# Mathématiques-Cryptographie

Anne Garcia-Sanchez

M2i cyber1 - CFA CCI Avignon

4 juin 2024

### Chiffrement AES

AES = Advanced Encryption Standard

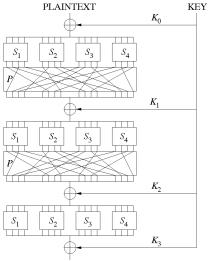
système de chiffrement retenu en 2000 par le NIST (National Institude of Standards and Tecnology)

AES conçu à partir de l'algorithme Rijndael des belges Joan Daemen et Vincent Rijmen.

l'AES est un chiffrement de type réseau de substitutions-permutations qui opère sur des blocs de 128 bits.

Les clés peuvent être de 128, 192 ou 256 bits.

## Réseau de substitutions-permutations - SPN



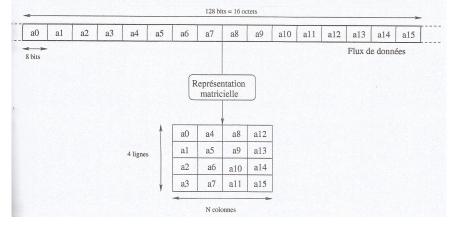
CIPHERTEXT

Sbox/PBox: confusion / diffusion

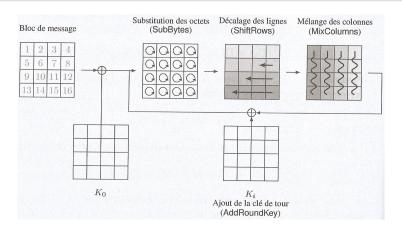
#### Chiffrement AES

Le chiffrement découpe les blocs de 128 bits en 16 octets.

Les blocs sont représentés sous la forme d'une matrice carrée  $4 \times 4$  où les octets sont numérotés de 1 à 16.

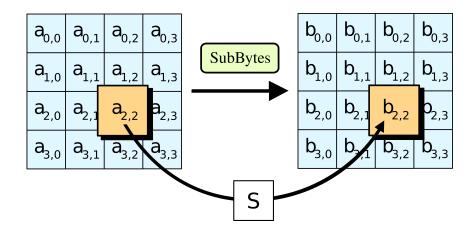


### Chiffrement AES



Le nombre de tours dépend de la taille de la clé. clé de 128 bits/10 tours - 192 bits/12 tours - 256 bits/14 tours La procédure MixColumns est omise lors du dernier tour.

