Séance 3

Le standard de chiffrement actuel : AES

AES : Advanced Encryption System

- 1996 : Evalutation du DES $\Rightarrow$ il faut un remplaçant
- Polémique : NSA soupçonnée d'avoir introduit des trappes
- 1997 : Appel à candidature **internationale et publique**
  - 15 propositions, 5 finalistes
    1. Rijndael (Daemen, Rijmen BE) 10/12/14 rondes
       Bloc : 128 bits ; Clé : 128/192/256 bits
    2. Serpent (Anderson, Biham, Knudsen UK) 32 rondes
       Bloc : 128 bits ; Clé : 128/192/256 bits
    3. Twofish (Schneier& *al* US) 16 rondes
       Bloc : 128 bits ; Clé : 128/192/256 bits
    4. RC6 (Rivest US) 20 rondes
       Bloc : 128 bits ; Clé : 128/192/256 bits
    5. MARS (Coppersmith/IBM US) 16 rondes
       Bloc : 128 bits ; Clé : 128$\rightarrow$ 448 bits (128+32k bits)

  And the winner is
- 2000 : Standard NIST : AES-Rijndael

Critères de sélection

- Sécurité
- Coût de l'implantation
- Paramètres comme vitesse, latence, complexité
- Flexibilité : Implantation sur des processeurs 8 bits, dans les cartes à puce, dans du matériel dédié.

Les inventeurs

- Joan Daemen (à Gauche)
  - 1965 : Naissance à Achel
  - 1988 : Rejoint l'UCL (Université Catholique de Louvain)
  - 1995 : Thèse sur un algorithme de chiffrement de sa conception 3 − *way*
  - 1997 : Concepteur de Rijndael
- Vincent Rijmen (à Droite)
  - 1970 : Naissance à Louvain
  - 1993 : Diplome d'électronique de l'UCL
  - 1997 : Thèse (*Cryptanalysis and design of iterated block ciphers)*

AES-Rijndael : les grandes lignes

Définition

Algorithme itératif de chiffrement par blocs appliquant sur un même bloc, 10/12/14 fois une fonction de ronde.

Fonction de ronde

- *ByteSub* : **non-linéarité**
- *ShiftRow* : **diffusion** entre les colonnes
- *MixColumn* : **diffusion** entre les octets à l'intérieur des colonnes
- *Addition de la clé de ronde* : **confusion**, dépendance de la clé

- La clé : 128, 192 ou 256 bits
- Les blocs : 128 bits (fixe pour l'AES-Rijndael), 192, 256 bits
- Blocs découpés en matrice 4×4 dont chaque élément est représenté par $8 bits$
- Opérations sur des octets

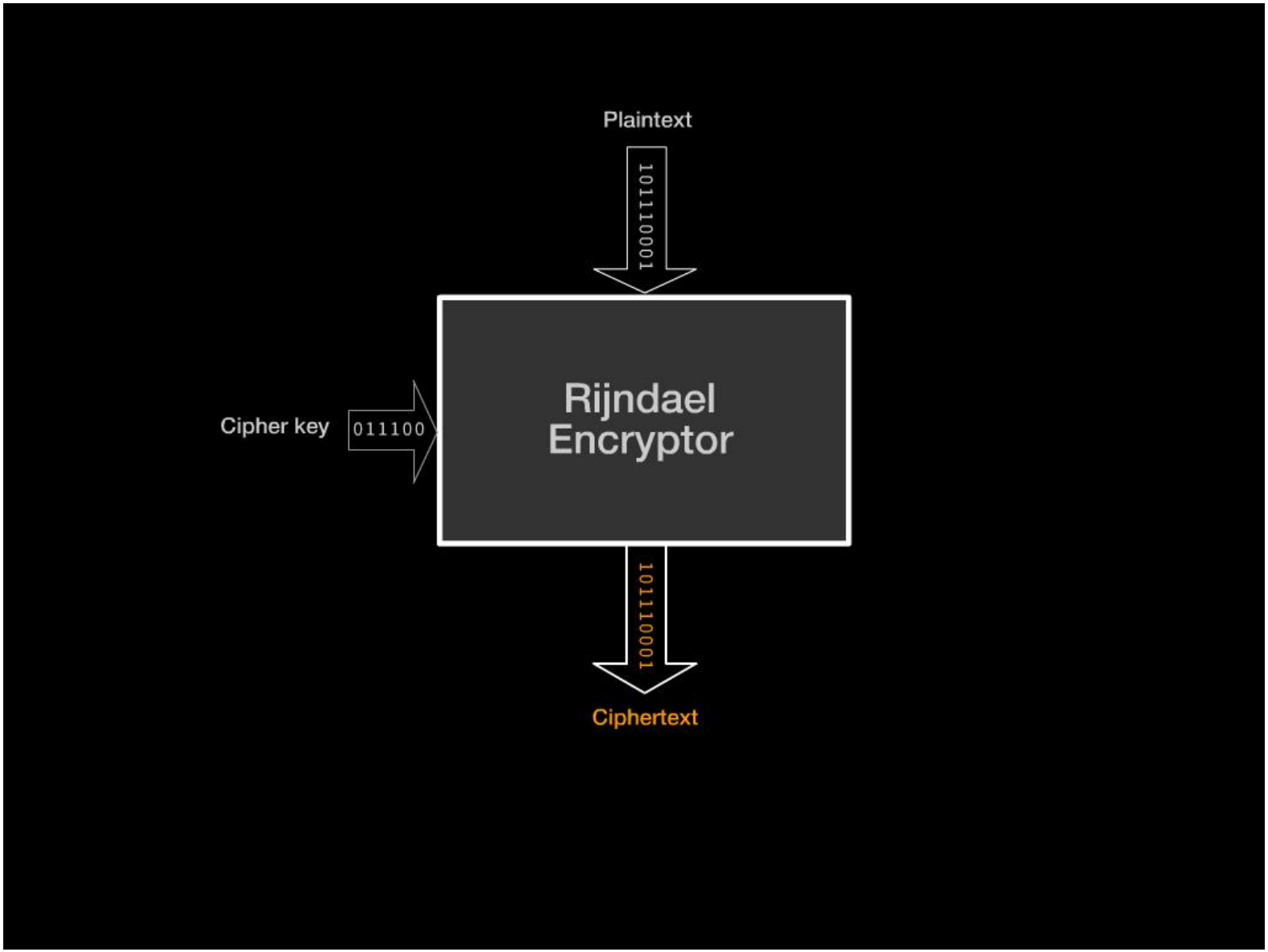
Relation nombre de rondes / Taille de la clé / Taille du bloc

Taille du bloc	Rondes Taille de la clé		
	128 bits	192 bits	256 bits
128 bits	10	12	14
192 bits	12	12	14
256 bits	14	14	14

Démonstration : Fonctionnement de l'AES

- Démo (www.cryptool.com)
- Corps finis, voir slide 56

AES-Rijndael : les détails



AES-Rijndael : les détails

Input

State

32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34

This is a block from the plaintext message to be encrypted.

Cipher key

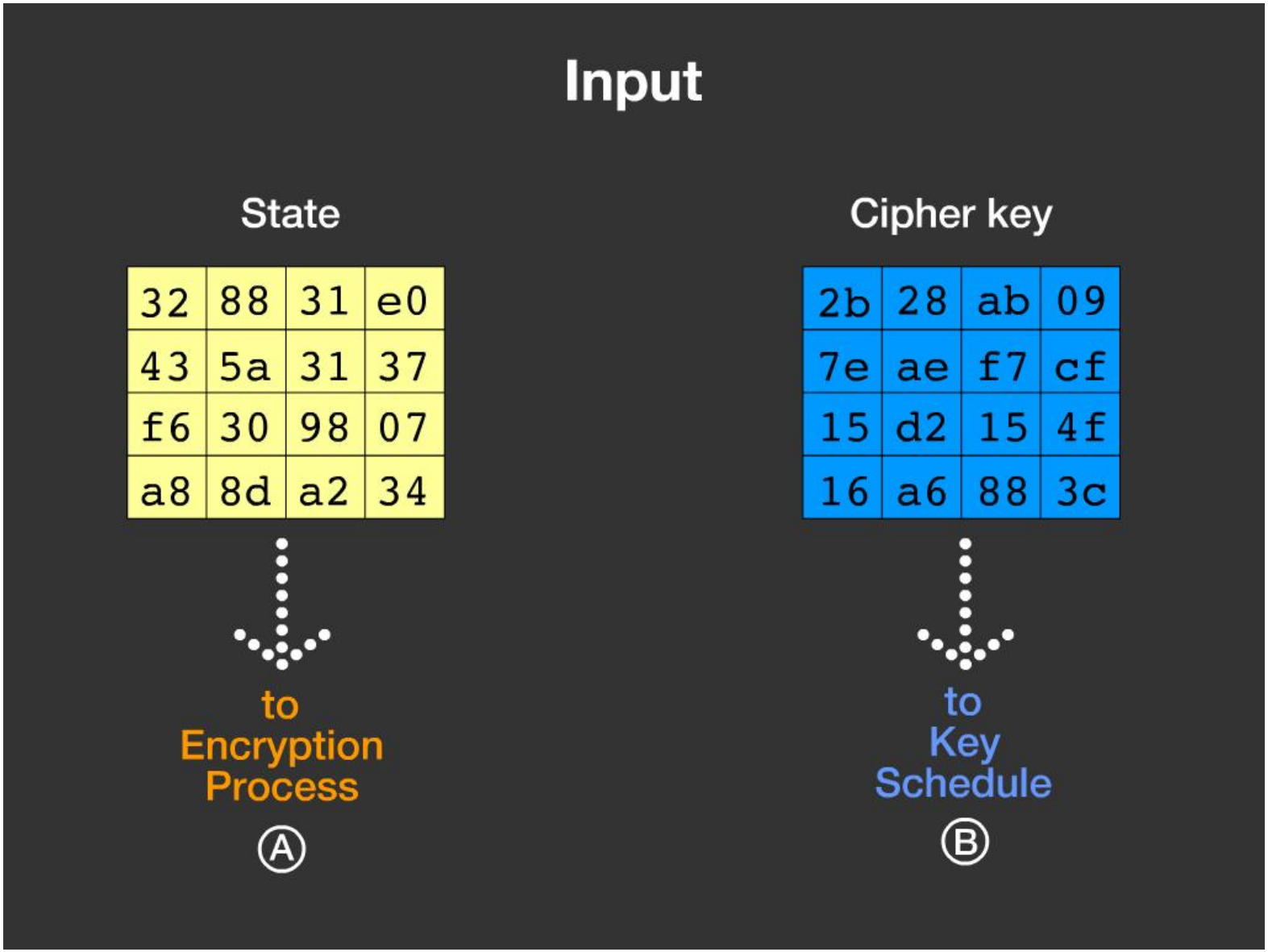
2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

Hexadecimal notation (sample):

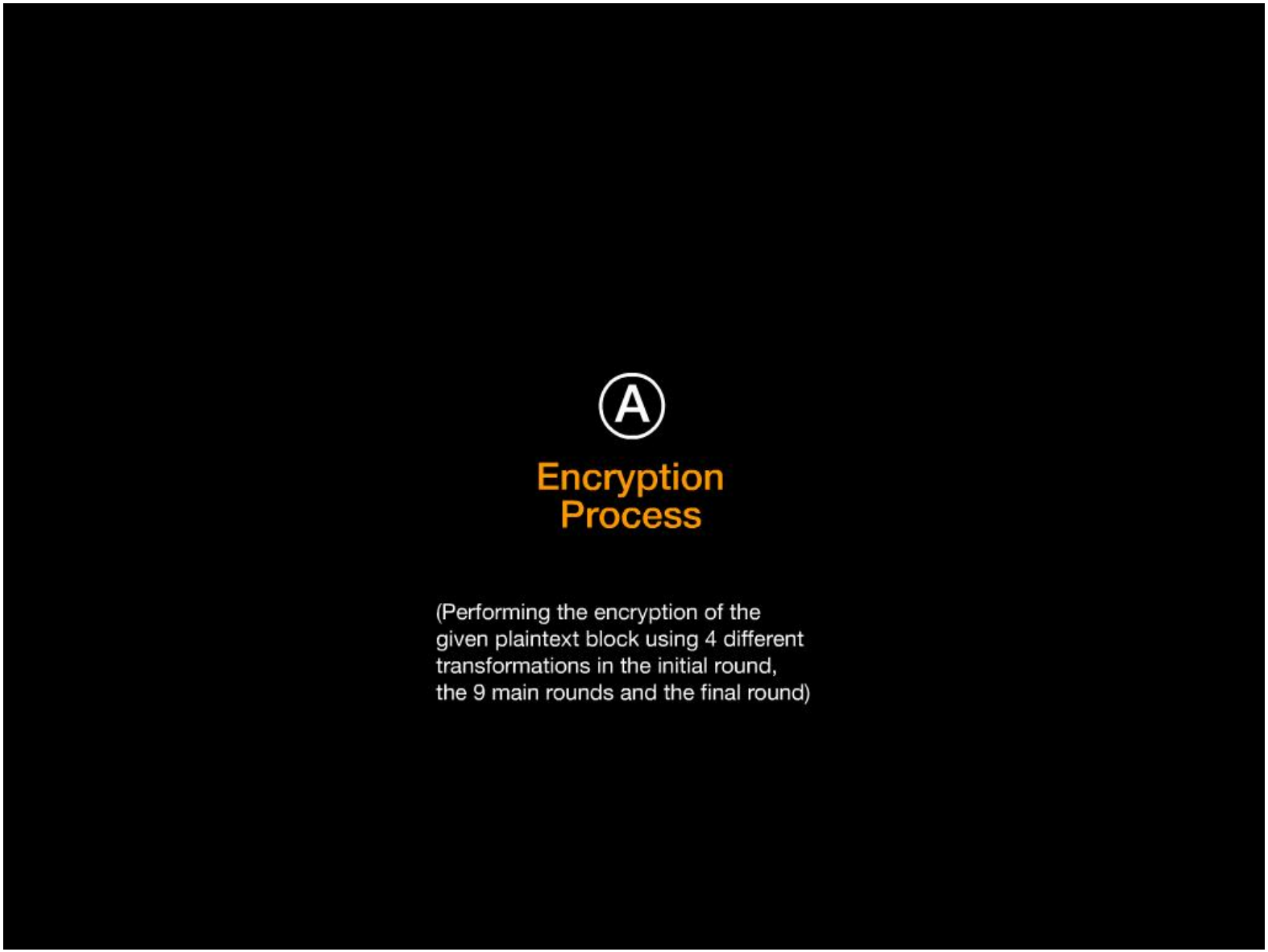
32 = 00110010 (1 byte)

