

Séance 3

Le standard de chiffrement actuel : AES

AES : Advanced Encryption System

- ▶ 1996 : Evaluation 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 : Diplôme 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 *8bits*
 - ▶ Opérations sur des octets

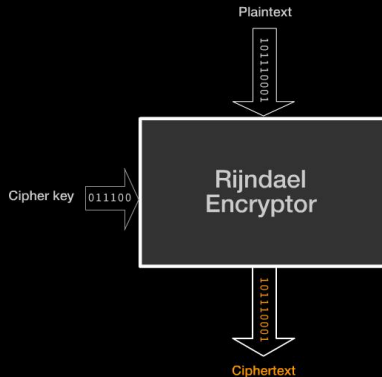
Relation nombre de rondes / Taille de la clé / Taille du bloc

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

Input

State

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

↓
to
Encryption
Process

Ⓐ

Cipher key

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

↓
to
Key
Schedule

Ⓑ

AES-Rijndael : les détails

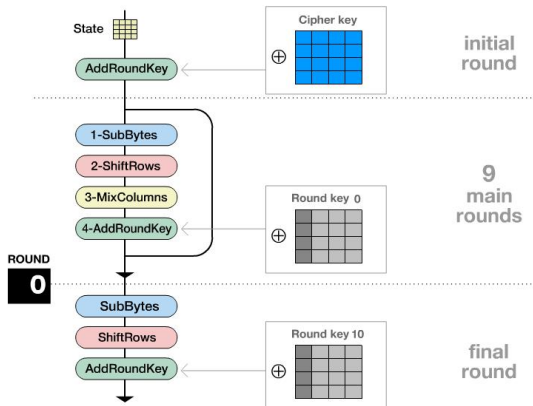


Encryption Process

(Performing the encryption of the given plaintext block using 4 different transformations in the initial round, the 9 main rounds and the final round)

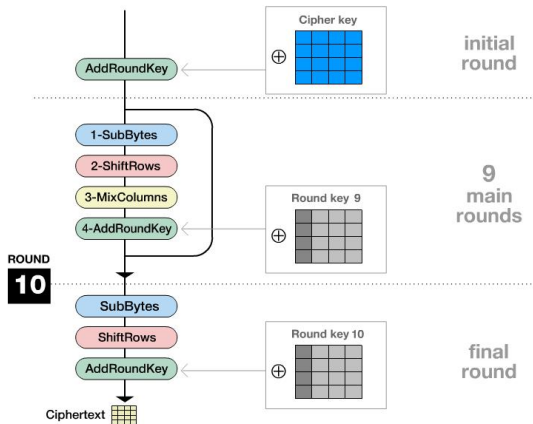
AES-Rijndael : les détails

Encryption Process



AES-Rijndael : les détails

Encryption Process



AES-Rijndael : les détails

The 4 types of transformations:

1-SubBytes

2-ShiftRows

3-MixColumns

4-AddRoundKey

AES-Rijndael : les détails

1 - SubBytes

Round 1

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

		y															
hex		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
x	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	ee	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-BOX byte substitution table

AES-Rijndael : les détails

1 - SubBytes

Round 1

19

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

		y															
hex		0	1	2	3	4	5	6	7								
		0	63	7c	77	7b	f2	6b	6f	c5							
	1	ca	82	c9	7d	fa	59	47	f0								
	2	b7	fd	93	26	36	3f	f7	cc								
	3	04	c7	23	c3	18	96	05	9a								
	4	09	83	2c	1a	1b	ee	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-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

		y															
hex		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
x	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	ee	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-BOX byte substitution table

2 - ShiftRows

Round 1

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

2 - ShiftRows

Round 1

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

 rotate over 1 byte

2 - ShiftRows

Round 1

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

..... rotate over 2 bytes

2 - ShiftRows

Round 1

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

..... rotate over 3 bytes

2 - ShiftRows

Round 1

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

..... rotate over 3 bytes

3 - MixColumns

Round 1

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

3 - MixColumns

Round 1

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

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

•

d4
bf
5d
30

The four numbers of one column are modulo multiplied in Rijndael's Galois Field by a given matrix.