# Chiffrement AES - SubBytes



## Chiffrement AES - SBox

00	01	02	03	04	05	06	07	80	09	0a	0b	0с	0d	0e	0f
63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
ca	82	с9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
b7	fd	93	26	36	3f	f7	сс	34	a5	e5	f1	71	d8	31	15
04	c7	23	с3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	е3	2f	84
53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3с	9f	a8
51	a3	40	8f	92	9d	38	f5	bc	<b>b6</b>	da	21	10	ff	f3	d2
cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
e7	с8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
ba	78	25	2e	1c	a6	b4	с6	e8	dd	74	1f	4b	bd	8b	8a
70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
8c	a1	89	0d	bf	e6	42	68	41	99	2d	Of	b0	54	bb	16
	63 ca b7 04 09 53 d0 51 cd 60 e0 e7 ba 70 e1	63 7c ca 82 b7 fd 04 c7 09 83 53 d1 d0 ef 51 a3 cd 0c 60 81 e0 32 e7 c8 ba 78 70 3e e1 f8	63 7c 77 ca 82 c9 b7 fd 93 04 c7 23 09 83 2c 53 d1 00 d0 ef aa 51 a3 40 cd 0c 13 60 81 4f e0 32 3a e7 c8 37 ba 78 25 70 3e b5 e1 f8 98	63 7c 77 7b ca 82 c9 7d b7 fd 93 26 04 c7 23 c3 09 83 2c 1a 53 d1 00 ed d0 ef aa fb 51 a3 40 8f cd 0c 13 ec 60 81 4f dc e0 32 3a 0a e7 c8 37 6d ba 78 25 2e 70 3e b5 66 e1 f8 98 11	63 7c 77 7b f2 ca 82 c9 7d fa b7 fd 93 26 36 04 c7 23 c3 18 09 83 2c 1a 1b 53 d1 00 ed 20 d0 ef aa fb 43 51 a3 40 8f 92 cd 0c 13 ec 5f 60 81 4f dc 22 e0 32 3a 0a 49 e7 c8 37 6d 8d ba 78 25 2e 1c 70 3e b5 66 48 e1 f8 98 11 69	63 7c 77 7b f2 6b ca 82 c9 7d fa 59 b7 fd 93 26 36 3f 04 c7 23 c3 18 96 09 83 2c 1a 1b 6e 53 d1 00 ed 20 fc d0 ef aa fb 43 4d 51 a3 40 8f 92 9d cd 0c 13 ec 5f 97 60 81 4f dc 22 2a e0 32 3a 0a 49 06 e7 c8 37 6d 8d d5 ba 78 25 2e 1c a6 70 3e b5 66 48 03 e1 f8 98 11 69 d9	63 7c 77 7b f2 6b 6f ca 82 c9 7d fa 59 47 b7 fd 93 26 36 3f f7 04 c7 23 c3 18 96 05 09 83 2c 1a 1b 6e 5a 53 d1 00 ed 20 fc b1 d0 ef aa fb 43 4d 33 51 a3 40 8f 92 9d 38 cd 0c 13 ec 5f 97 44 60 81 4f dc 22 2a 90 e0 32 3a 0a 49 06 24 e7 c8 37 6d 8d d5 4e ba 78 25 2e 1c a6 b4 70 3e b5 66 48 03 f6 e1 f8 98 11 69 d9 8e	63 7c 77 7b f2 6b 6f c5 ca 82 c9 7d fa 59 47 f0 b7 fd 93 26 36 3f f7 cc 04 c7 23 c3 18 96 05 9a 09 83 2c 1a 1b 6e 5a a0 53 d1 00 ed 20 fc b1 5b d0 ef aa fb 43 4d 33 85 51 a3 40 8f 92 9d 38 f5 cd 0c 13 ec 5f 97 44 17 60 81 4f dc 22 2a 90 88 e0 32 3a 0a 49 06 24 5c e7 c8 37 6d 8d d5 4e a9 ba 78 25 2e 1c a6 b4 c6 70 3e b5 66 48 03 f6 0e e1 f8 98 11 69 d9 8e 94	63 7c 77 7b f2 6b 6f c5 30 ca 82 c9 7d fa 59 47 f0 ad b7 fd 93 26 36 3f f7 cc 34 04 c7 23 c3 18 96 05 9a 07 09 83 2c 1a 1b 6e 5a a0 52 53 d1 00 ed 20 fc b1 5b 6a d0 ef aa fb 43 4d 33 85 45 51 a3 40 8f 92 9d 38 f5 bc cd 0c 13 ec 5f 97 44 17 c4 60 81 4f dc 22 2a 90 88 46 e0 32 3a 0a 49 06 24 5c c2 e7 c8 37 6d 8d d5 4e a9 6c ba 78 25 2e 1c a6 b4 c6 e8 70 3e b5 66 48 03 f6 0e 61 e1 f8 98 11 69 d9 8e 94 9b	63 7c 77 7b f2 6b 6f c5 30 01 ca 82 c9 7d fa 59 47 f0 ad d4 b7 fd 93 26 36 3f f7 cc 34 a5 04 c7 23 c3 18 96 05 9a 07 12 09 83 2c 1a 1b 6e 5a a0 52 3b 53 d1 00 ed 20 fc b1 5b 6a cb d0 ef aa fb 43 4d 33 85 45 f9 51 a3 40 8f 92 9d 38 f5 bc b6 cd 0c 13 ec 5f 97 44 17 c4 a7 60 81 4f dc 22 2a 90 88 46 ee e0 32 3a 0a 49 06 24 5c c2 d3 e7 c8 37 6d 8d d5 4e a9 6c 56 ba 78 25 2e 1c a6 b4 c6 e8 dd 70 3e b5 66 48 03 f6 0e 61 35 e1 f8 98 11 69 d9 8e 94 