3hex 2hex

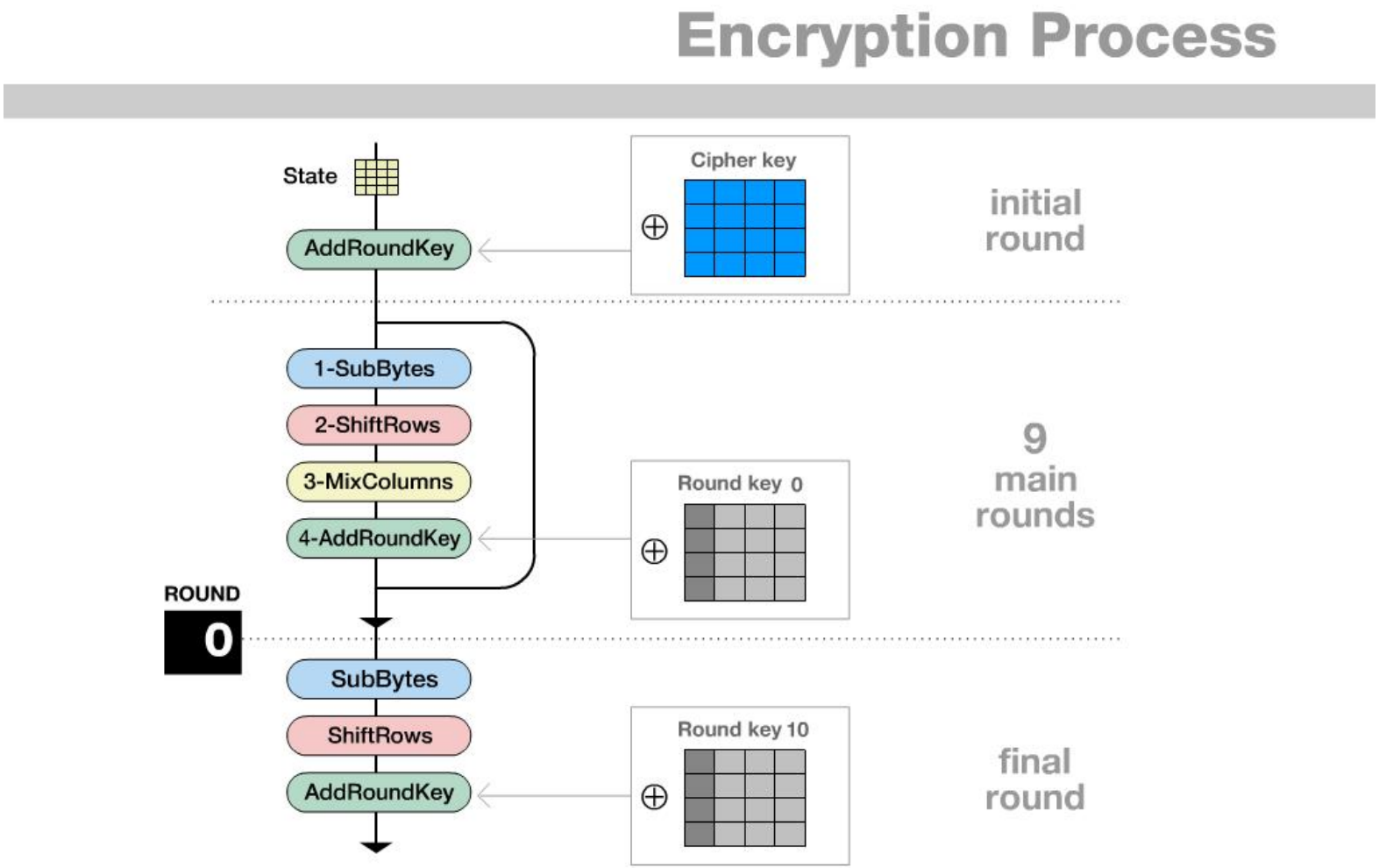
AES-Rijndael : les détails



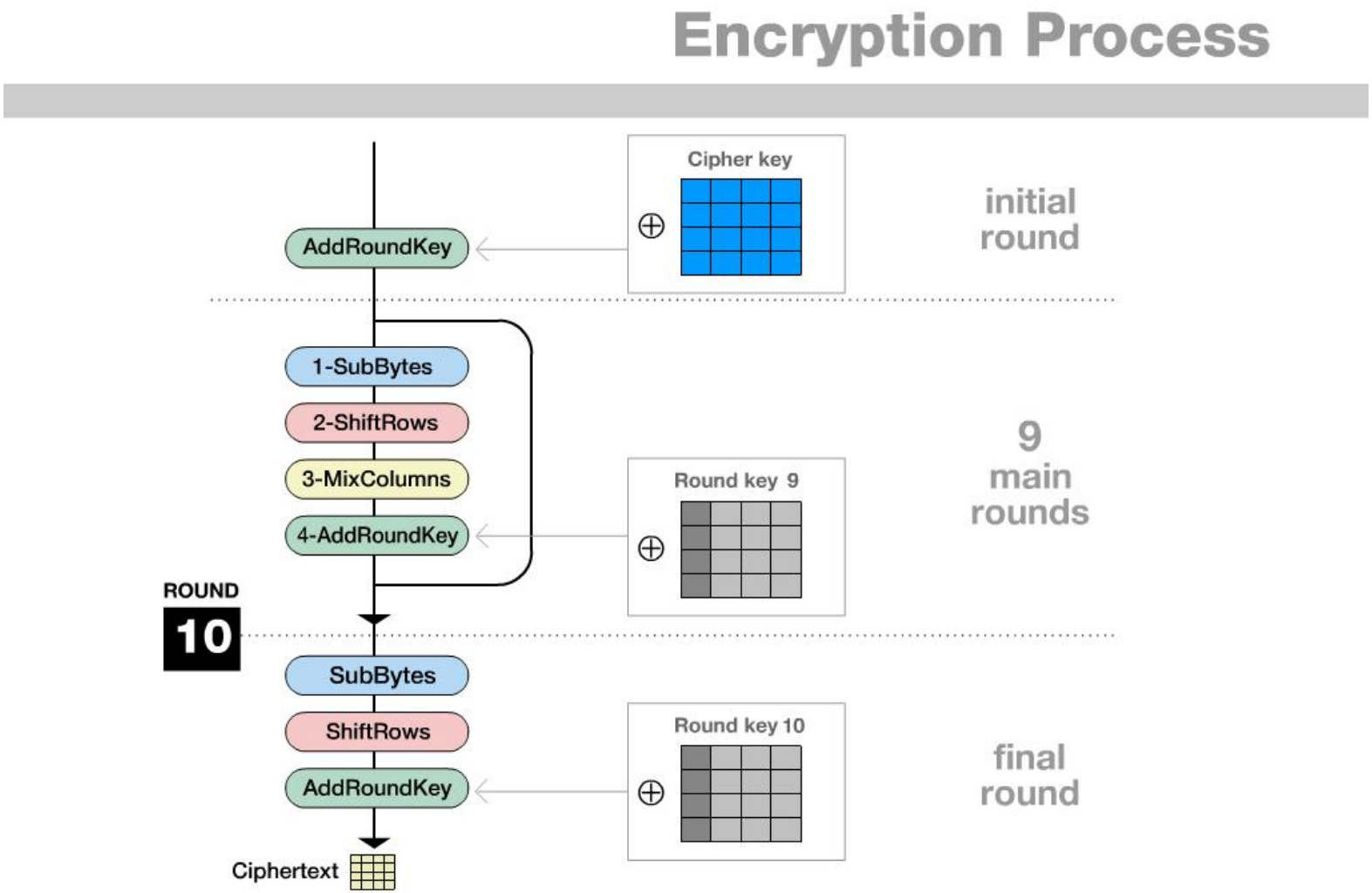
AES-Rijndael : les détails



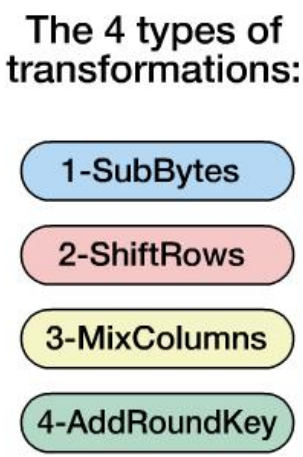
AES-Rijndael : les détails



AES-Rijndael : les détails



AES-Rijndael : les détails



AES-Rijndael : les détails

1 - SubBytes

Round 1

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

hex	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

x

S-BOX byte substitution table

AES-Rijndael : les détails

1 - SubBytes

Round 1

	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

19

d4

hex	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

x

S-BOX byte substitution table

AES-Rijndael : les détails

1 - SubBytes

Round 1

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

hex	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

x

S-BOX byte substitution table

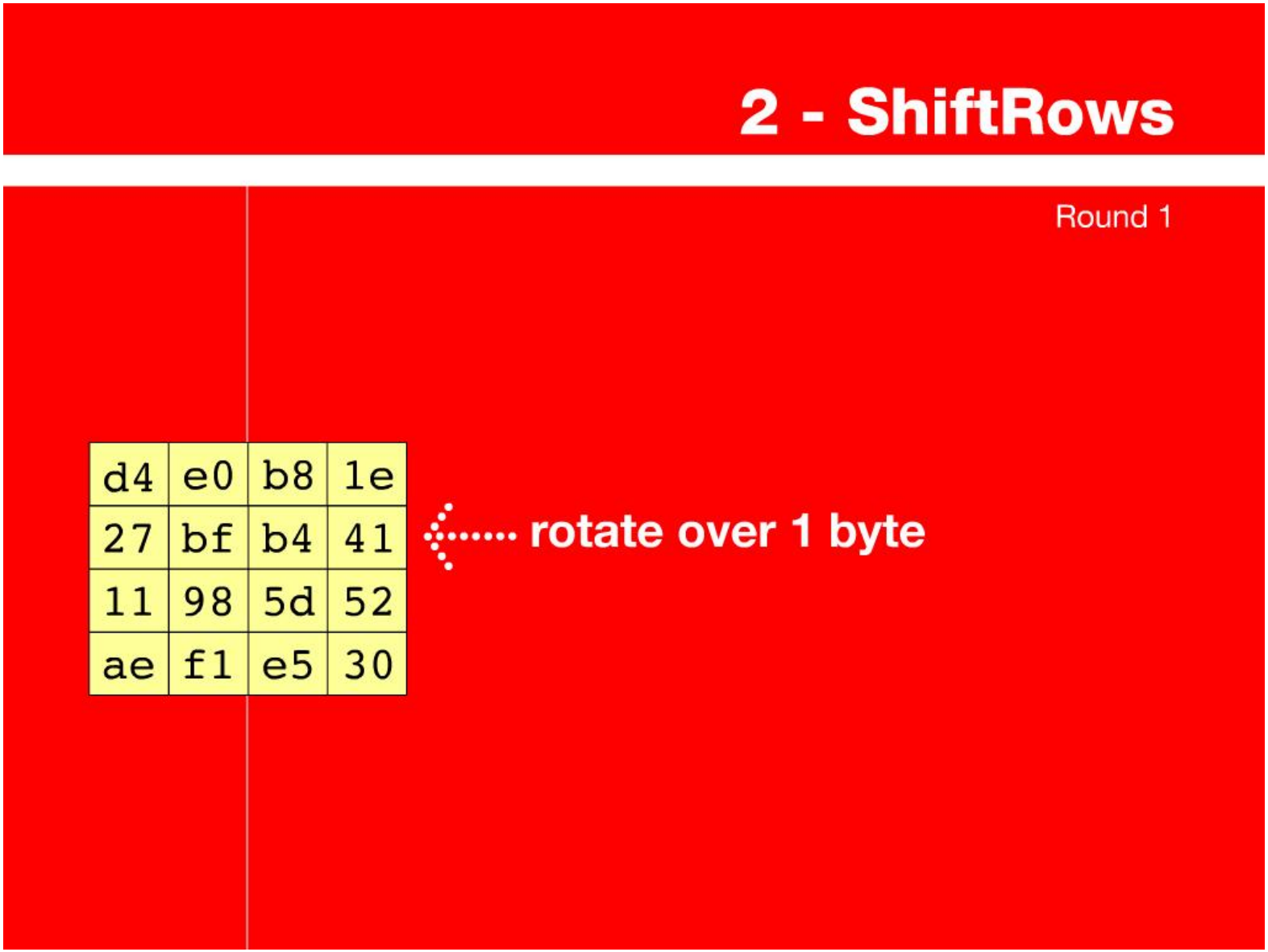
AES-Rijndael : les détails

2 - ShiftRows

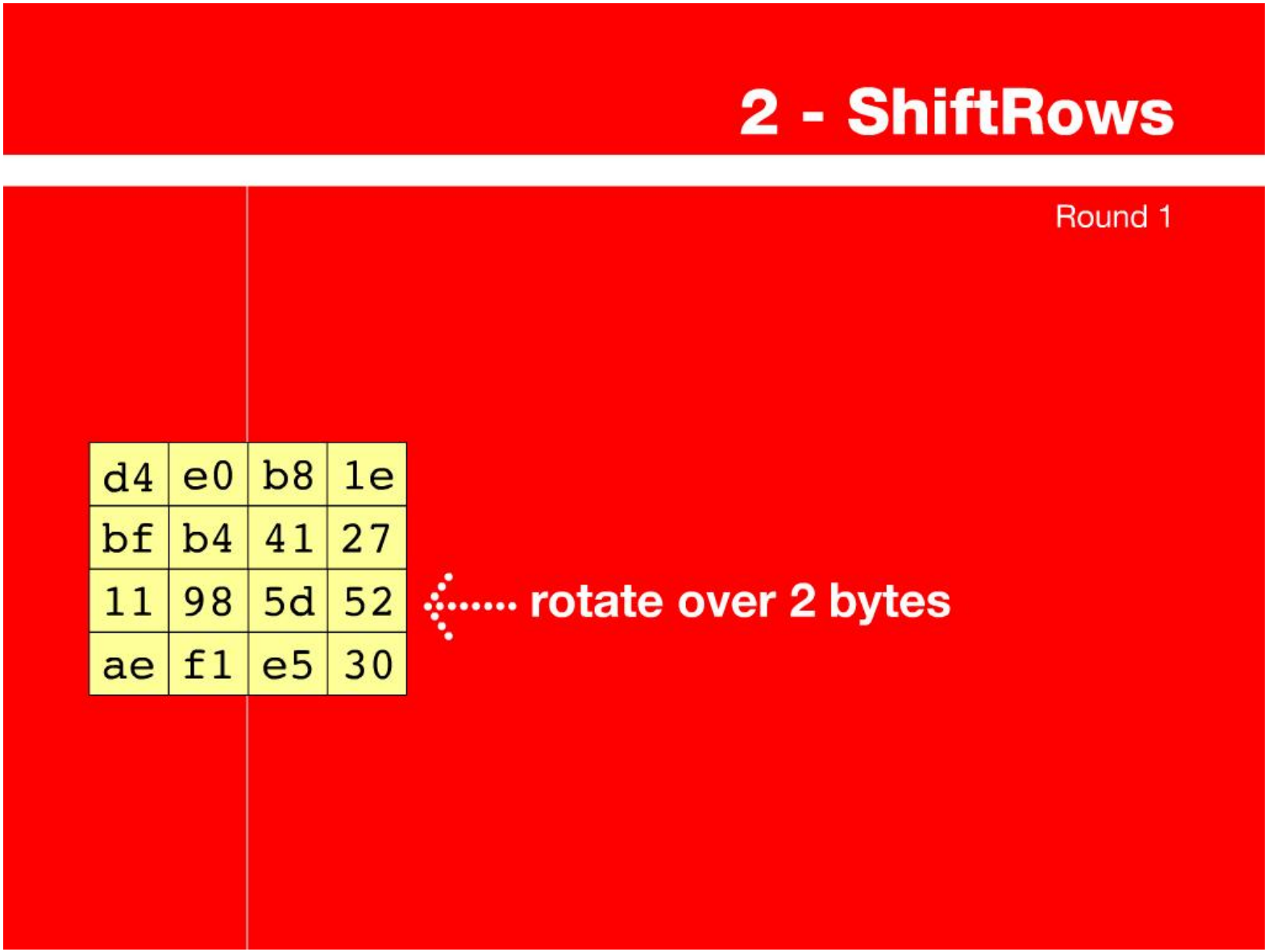