3 - MixColumns

Round 1

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

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

•

d4
bf
5d
30

=

04
66
81
e5

The four numbers of one column are modulo multiplied in Rijndael's Galois Field by a given matrix.

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.

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.

4 - AddRoundKey

Round 1

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

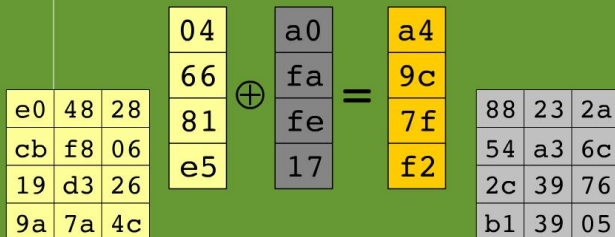
a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

Round key

(produced as Round key 1
during the Key Schedule -
see slide 19)

4 - AddRoundKey

Round 1



Round key

(produced as Round key 1
during the Key Schedule -
see slide 19)

4 - AddRoundKey

Round 1

a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

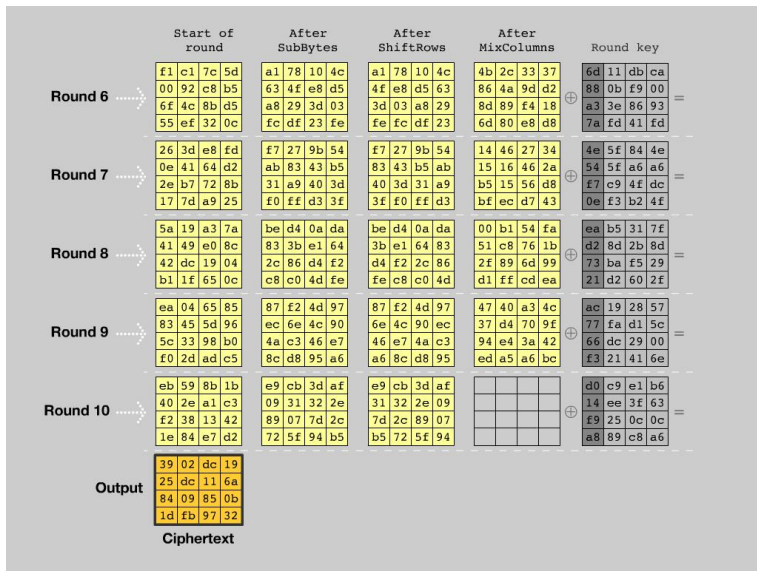
AES-Rijndael : les détails

These transformations are applied to
the State for 9 more rounds.
The final round does not include
the MixColumns transformation.

AES-Rijndael : les détails

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



Key Schedule

(Expansion of the given Cipher key into
11 partial keys, used in the initial round,
the 9 main rounds and the final round)

Cipher key

A large rectangular area divided into three equal vertical sections by two vertical lines. Each section contains a 4x4 grid of smaller squares, totaling 48 squares. This area is intended for drawing a picture related to the text.

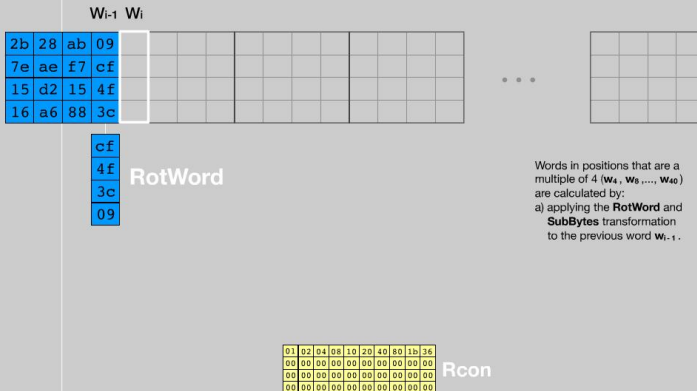
• • •

[illegible]

YREL Protection de l'information

AES-Rijndael : les détails

Key Schedule



AES-Rijndael : les détails

Key Schedule

$W_{i-1} \ W_i$

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

...

