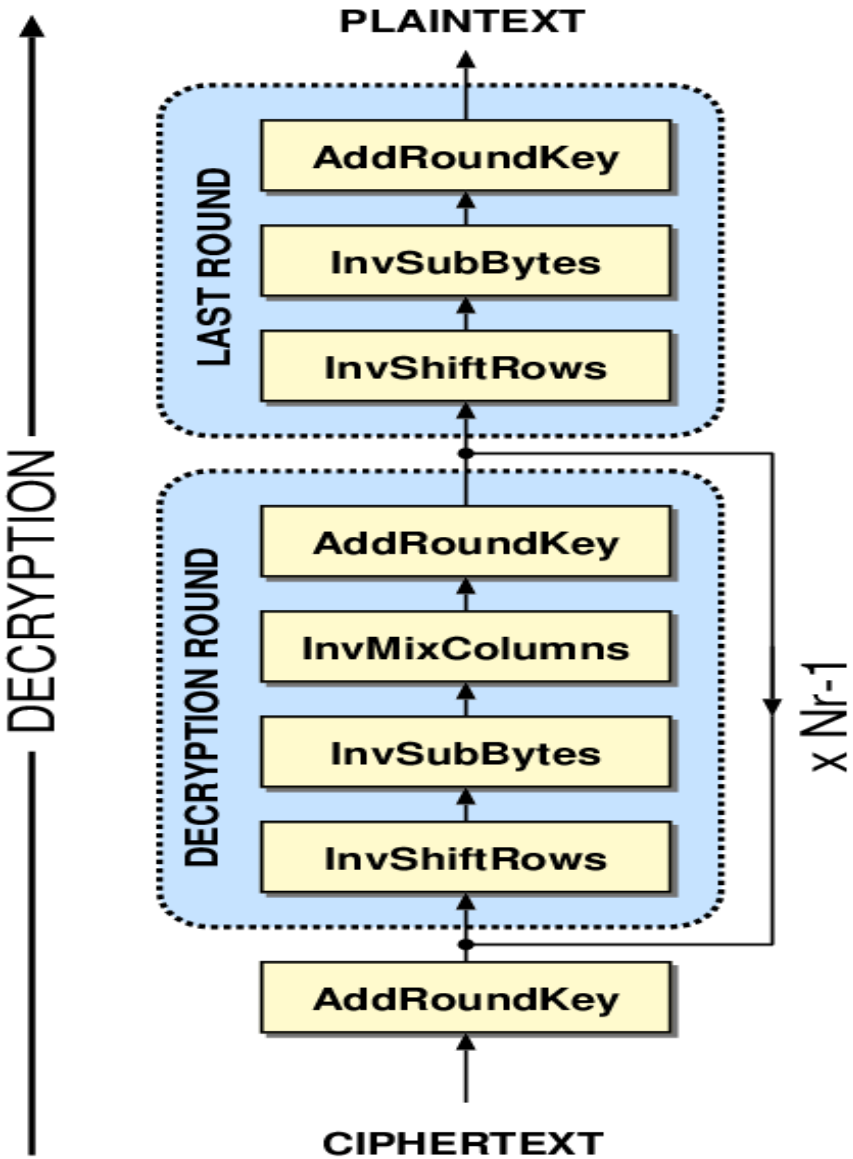


AES: algoritme de desxifratge

1. AddRoundKey(State, InvRoundKey_{N_r})
2. Round(State, InvRoundKey_i), $i = N_r - 1, \ldots, 1$:
   1. InvByteSub(State)
   2. InvShiftRow(State)
   3. InvMixColumn(State)
   4. AddRoundKey(State, InvRoundKey_i)
3. FinalRound(State, InvRoundKey_{N_0}):
   1. InvByteSub(State)
   2. InvShiftRow(State)
   3. AddRoundKey(State, InvRoundKey_{N_0})

RIJNDAEL-AES





AES: algoritme de desxifratge

Les funcions `InvByteSub`, `InvShiftRow`, `InvMixColumn` són les inverses respectives

Les subclaus `InvRoundKey` venen donades per

$\texttt{InvRoundKey}_0 = \texttt{RoundKey}_0$

$\texttt{InvRoundKey}_i = \texttt{InvMixColumn}(\texttt{RoundKey}_i), \; i = 1, \ldots, N_r - 1$

$\texttt{InvRoundKey}_{N_r} = \texttt{RoundKey}_{N_r}$

AES: algoritme de desxifratge

InvByteSub

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

MixColumn and InvMixColumn

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \quad \text{C} \qquad \overset{\text{Inverse}}{\longleftrightarrow} \qquad \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \quad \text{C}^{-1}$$

RIJNDAEL-AES