Round 1

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

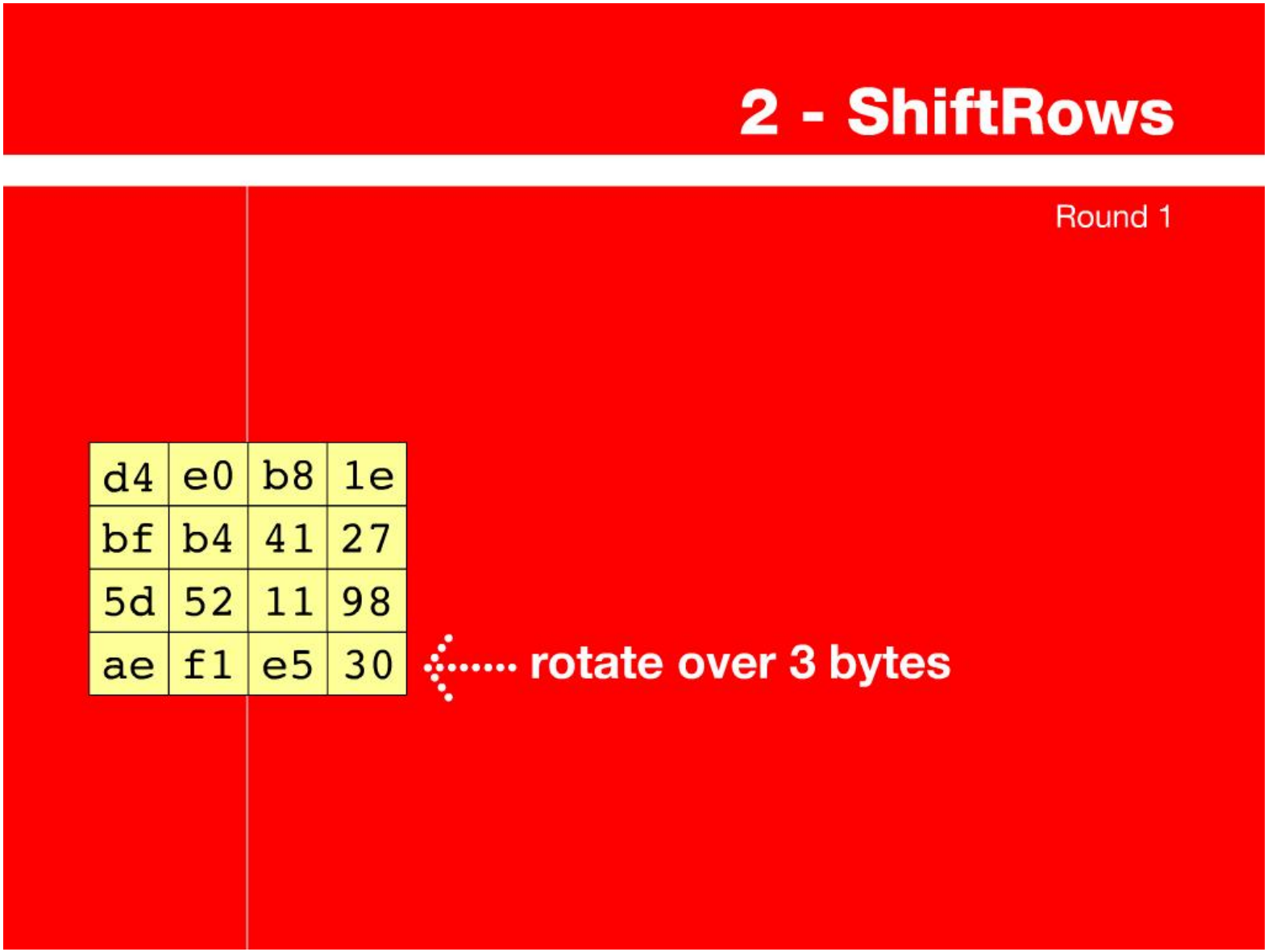
AES-Rijndael : les détails



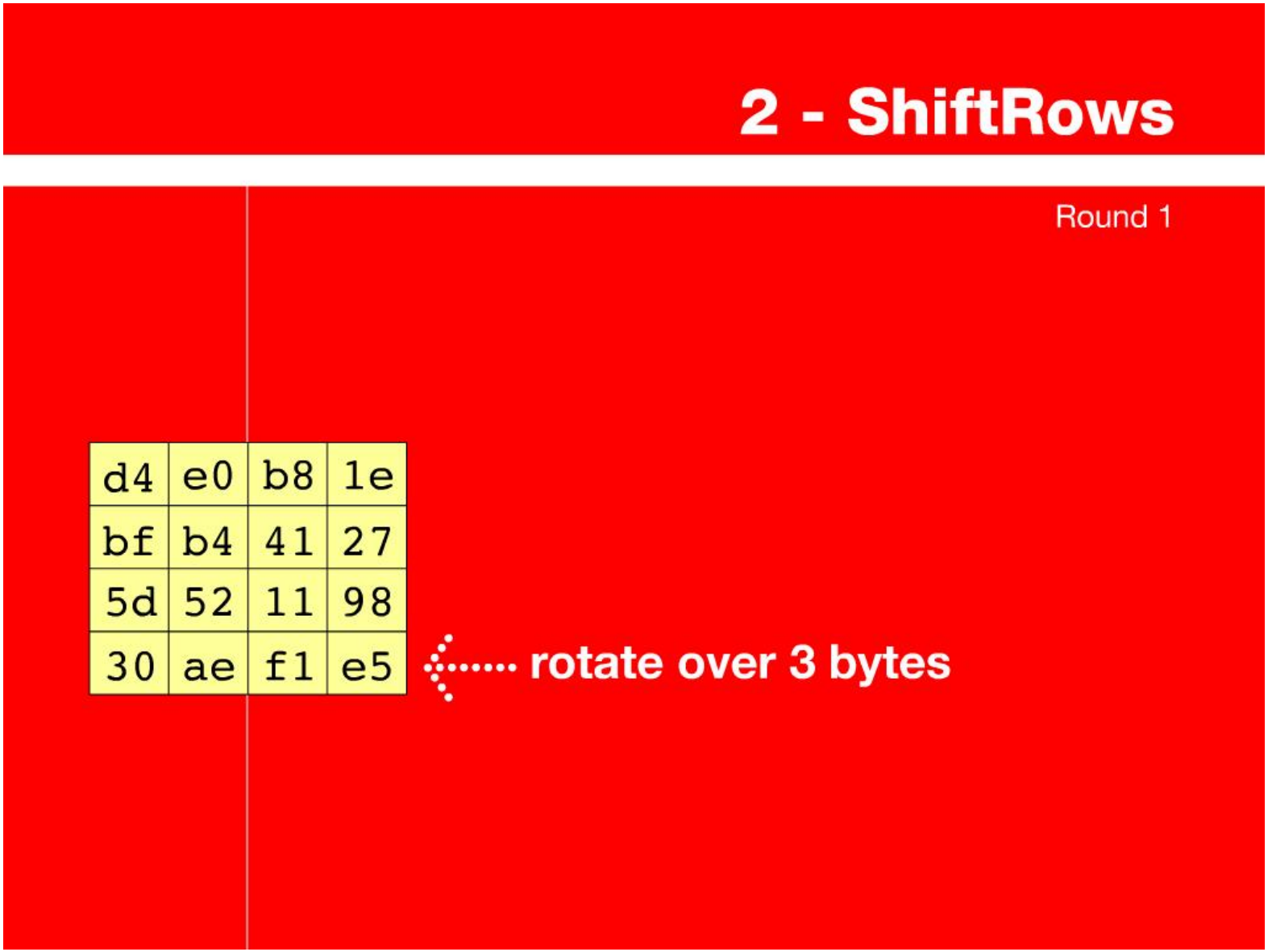
AES-Rijndael : les détails



AES-Rijndael : les détails



AES-Rijndael : les détails



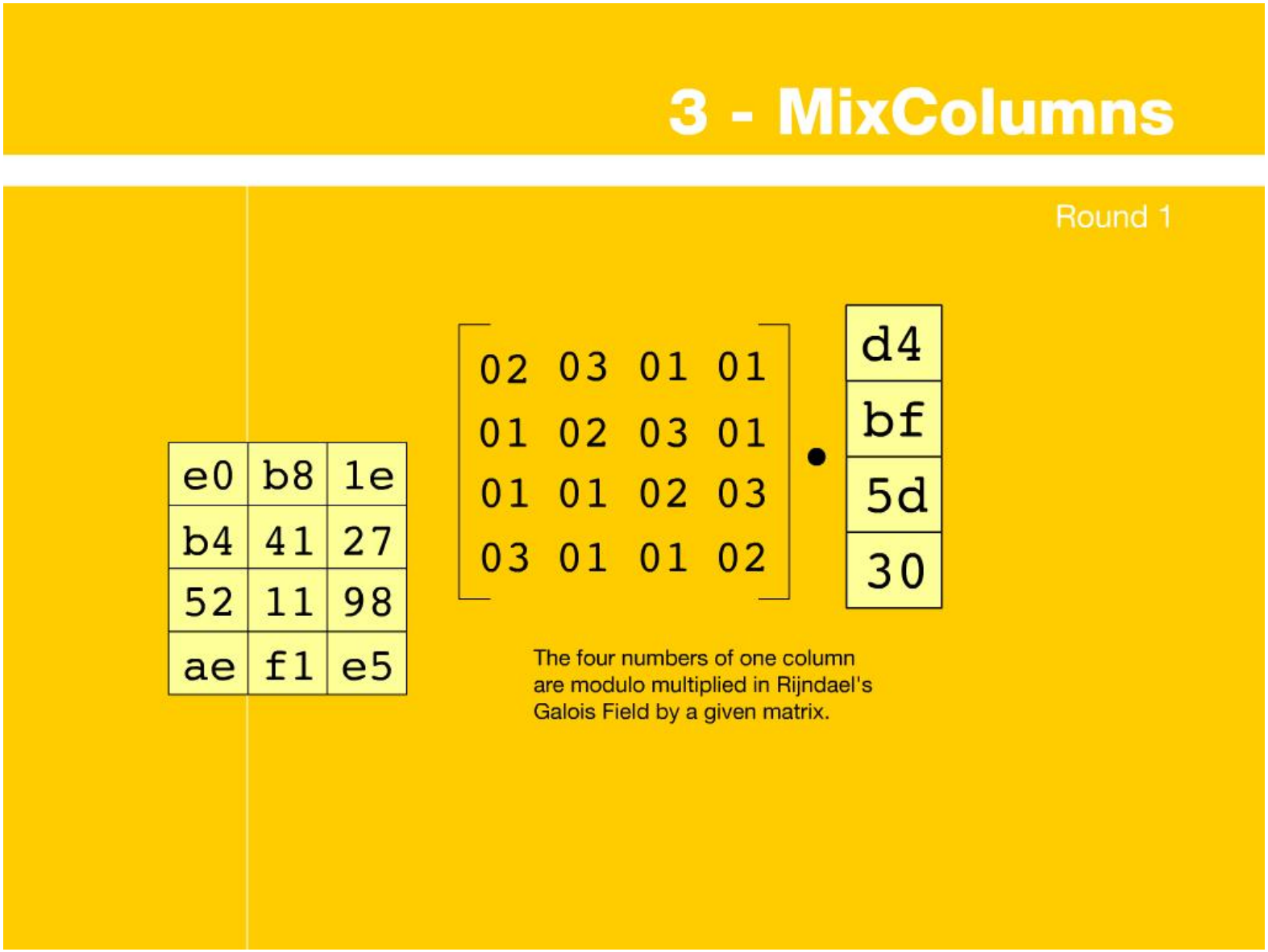
AES-Rijndael : les détails

3 - MixColumns

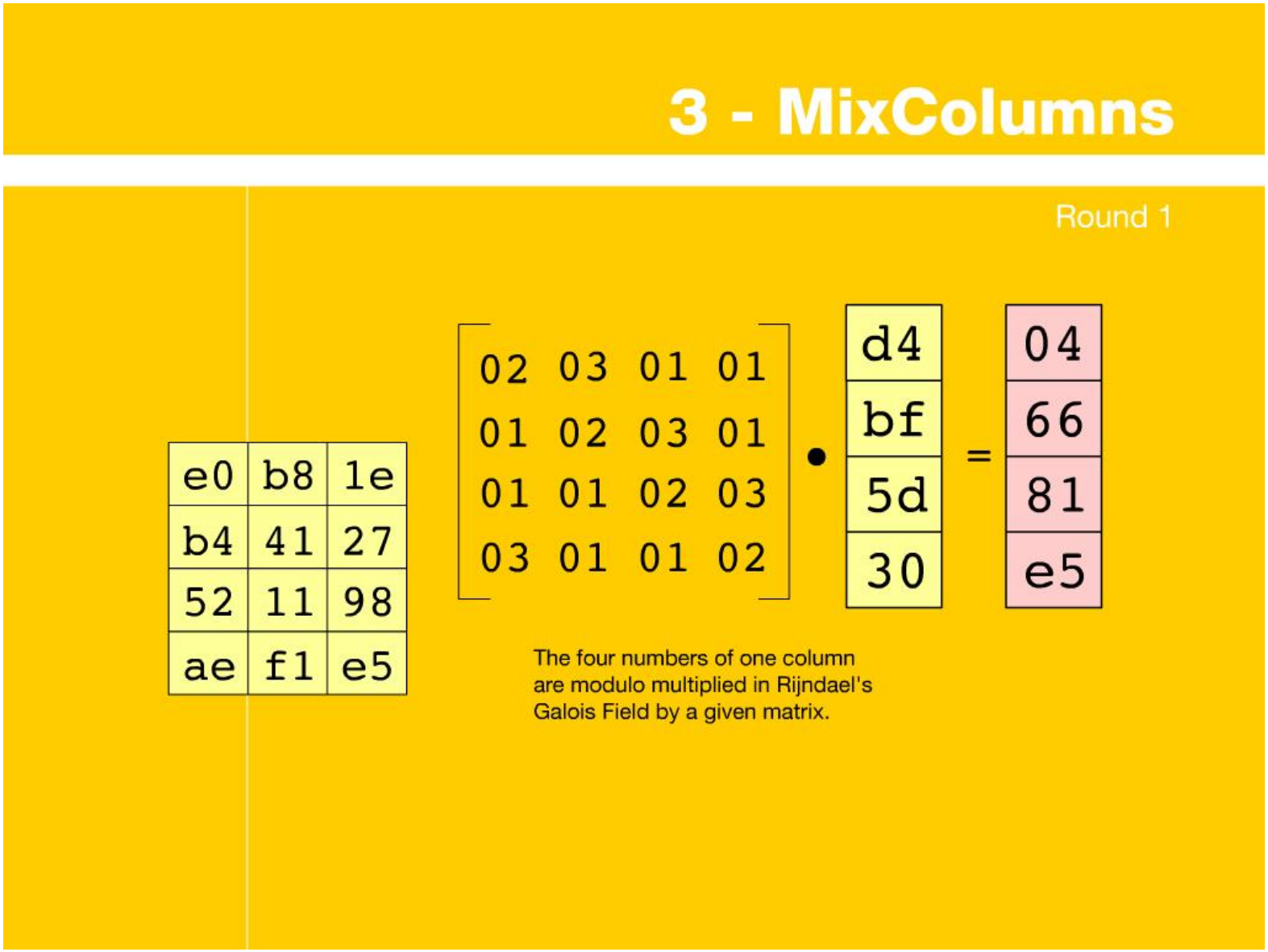
Round 1

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

AES-Rijndael : les détails



AES-Rijndael : les détails



AES-Rijndael : les détails

3 - MixColumns

Round 1

04	e0	b8	1e
66	b4	41	27
81	52	11	98
e5	ae	f1	e5

The MixColumns step along with the ShiftRows step is the primary source of diffusion in Rijndael.

AES-Rijndael : les détails

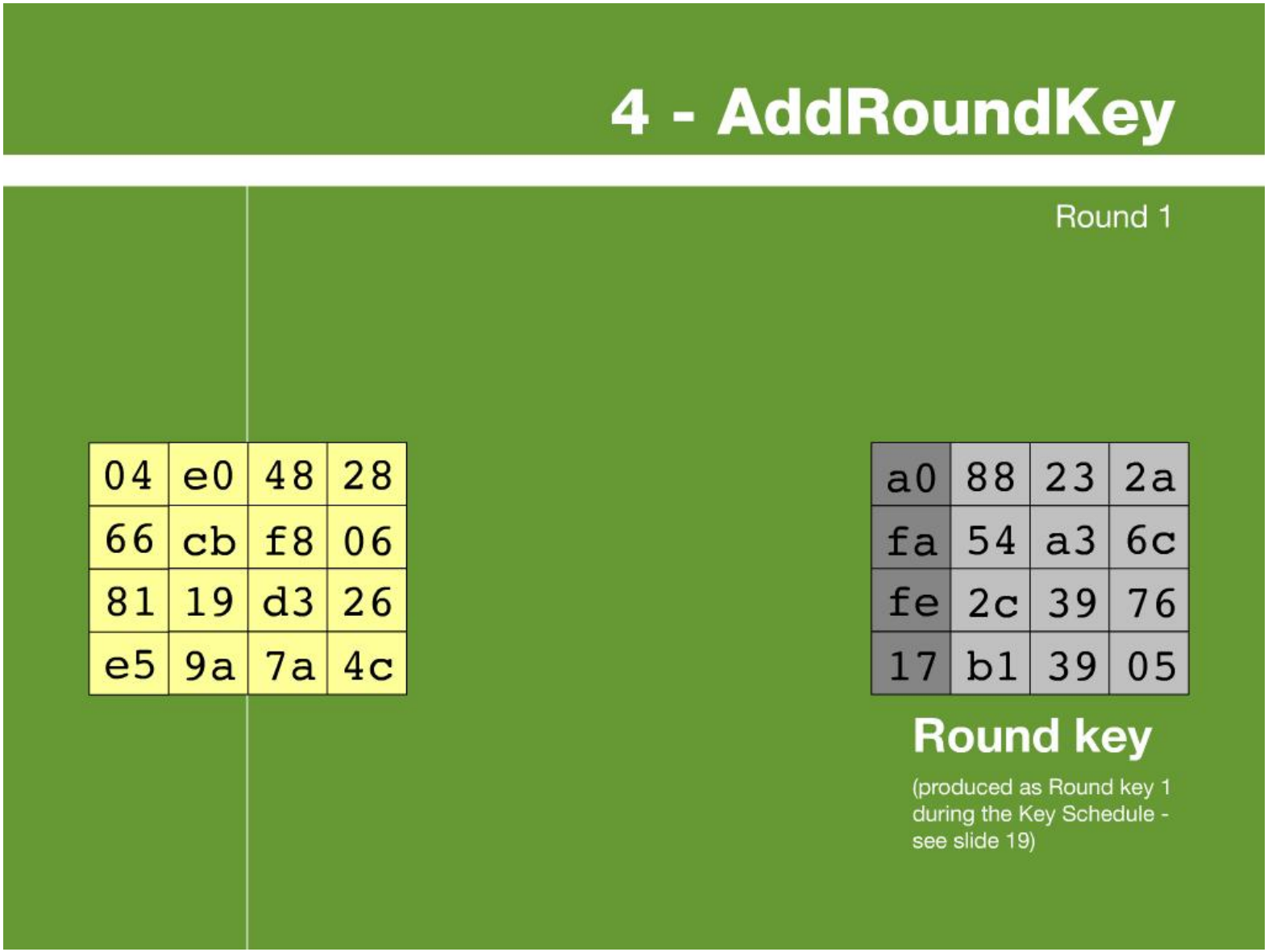
3 - MixColumns

Round 1

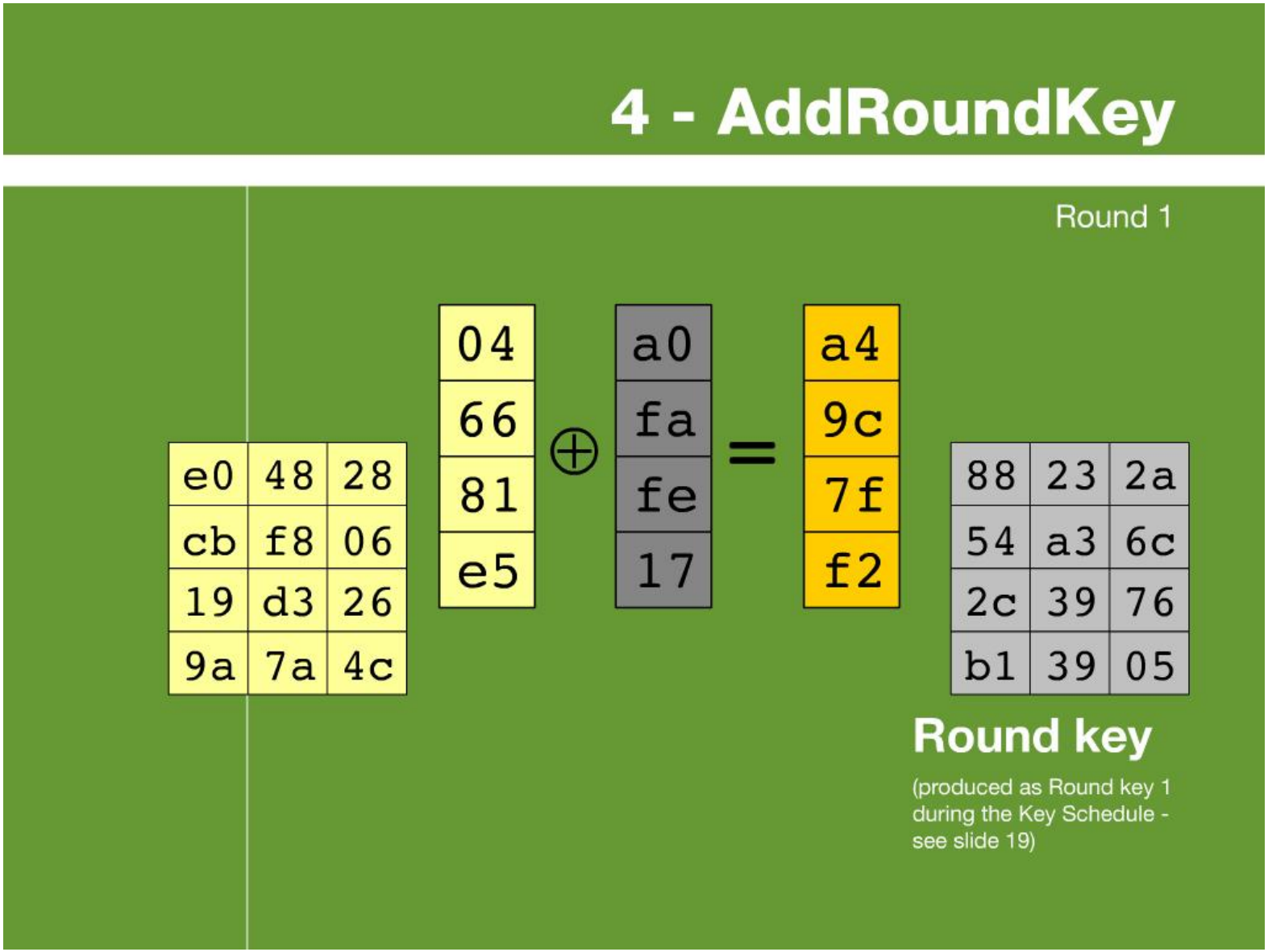
04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

The MixColumns step along with the ShiftRows step is the primary source of diffusion in Rijndael.