9b 1e	63 7c 77 7b f2 6b 6f c5 30 01 67 ca 82 c9 7d fa 59 47 f0 ad d4 a2 b7 fd 93 26 36 3f f7 cc 34 a5 e5 04 c7 23 c3 18 96 05 9a 07 12 80 09 83 2c 1a 1b 6e 5a a0 52 3b d6 53 d1 00 ed 20 fc b1 5b 6a cb be d0 ef aa fb 43 4d 33 85 45 f9 02 51 a3 40 8f 92 9d 38 f5 bc b6 da cd 0c 13 ec 5f 97 44 17 c4 a7 7e 60 81 4f dc 22 2a 90 88 46 ee b8 e0 32 3a 0a 49 06 24 5c c2 d3 ac e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ba 78 25 2e 1c a6 b4 c6 e8 dd 74 70 3e b5 66 48 03 f6 0e 61 35 57 e1 f8 98 11 69 d9 8e 94 9b 1e 87	63 7c 77 7b f2 6b 6f c5 30 01 67 2b ca 82 c9 7d fa 59 47 f0 ad d4 a2 af b7 fd 93 26 36 3f f7 cc 34 a5 e5 f1 04 c7 23 c3 18 96 05 9a 07 12 80 e2 09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 53 d1 00 ed 20 fc b1 5b 6a cb be 39 d0 ef aa fb 43 4d 33 85 45 f9 02 7f 51 a3 40 8f 92 9d 38 f5 bc b6 da 21 cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 60 81 4f dc 22 2a 90 88 46 ee b8 14 e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ea ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 70 3e b5 66 48 03 f6 0e 61 35 57 b9 e1 88 98 11 69 d9 8e 94 9b 1e 87 e9	63 7c 77 7b f2 6b 6f c5 30 01 67 2b fe ca 82 c9 7d fa 59 47 f0 ad d4 a2 af 9c b7 fd 93 26 36 3f f7 cc 34 a5 e5 f1 71 04 c7 23 c3 18 96 05 9a 07 12 80 e2 eb 09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a d0 ef aa fb 43 4d 33 85 45 f9 02 7f 50 51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 64 60 81 4f dc 22 2a 90 88 46 ee b8 14 de e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ea 65 ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b 70 3e b5 66 48 03 f6 0e 61 35 57 b9 86 e1 f8 98 11 69 d9 8e 94 9b 1e 87 e9 ce	63 7c 77 7b f2 6b 6f c5 30 01 67 2b fe d7 ca 82 c9 7d fa 59 47 f0 ad d4 a2 af 9c a4 b7 fd 93 26 36 3f f7 cc 34 a5 e5 f1 71 d8 04 c7 23 c3 18 96 05 9a 07 12 80 e2 eb 27 09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 e3 53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a 4c d0 ef aa fb 43 4d 33 85 45 f9 02 7f 50 3c 51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 ff cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 64 5d 60 81 4f dc 22 2a 90 88 46 ee b8 14 de 5e e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 95 e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ea 65 7a ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b bd 70 3e b5 66 48 03 f6 0e 61 35 57 b9 86 c1 e1 f8 98 11 69 d9 8e 94 9b 1e 87 e9 ce 55	63 7c 77 7b f2 6b 6f c5 30 01 67 2b fe d7 ab ca 82 c9 7d fa 59 47 f0 ad d4 a2 af 9c a4 72 b7 fd 93 26 36 3f f7 cc 34 a5 e5 f1 71 d8 31 04 c7 23 c3 18 96 05 9a 07 12 80 e2 eb 27 b2 09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 e3 2f 53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a 4c 58 d0 ef aa fb 43 4d 33 85 45 f9 02 7f 50 3c 9f 51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 ff f3 cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 64 5d 19 60 81 4f dc 22 2a 90 88 46 ee b8 14 de 5e 0b e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 95 e4 e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ea 65 7a ae ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b bd 8b 70 3e b5 66 48 03 f6 0e 61 35 57 b9 86 c1 1d e1 f8 88 11 69 d9 8e 94 9b 1e 87 e9 ce 55 28