8a
4f
3c
09

SubBytes

S-box															
row								col							
0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
1	4	5	7	7f	7e	f2	6b	6c	a5	10	01	61	2b	7a	a7
2	5b	82	c3	7d	7a	53	47	20	2d	24	a2	a7	7c	24	72
3	07	16	93	20	16	17	f1	e0	14	a5	a5	01	11	0b	13
4	04	c7	23	c3	18	9c	05	3a	07	32	00	c2	ab	27	52
5	09	83	20	14	16	4a	5a	40	52	0b	00	33	27	a3	22
6	53	a1	00	c0	20	2c	2c	51	53	5a	c0	3a	73	4a	62
7	20	a4	aa	2b	81	46	13	85	45	f3	02	12	70	37	10
8	15	a3	40	04	93	50	12	c5	4c	5a	0a	21	10	f7	12
9	ad	0a	13	ae	55	97	44	17	24	a7	7a	5d	44	5d	13
a	20	81	47	4b	22	2a	10	81	46	aa	1a	14	2a	0a	2b
b	00	c2	7a	5b	49	48	24	50	c2	43	2a	c2	7a	5b	49
c	27	08	27	04	04	a5	4a	a7	6a	5c	f4	aa	c5	7a	aa
d	0a	7a	27	20	12	4a	1a	2a	aa	4a	1a	12	0a	1a	0a
e	10	2a	4c	c5	48	51	20	6a	51	35	13	20	c5	48	51
f	a3	8a	00	11	a3	a3	8a	34	0b	1a	87	a3	0a	55	2a
10	8a	a3	03	04	c5	a5	42	c4	41	33	2a	c4	a5	5a	14

S-BOX byte substitution table

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

Words in positions that are a multiple of 4 (w_4, w_8, \dots, w_{40}) are calculated by:

- applying the **RotWord** and **SubBytes** transformation to the previous word w_{i-1} .

Pierre-Louis CAYREL

Protection de l'information

39/56





AES-Rijndael : les détails

Key Schedule

2b	28	ab	09	a0
7e	ae	f7	cf	fa
15	d2	15	4f	fe
16	a6	88	3c	17

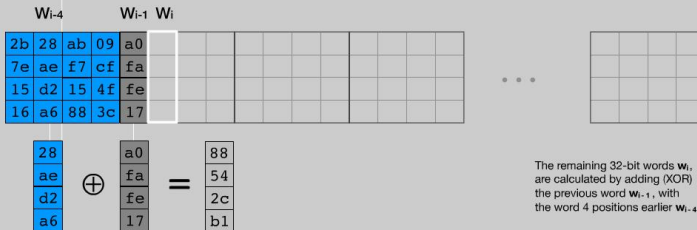
...