AES-Rijndael : les détails



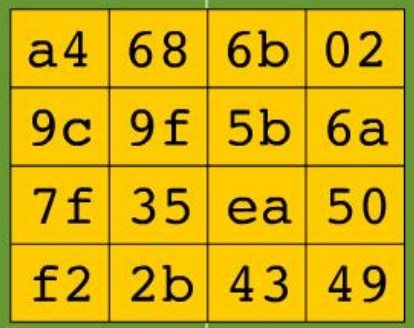
AES-Rijndael : les détails



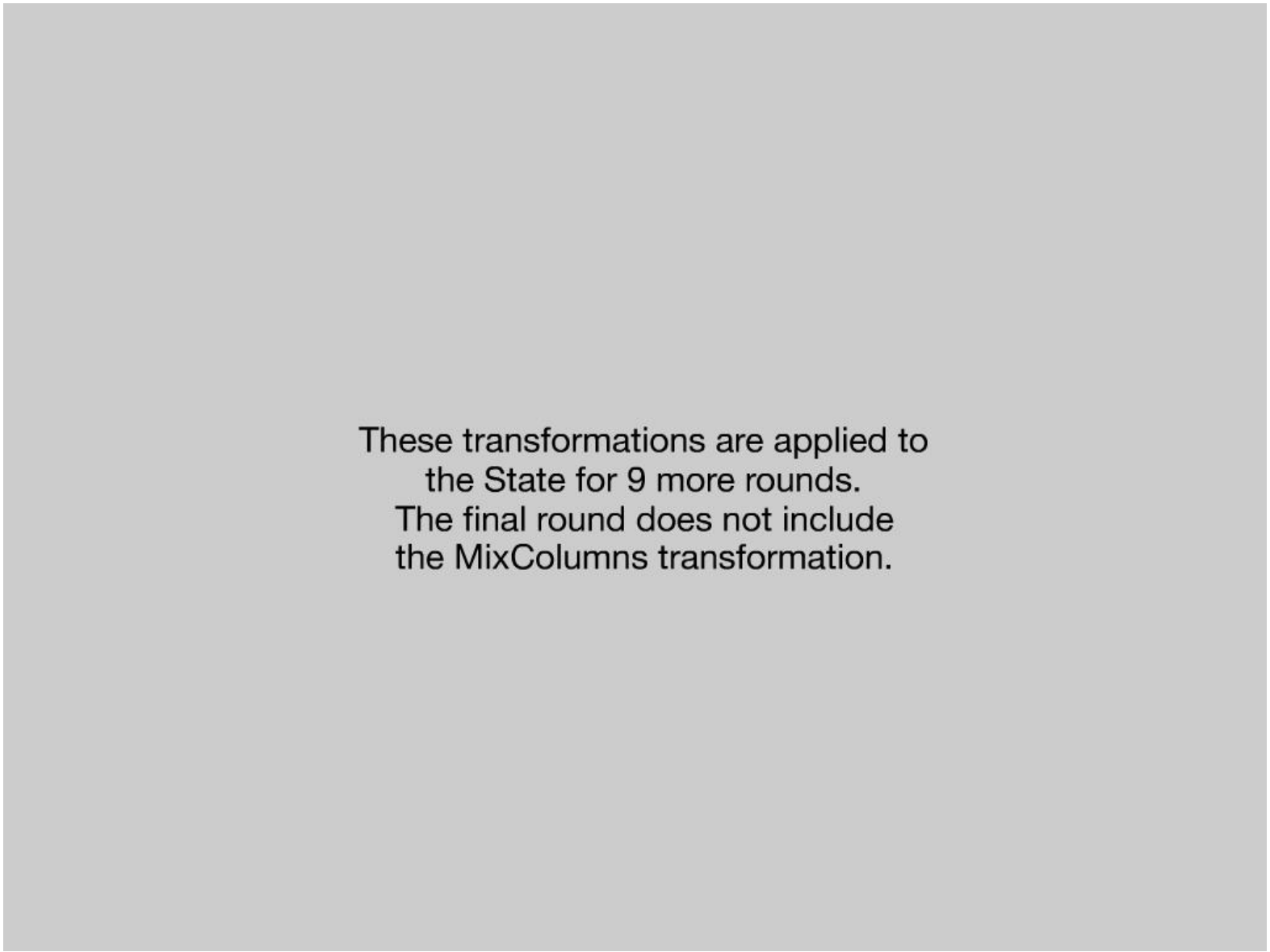
AES-Rijndael : les détails

4 - AddRoundKey

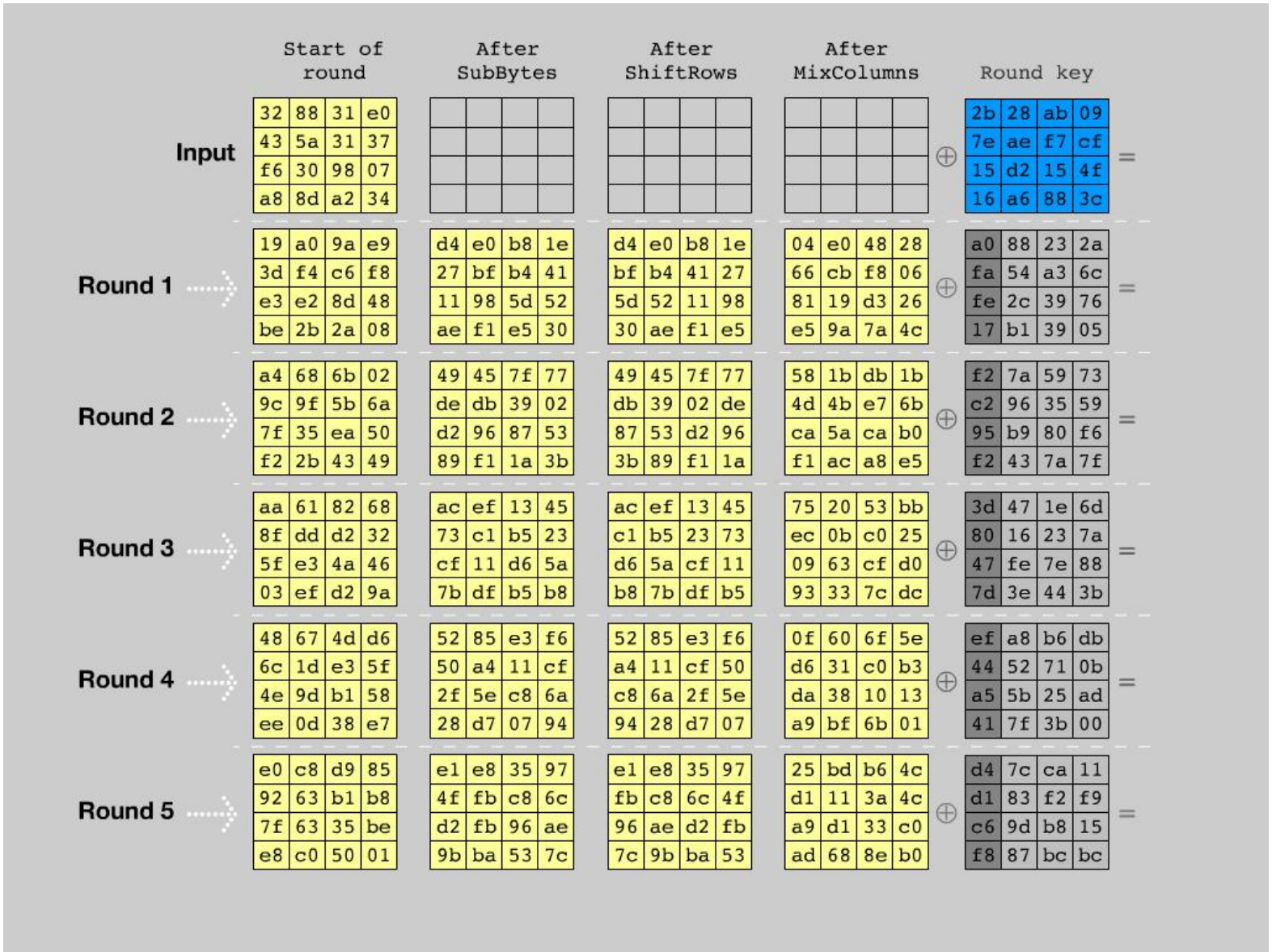
Round 1



AES-Rijndael : les détails

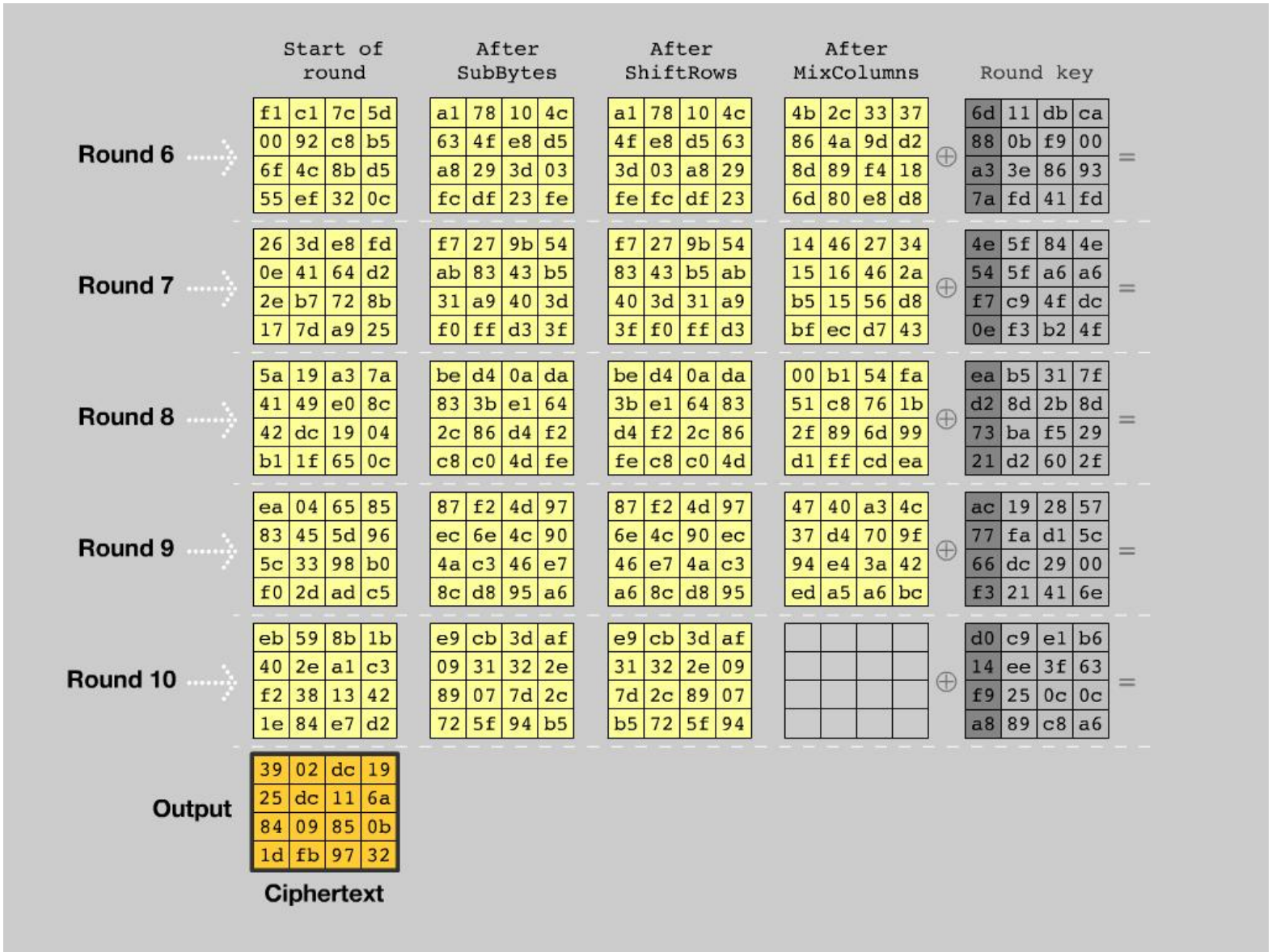


AES-Rijndael : les détails

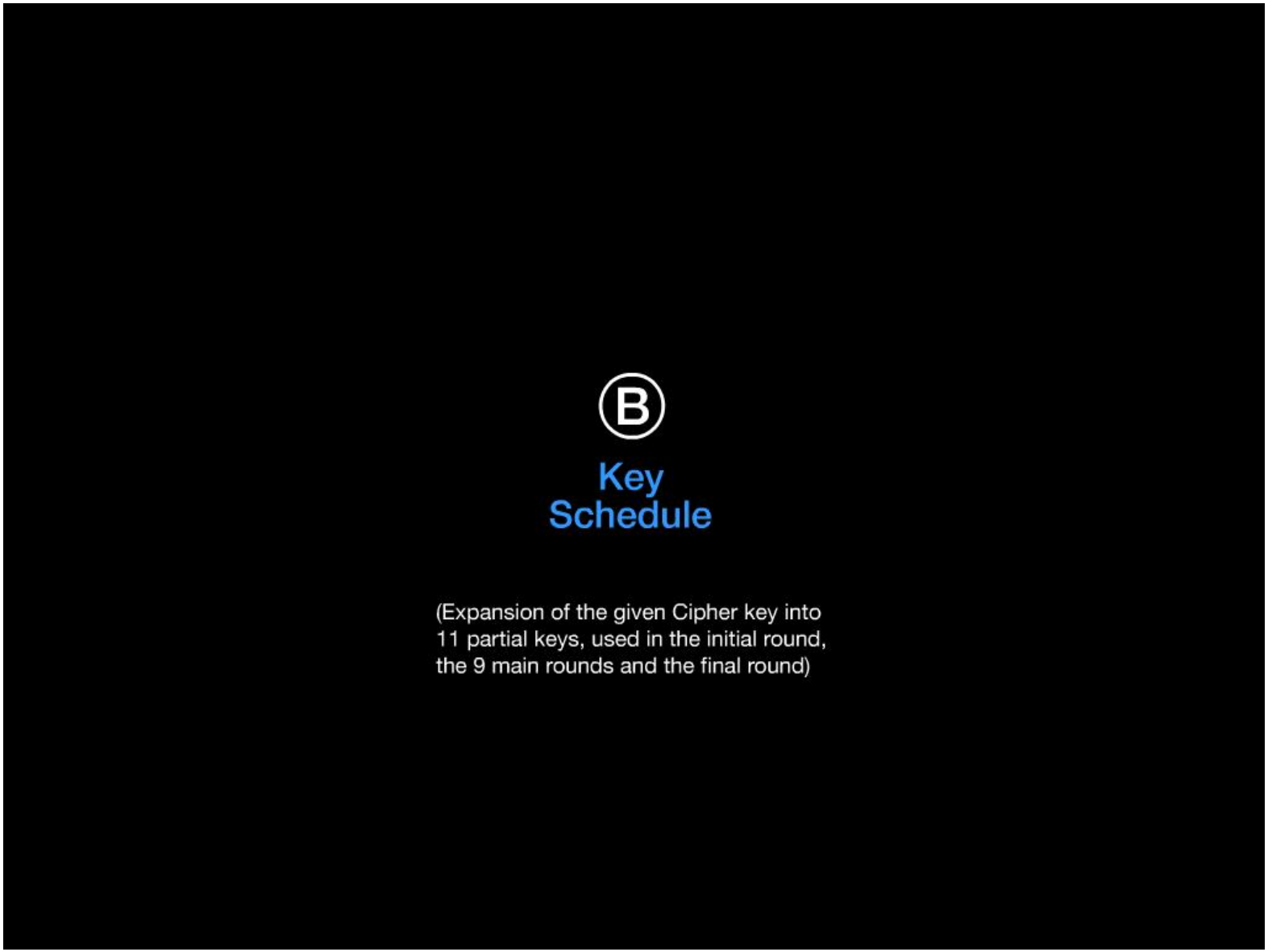


	Start of round	After SubBytes	After ShiftRows	After MixColumns	Round key
Input	32 88 31 e0 43 5a 31 37 f6 30 98 07 a8 8d a2 34				2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c
Round 1	19 a0 9a e9 3d f4 c6 f8 e3 e2 8d 48 be 2b 2a 08	d4 e0 b8 1e 27 bf b4 41 11 98 5d 52 ae f1 e5 30	d4 e0 b8 1e bf b4 41 27 5d 52 11 98 30 ae f1 e5	04 e0 48 28 66 cb f8 06 81 19 d3 26 e5 9a 7a 4c	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05
Round 2	a4 68 6b 02 9c 9f 5b 6a 7f 35 ea 50 f2 2b 43 49	49 45 7f 77 de db 39 02 d2 96 87 53 89 f1 1a 3b	49 45 7f 77 db 39 02 de 87 53 d2 96 3b 89 f1 1a	58 1b db 1b 4d 4b e7 6b ca 5a ca b0 f1 ac a8 e5	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f
Round 3	aa 61 82 68 8f dd d2 32 5f e3 4a 46 03 ef d2 9a	ac ef 13 45 73 c1 b5 23 cf 11 d6 5a 7b df b5 b8	ac ef 13 45 c1 b5 23 73 d6 5a cf 11 b8 7b df b5	75 20 53 bb ec 0b c0 25 09 63 cf d0 93 33 7c dc	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b
Round 4	48 67 4d d6 6c 1d e3 5f 4e 9d b1 58 ee 0d 38 e7	52 85 e3 f6 50 a4 11 cf 2f 5e c8 6a 28 d7 07 94	52 85 e3 f6 a4 11 cf 50 c8 6a 2f 5e 94 28 d7 07	0f 60 6f 5e d6 31 c0 b3 da 38 10 13 a9 bf 6b 01	ef a8 b6 db 44 52 71 0b a5 5b 25 ad 41 7f 3b 00
Round 5	e0 c8 d9 85 92 63 b1 b8 7f 63 35 be e8 c0 50 01	e1 e8 35 97 4f fb c8 6c d2 fb 96 ae 9b ba 53 7c	e1 e8 35 97 fb c8 6c 4f 96 ae d2 fb 7c 9b ba 53	25 bd b6 4c d1 11 3a 4c a9 d1 33 c0 ad 68 8e b0	d4 7c ca 11 d1 83 f2 f9 c6 9d b8 15 f8 87 bc bc