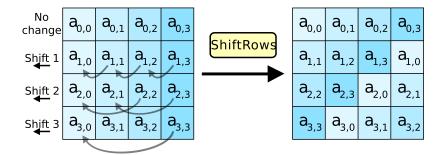
### Chiffrement AES - SBox

SBox conçue mathématiquement pour avoir de bonnes propriétés.

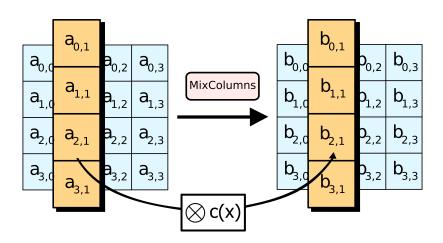
Pour effectuer ces différentes opérations, chaque octet est vu comme un polynôme de degré 7 dans le corps fini  $\mathbb{F}_{2^8}$  où

- l'addition de deux polynômes correspond à l'opération ou exclusif sur les octets: addition terme à terme des coefficients dans  $\mathbb{Z}/2\mathbb{Z}$
- la multiplication est la multiplication des polynômes modulo le polynôme irréductible  $m(x) = x^8 + x^4 + x^3 + x + 1$

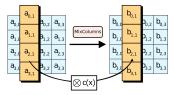
#### Chiffrement AES - ShiftRows



### Chiffrement AES - MixColumns



#### Chiffrement AES - MixColumns



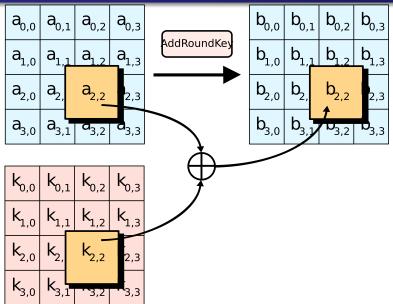
Chaque colonne est vue comme un polynôme a(X) de degré 3 à coefficients dans  $\mathbb{F}_{28}$ 

Chaque colonne est multipliée par le polynôme  $c(X) = 03X^3 + X^2 + X + 02$  modulo le polynôme  $X^4 + 1$ 

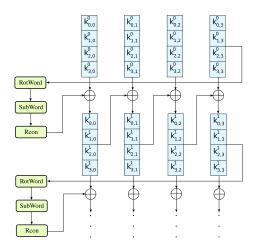
$$egin{bmatrix} b_{0,j} \ b_{1,j} \ b_{2,j} \ b_{2,j} \ \end{bmatrix} = egin{bmatrix} 2 & 3 & 1 & 1 \ 1 & 2 & 3 & 1 \ 1 & 1 & 2 & 3 \ 3 & 1 & 1 & 2 \ \end{bmatrix} egin{bmatrix} a_{0,j} \ a_{2,j} \ a_{2,j} \ a_{2,j} \ \end{bmatrix} \qquad 0 \leq j \leq 3$$

Ceci s'écrit matriciellement:

# Chiffrement AES - AddRoundKey



# Chiffrement AES - Diversification de clé - key schedule



#### Chiffrement AES - Sécurité

Sbox conçue pour être résistante à la cryptanalyse linéaire et différentielle.

ShiftRows + MixColumns: diffusion

 $2^{128}$  ou  $2^{192}$  ou  $2^{256}$  clés: brute force irréaliste

Attaques sur des nombres de tours inférieurs à ceux recommandés

Attaques exploitant les faiblesses du système qui implémente l'algorithme de chiffrement