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

Key Schedule

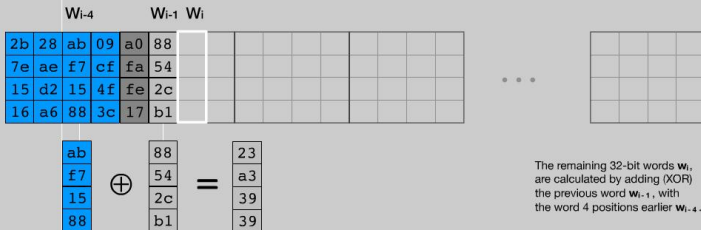


02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00

Rcon

AES-Rijndael : les détails

Key Schedule

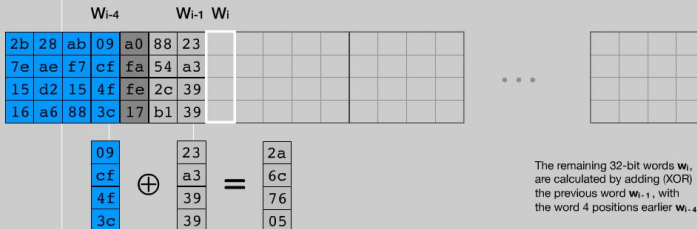


02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00

Rcon

AES-Rijndael : les détails

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

Key Schedule

2b	28	ab	09	a0	88	23	2a												
7e	ae	f7	cf	fa	54	a3	6c												
15	d2	15	4f	fe	2c	39	76												
16	a6	88	3c	17	b1	39	05												