AES-Rijndael : les détails

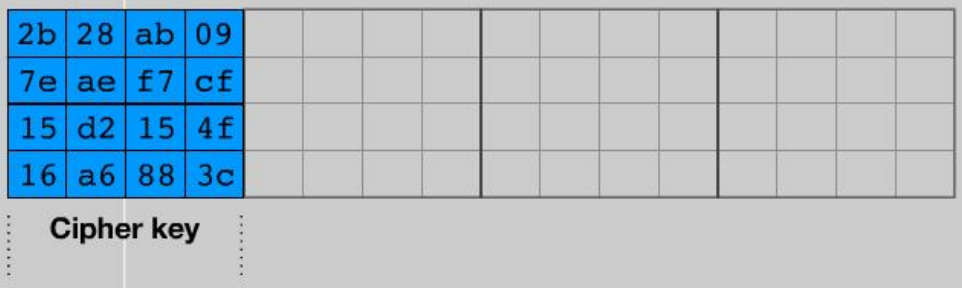


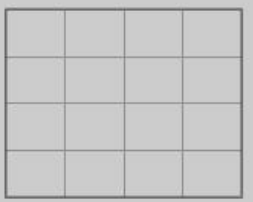
AES-Rijndael : les détails



AES-Rijndael : les détails

Key Schedule



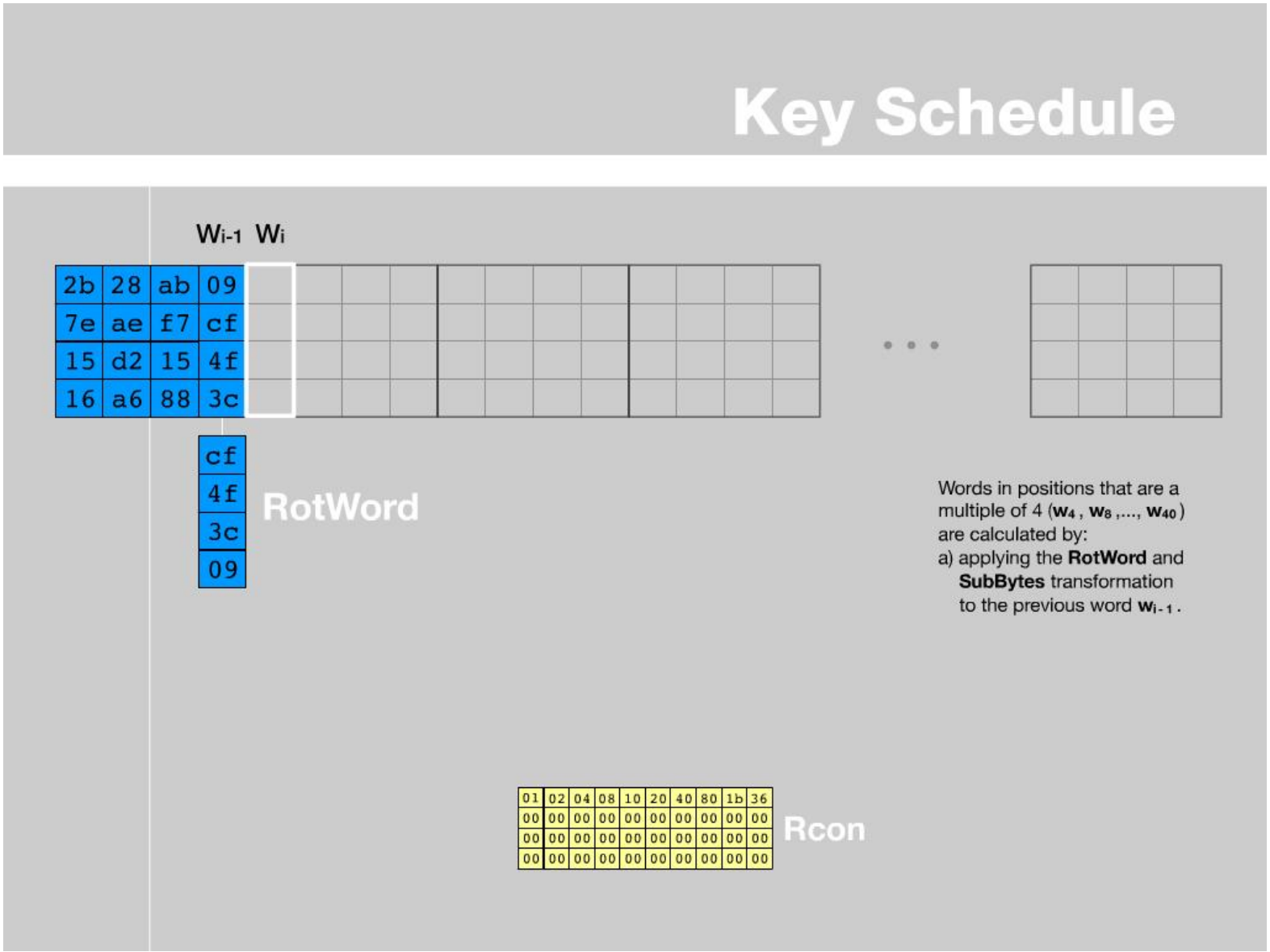


The expanded key can be seen as an array of 32-bit words (columns), numbered from 0 to 43.
The first four columns are filled with the given Cipher key.

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

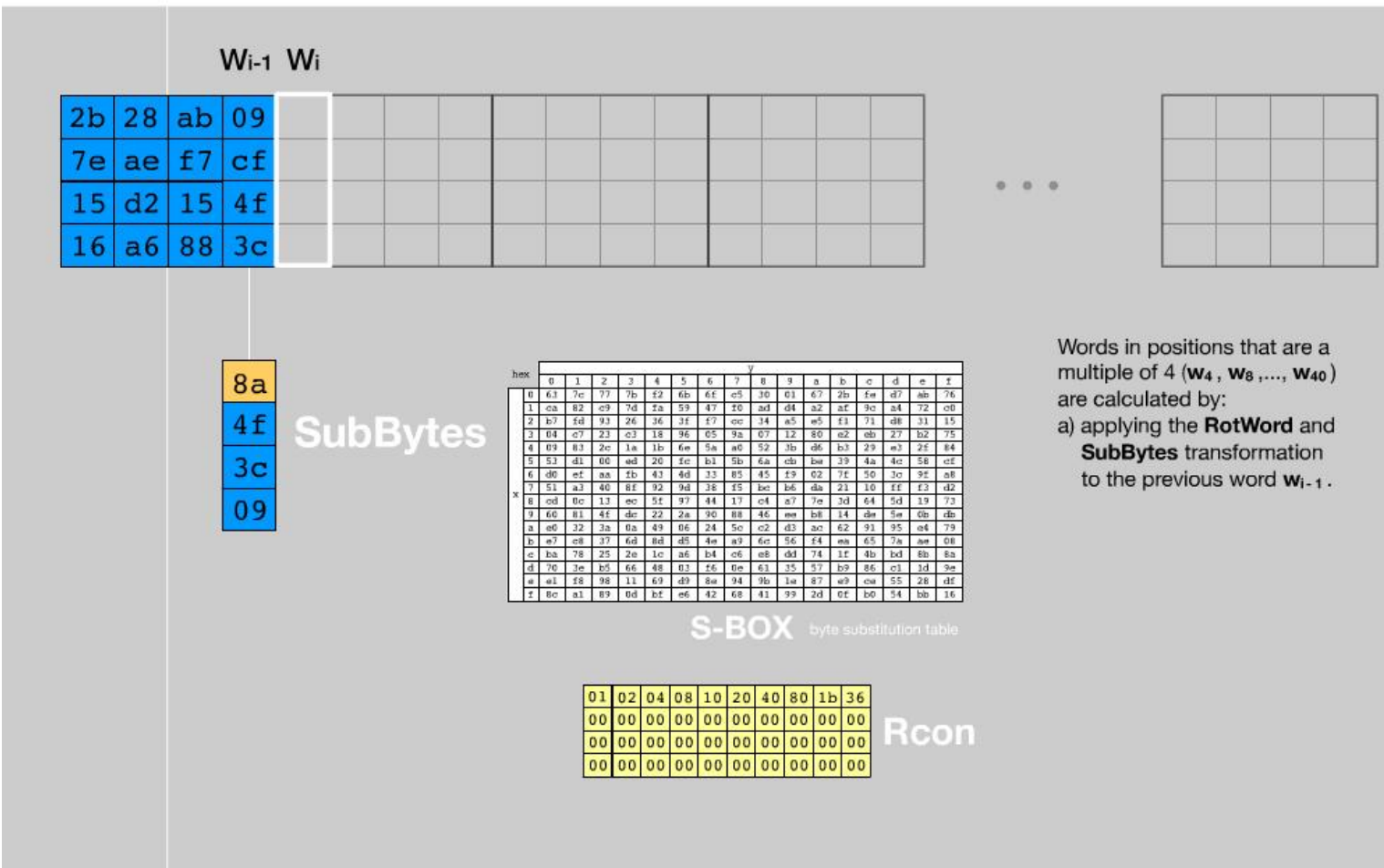
Rcon

AES-Rijndael : les détails

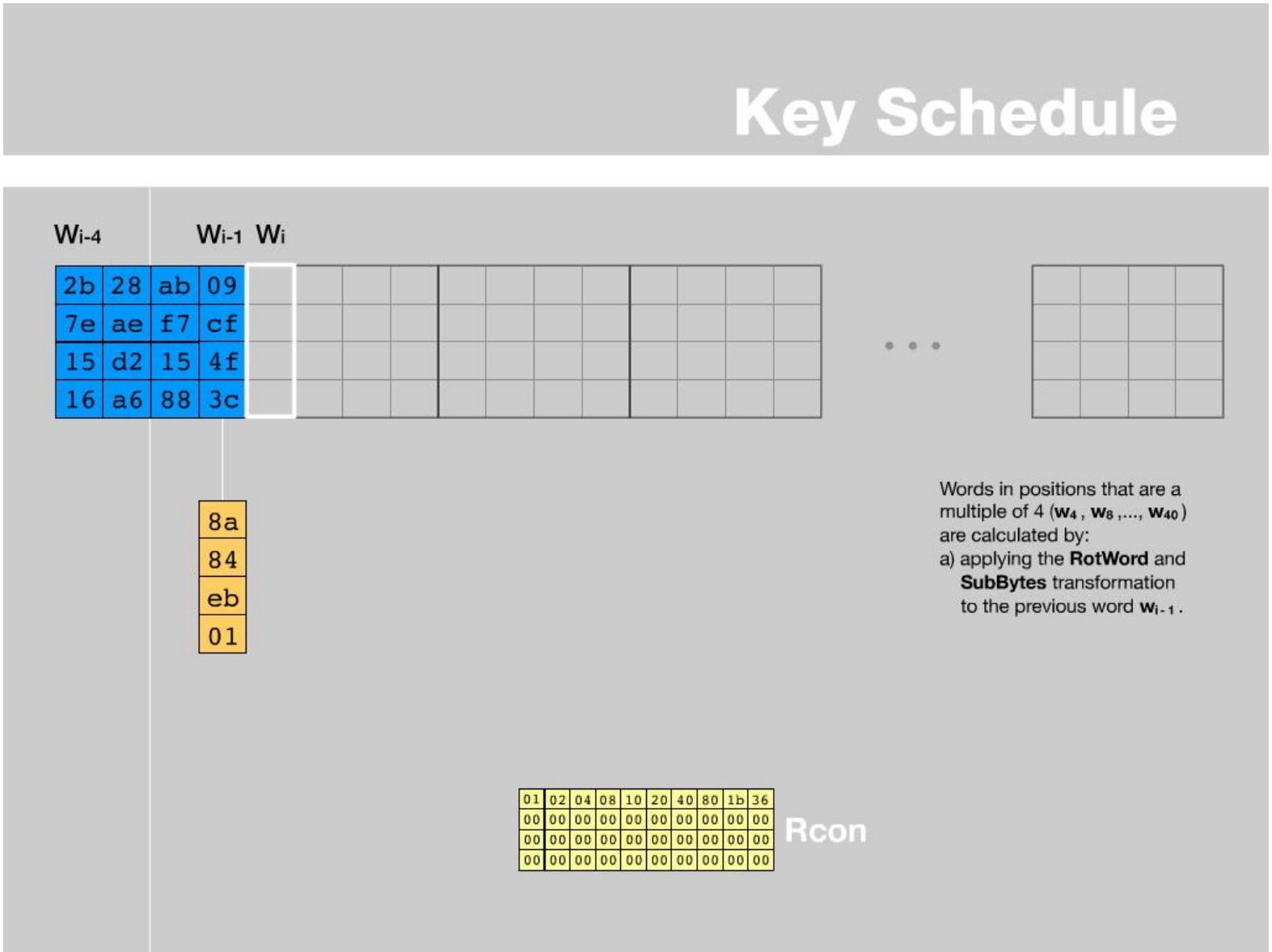


AES-Rijndael : les détails

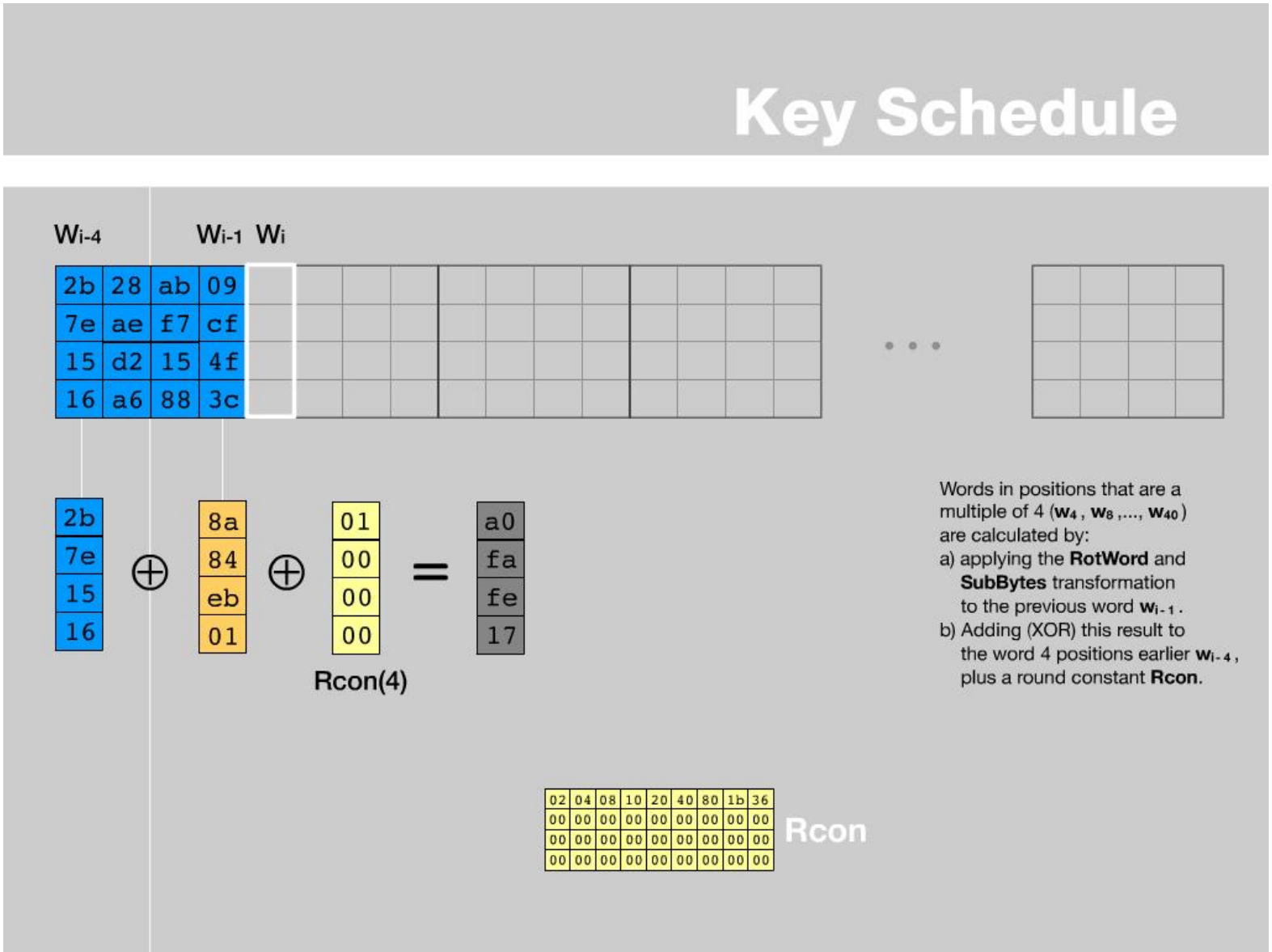
Key Schedule



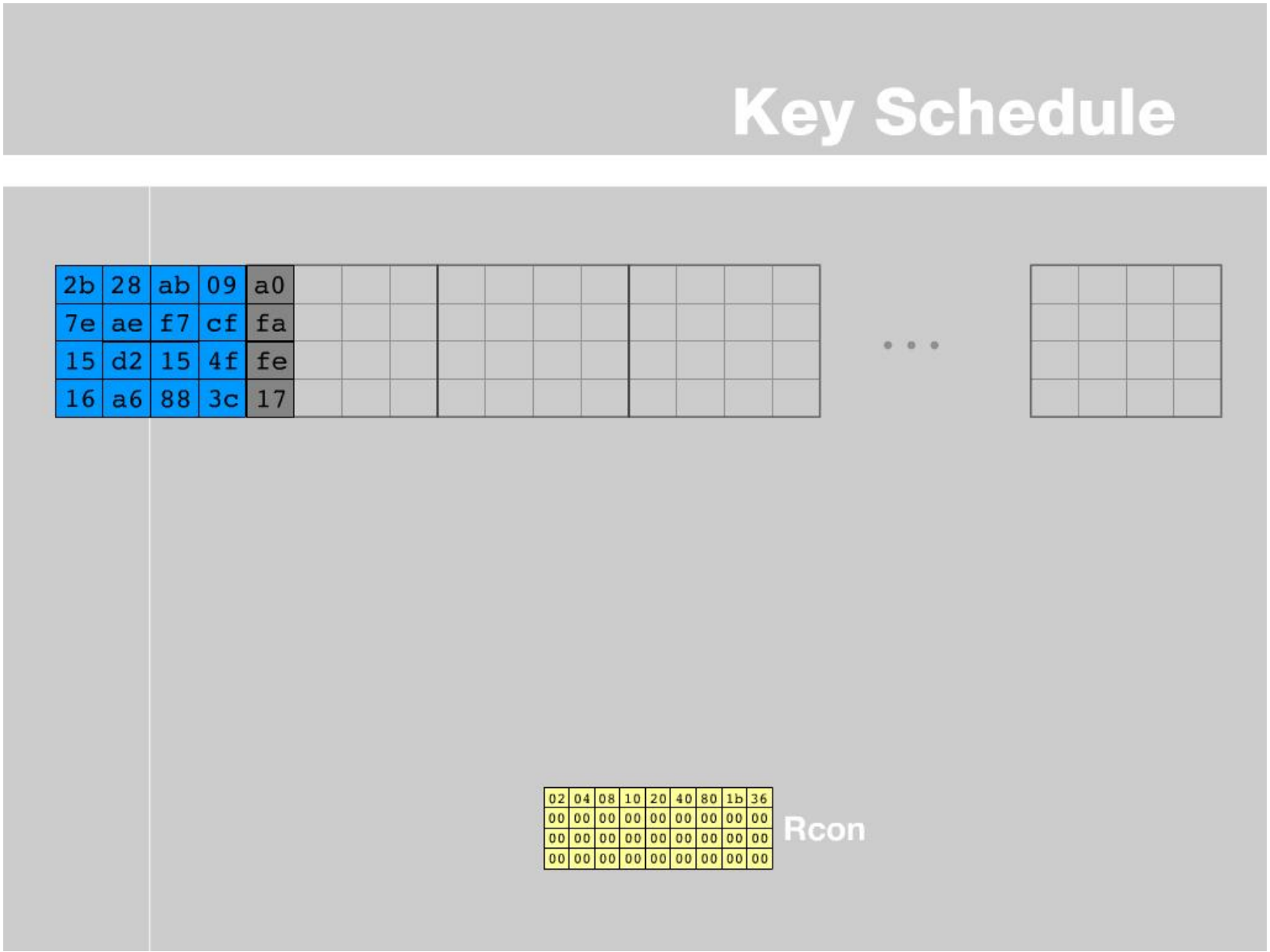
AES-Rijndael : les détails



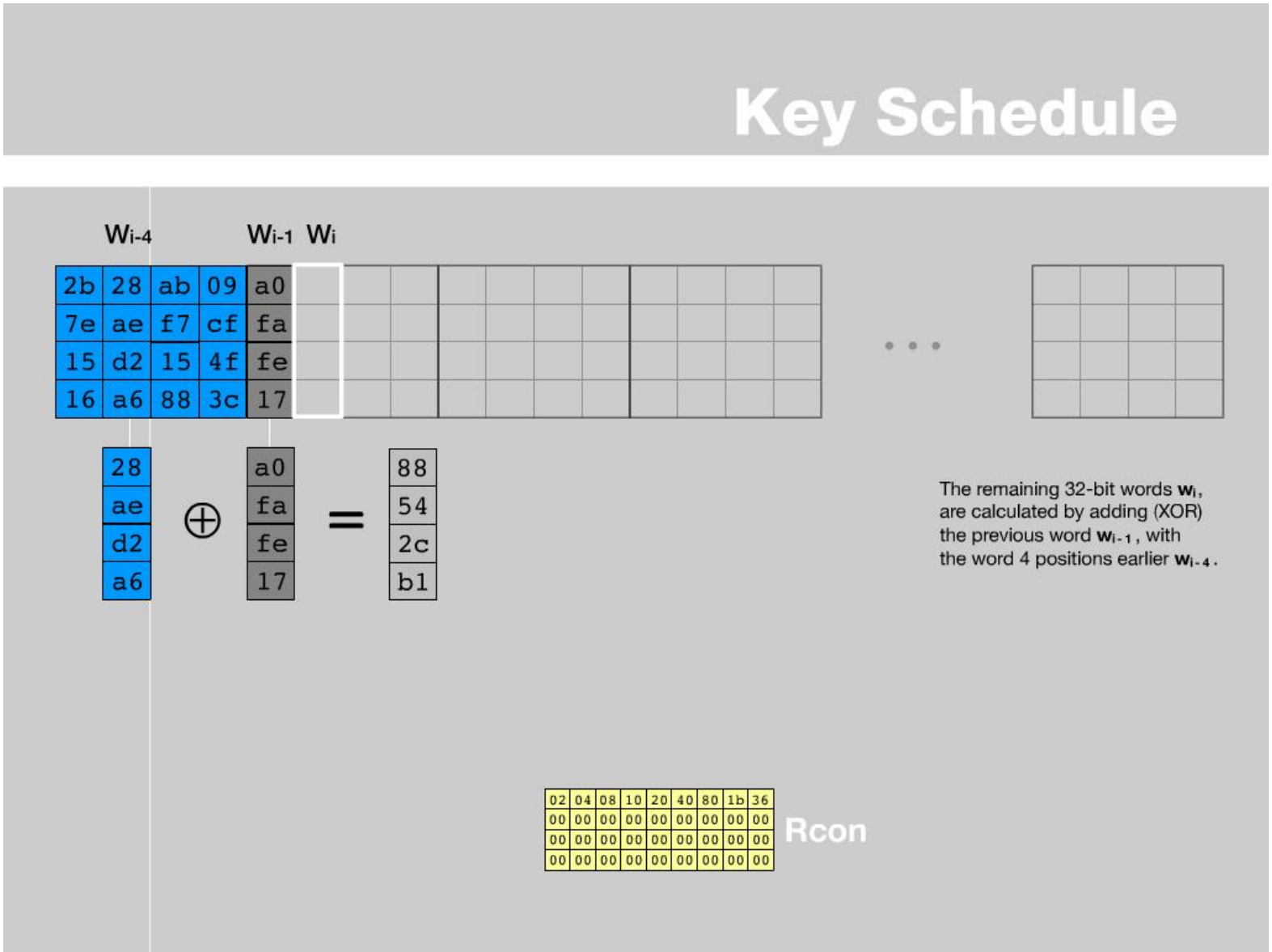
AES-Rijndael : les détails



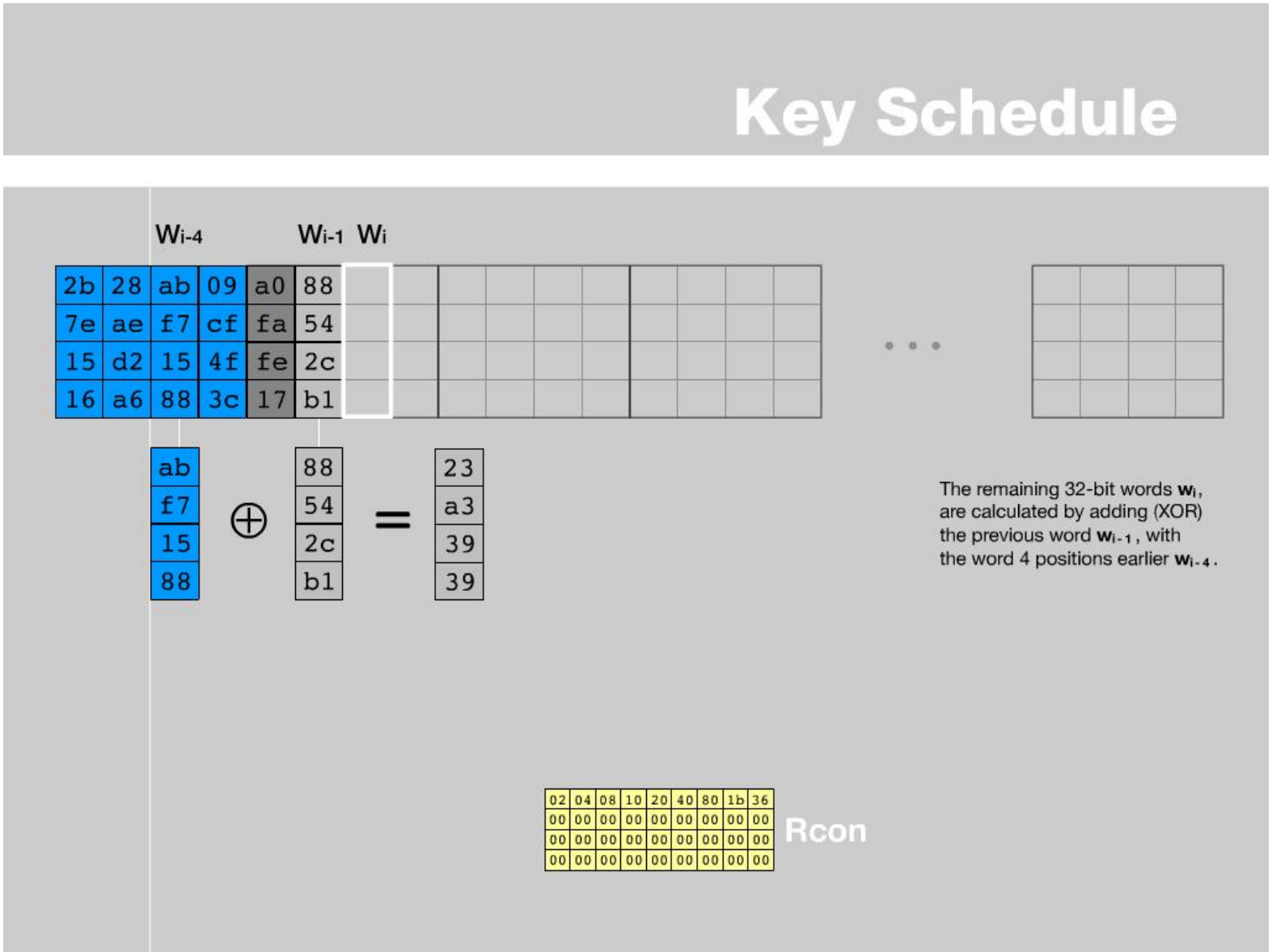
AES-Rijndael : les détails



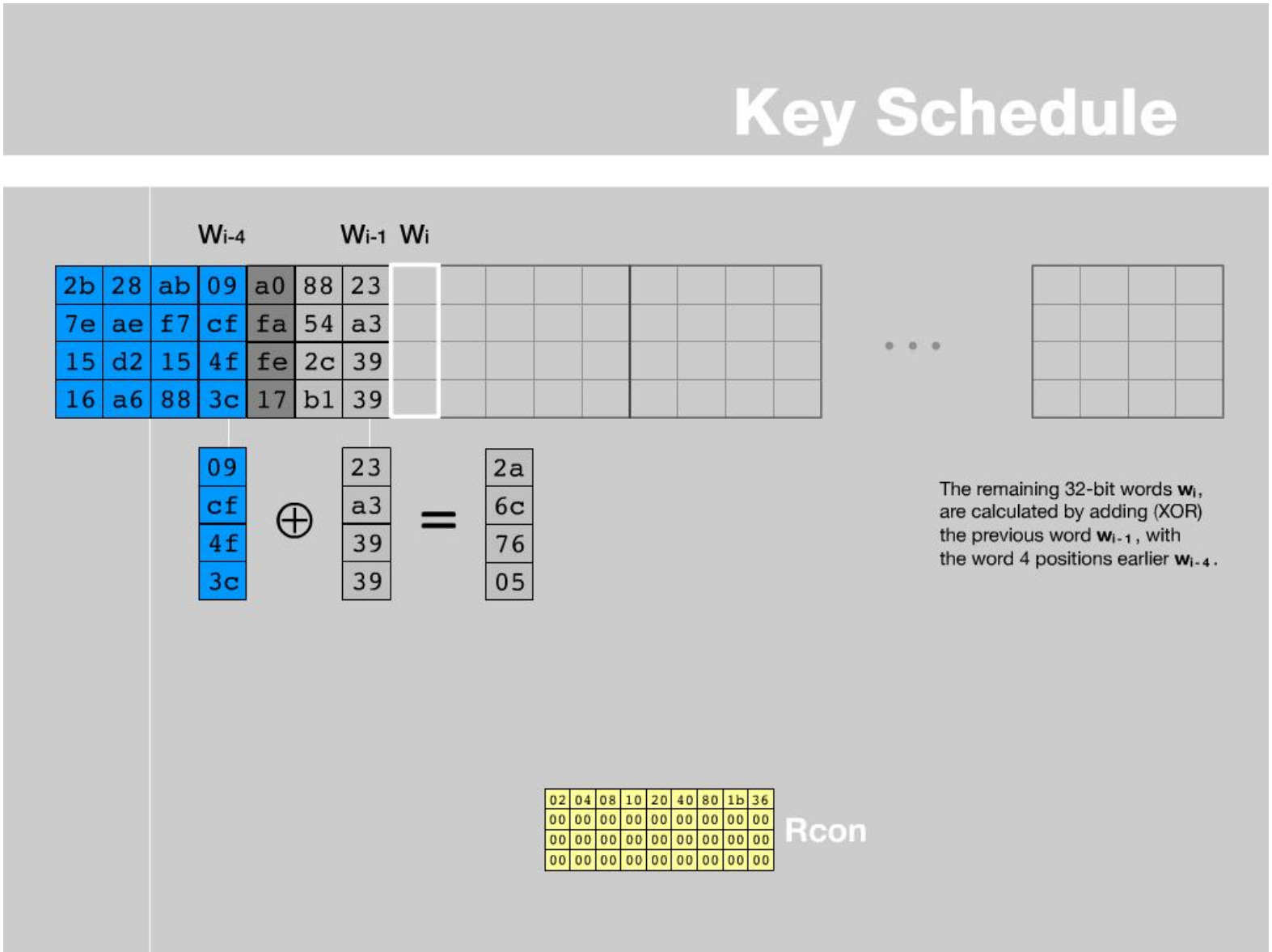
AES-Rijndael : les détails



AES-Rijndael : les détails

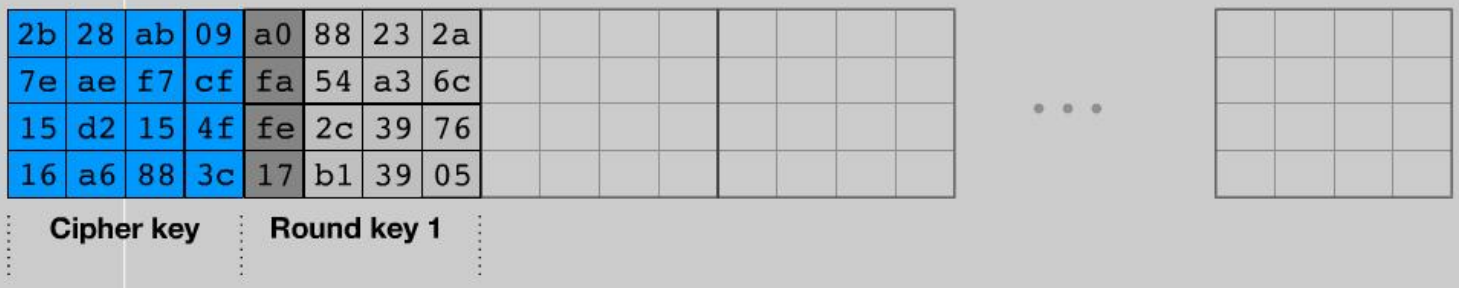


AES-Rijndael : les détails



AES-Rijndael : les détails

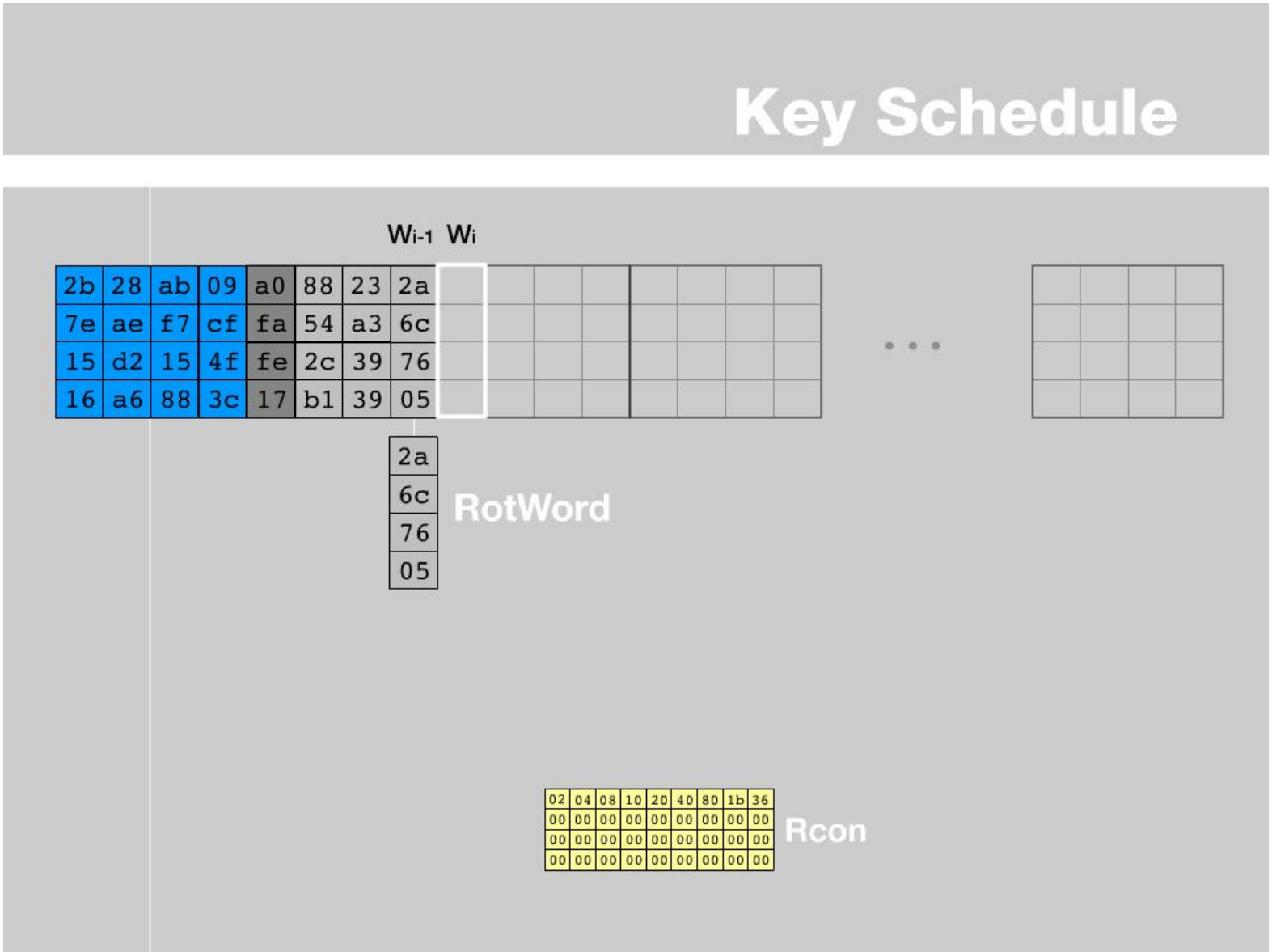
Key Schedule



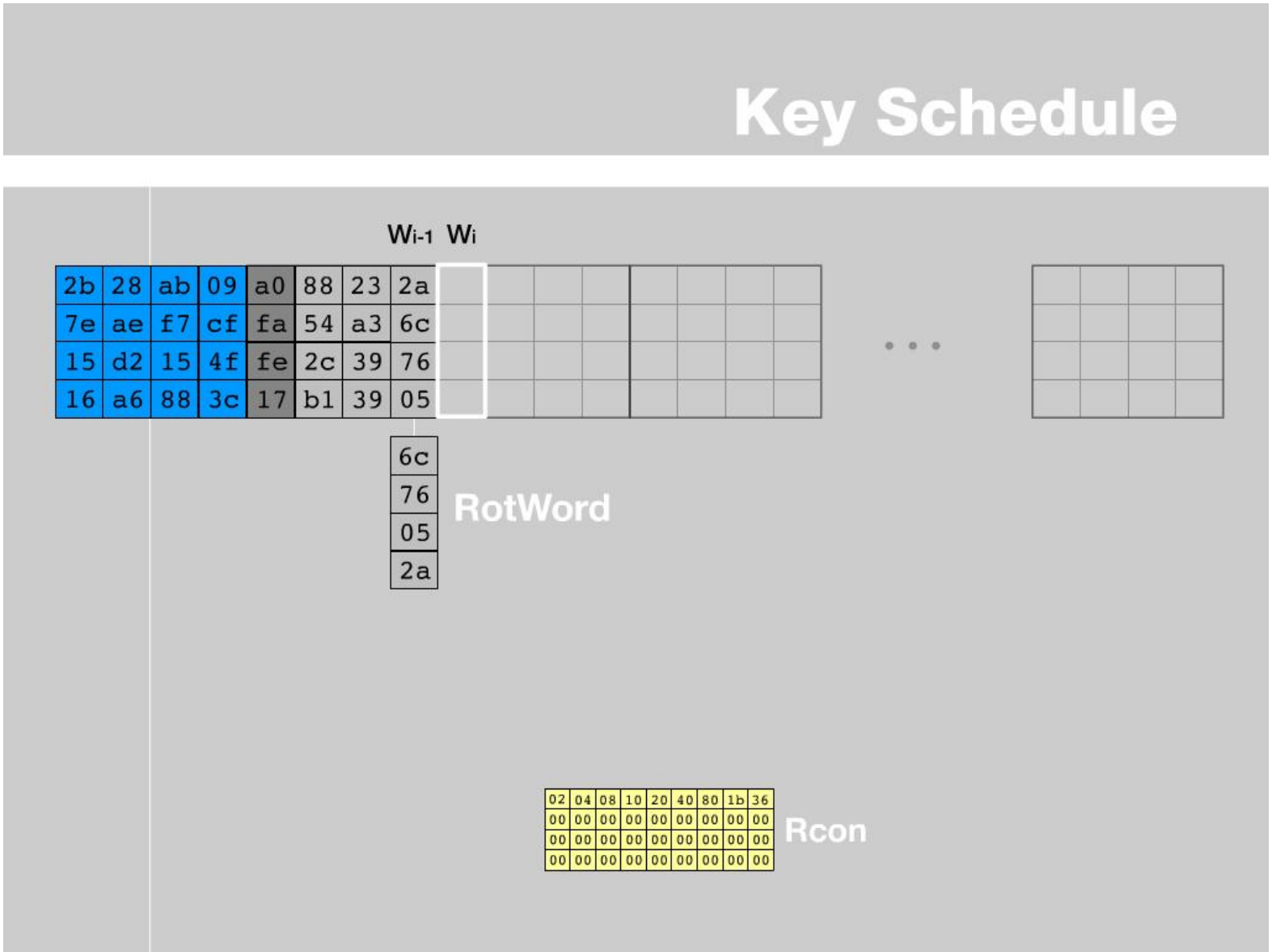
02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00

Rcon

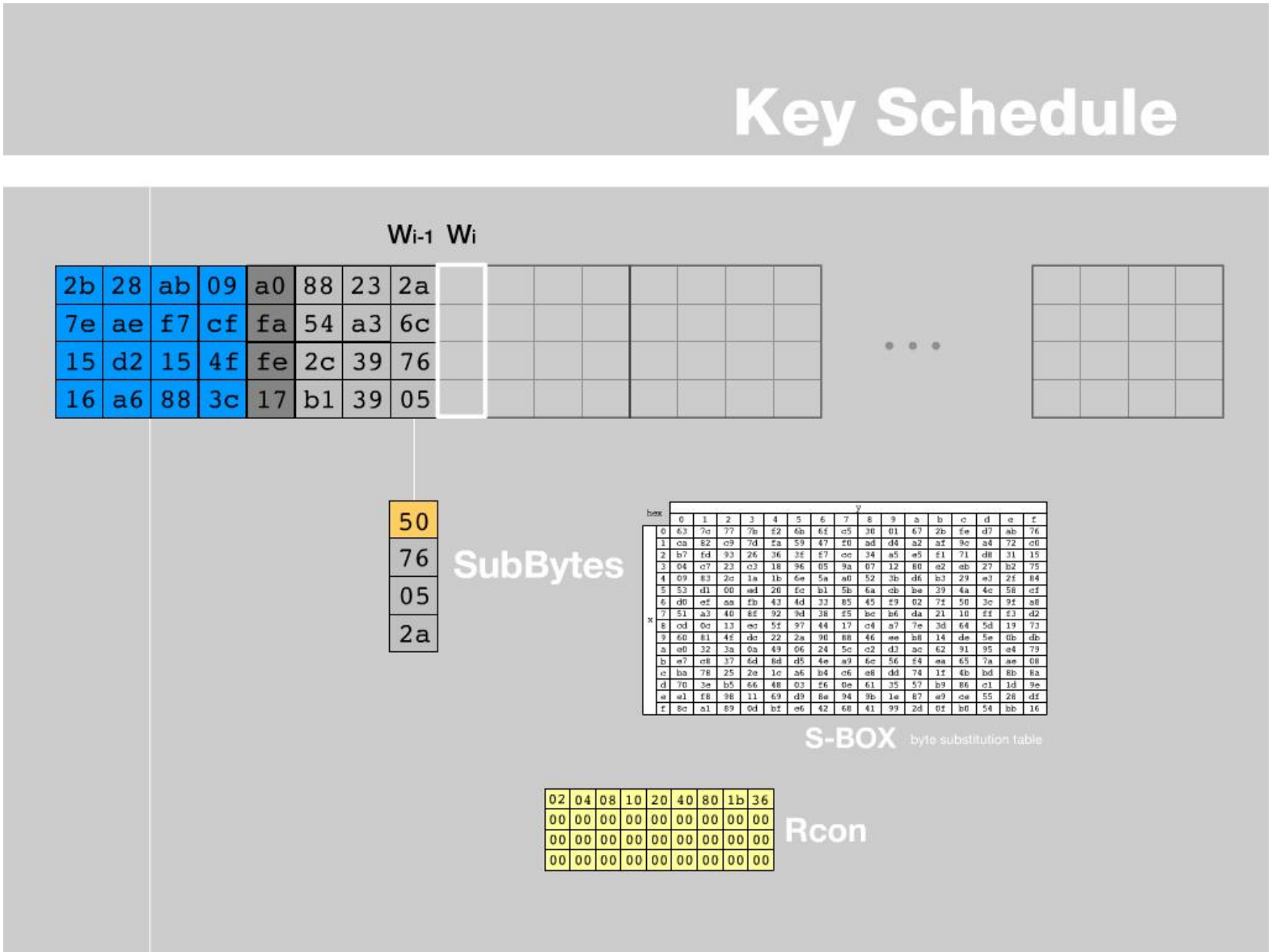
AES-Rijndael : les détails



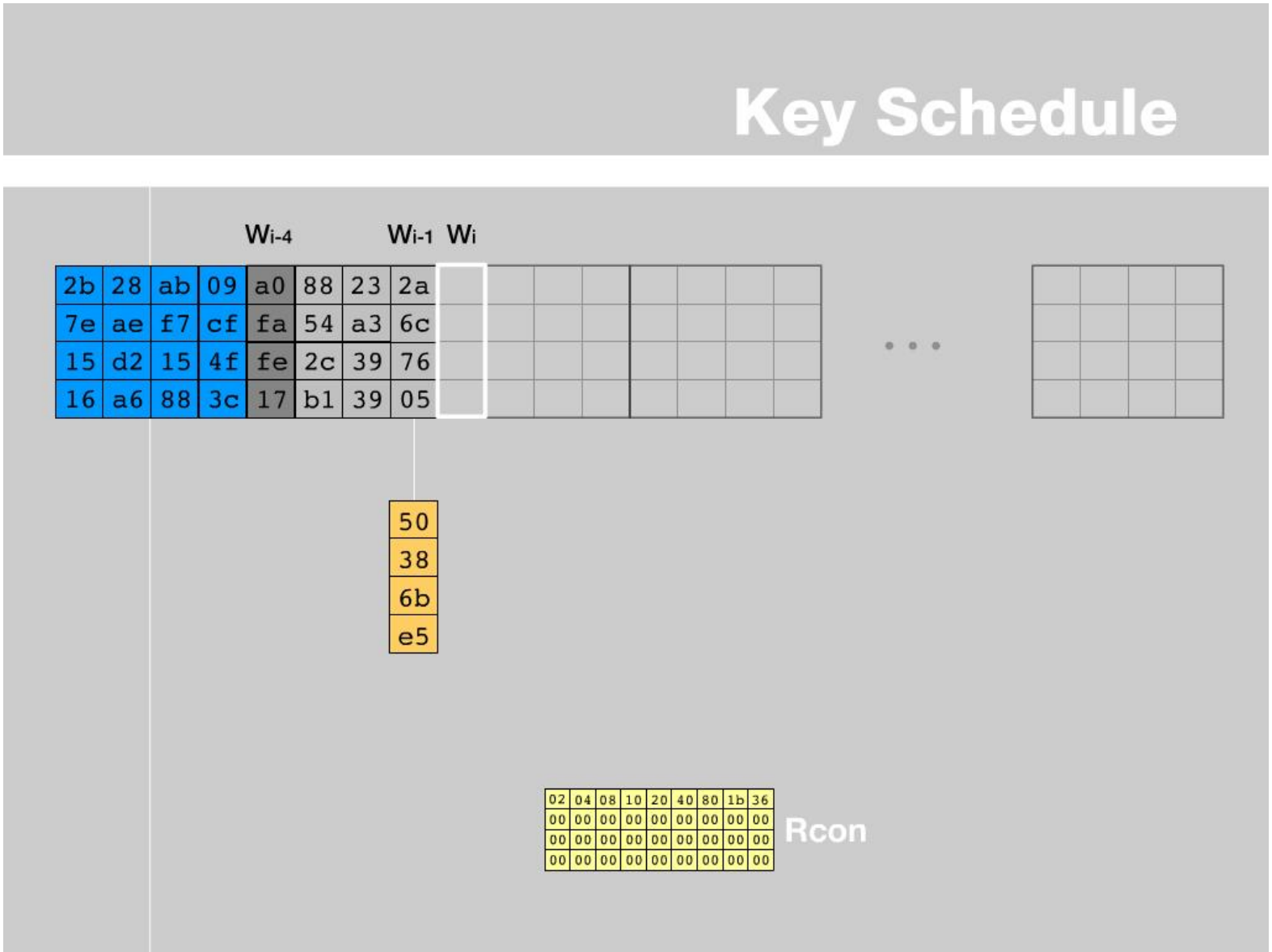
AES-Rijndael : les détails



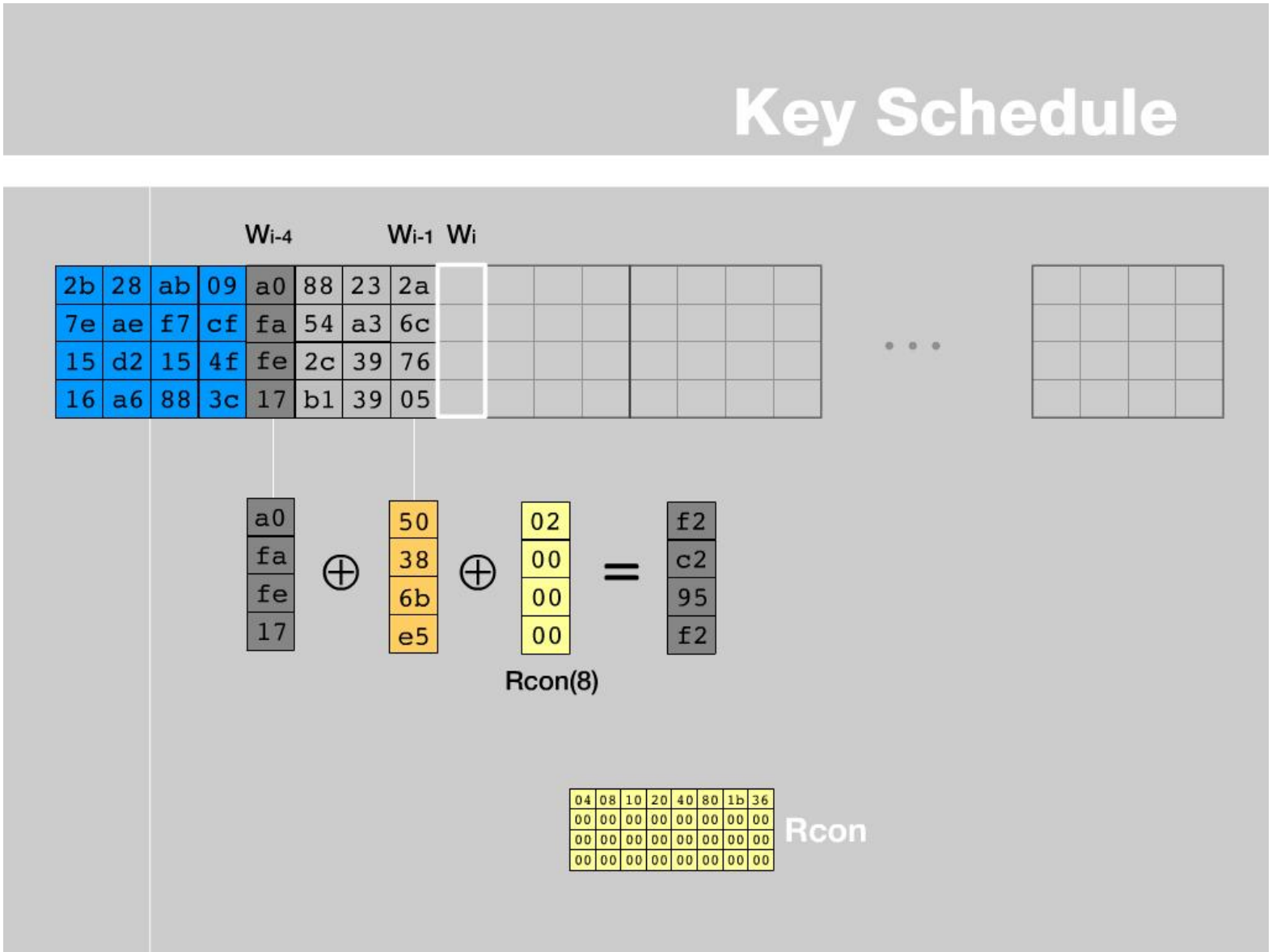
AES-Rijndael : les détails



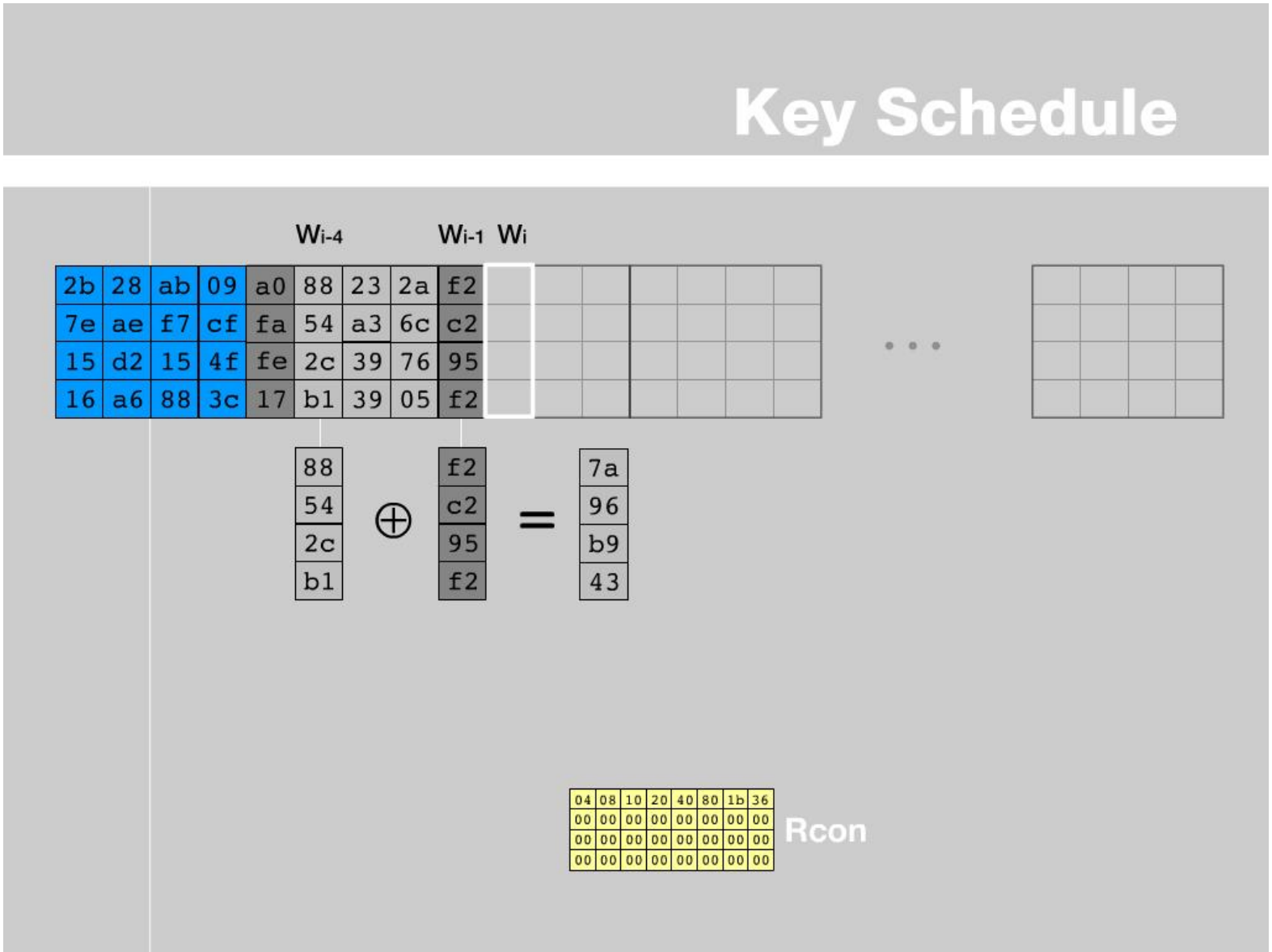
AES-Rijndael : les détails



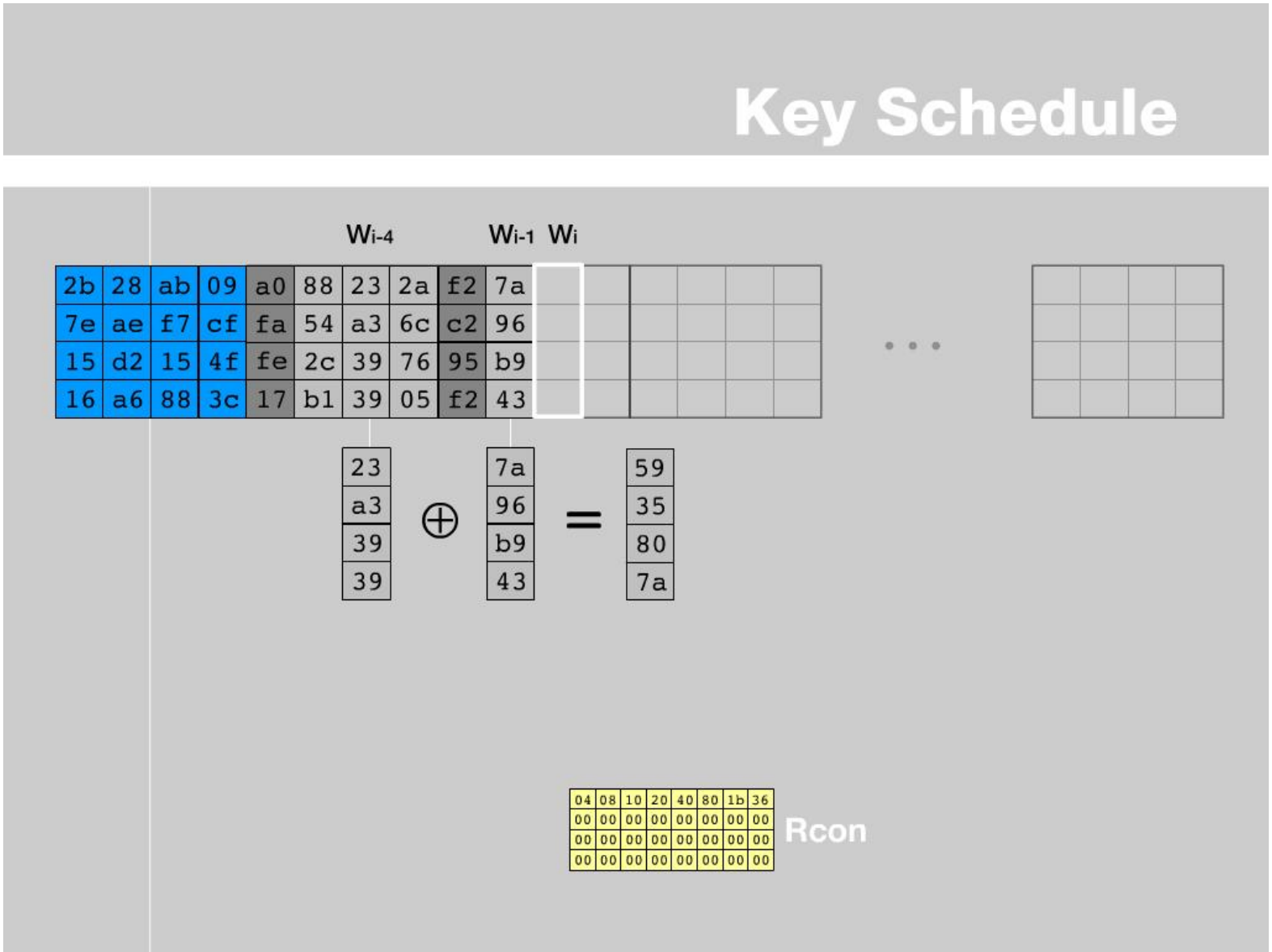
AES-Rijndael : les détails



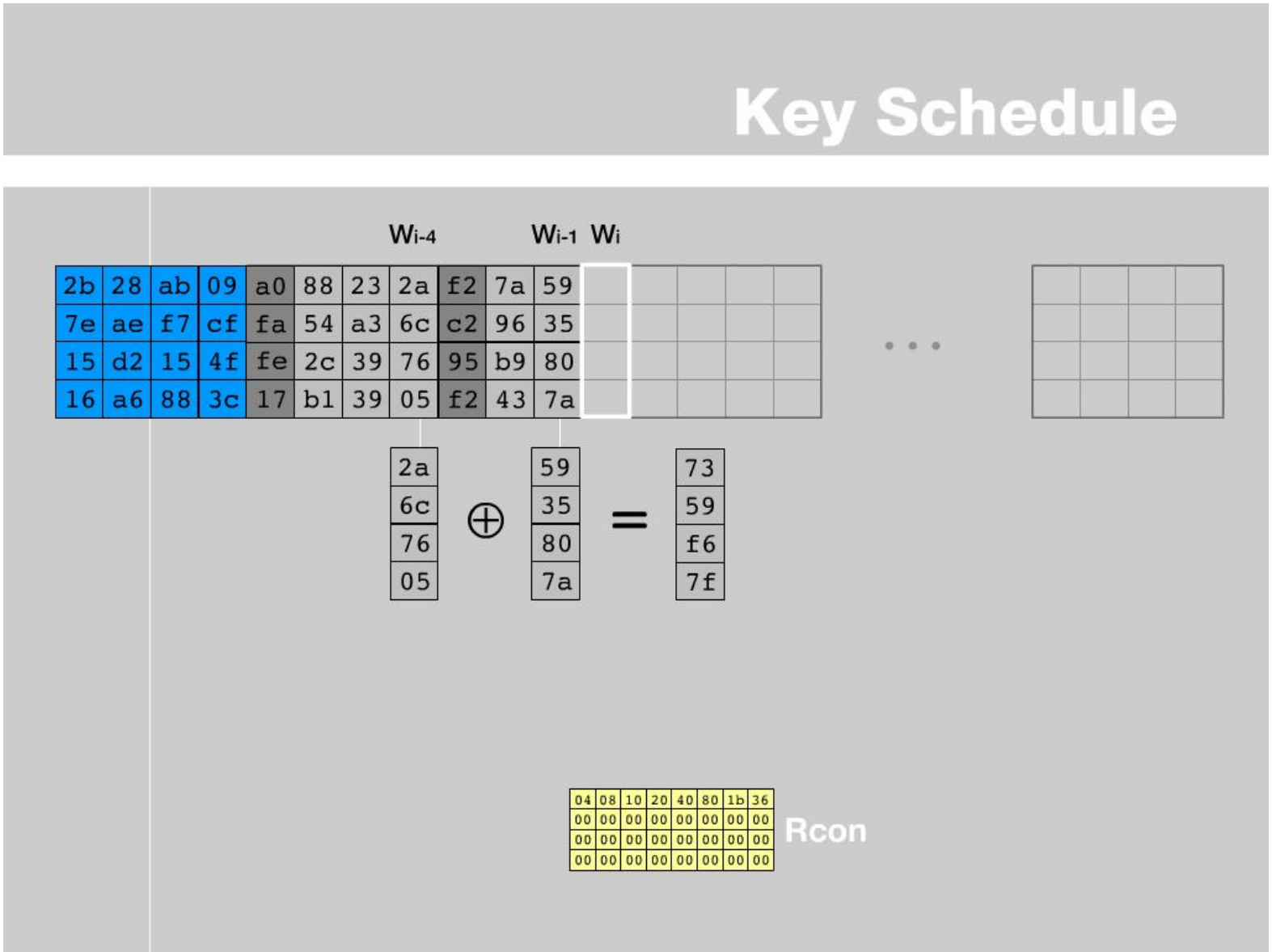
AES-Rijndael : les détails



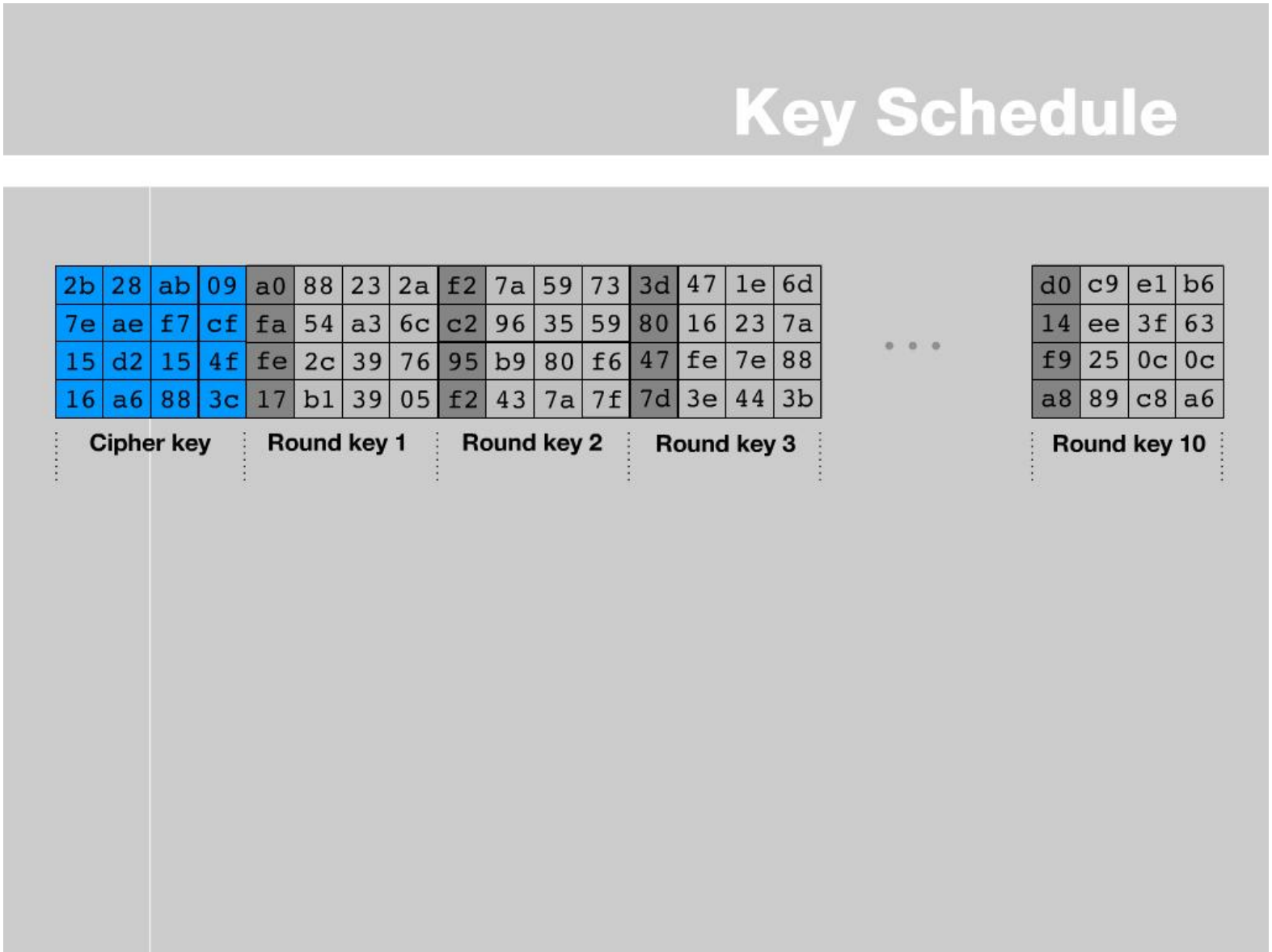
AES-Rijndael : les détails



AES-Rijndael : les détails



AES-Rijndael : les détails



Corps finis quelques mots

- Opération *MixColumn* :

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} d4 \\ bf \\ 5d \\ 30 \end{pmatrix} = \begin{pmatrix} 04 \\ 66 \\ 81 \\ e5 \end{pmatrix}$$

- Opération de multiplication matrice vecteur.
- $r_{i,j} = \underbrace{\sum_{k=0}^{n-1} a_{i,k} b_k}$

où fait on cette opération ?

- Dans $GF(2^m)$ (Corps de Galois à 2^m éléments)