Cipher key

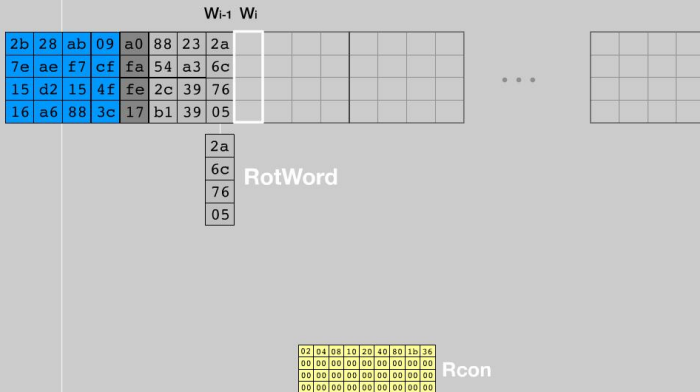
Round key 1

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

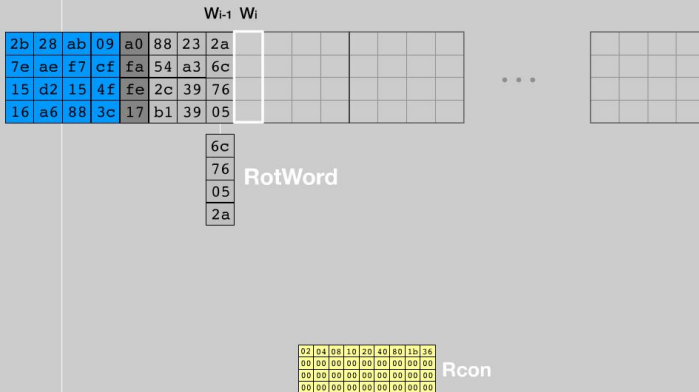
AES-Rijndael : les détails

Key Schedule



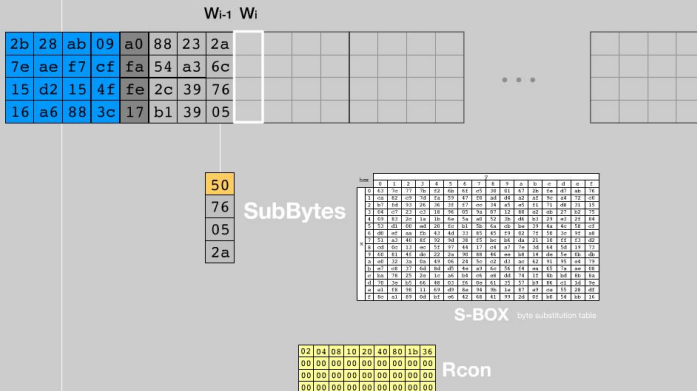
AES-Rijndael : les détails

Key Schedule



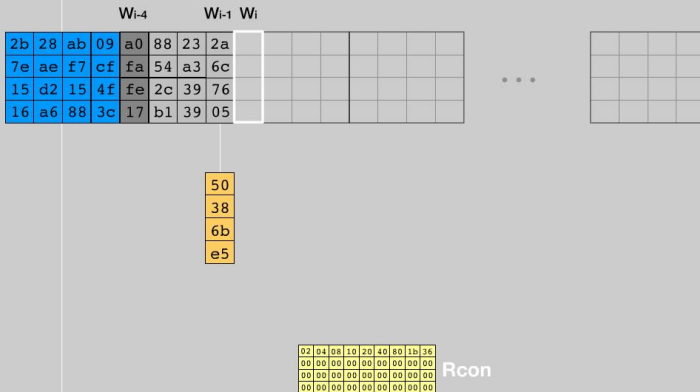
AES-Rijndael : les détails

Key Schedule



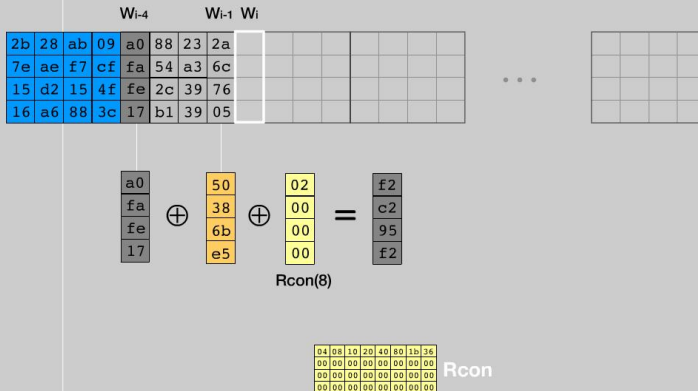
AES-Rijndael : les détails

Key Schedule



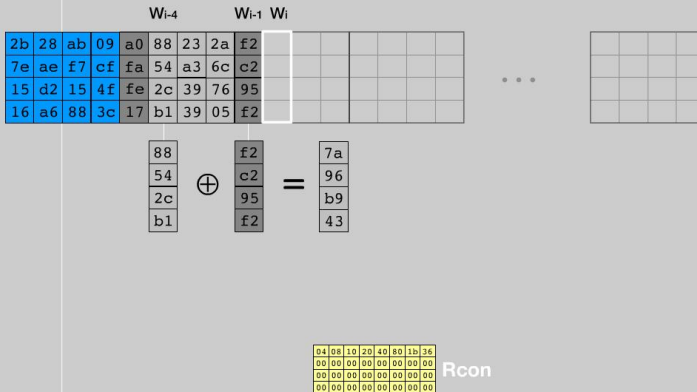
AES-Rijndael : les détails

Key Schedule



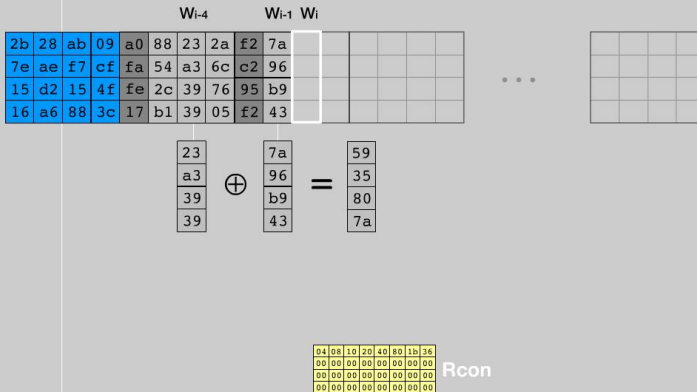
AES-Rijndael : les détails

Key Schedule



AES-Rijndael : les détails

Key Schedule





AES-Rijndael : les détails

Key Schedule

2b	28	ab	09	a0	88	23	2a	f2	7a	59	73	3d	47	1e	6d
7e	ae	f7	cf	fa	54	a3	6c	c2	96	35	59	80	16	23	7a
15	d2	15	4f	fe	2c	39	76	95	b9	80	f6	47	fe	7e	88
16	a6	88	3c	17	b1	39	05	f2	43	7a	7f	7d	3e	44	3b

Cipher key

Round key 1

Round key 2

Round key 3

...

d0	c9	e1	b6
14	ee	3f	63
f9	25	0c	0c
a8	89	c8	a6

Round key 10

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.

$$\text{▶ } r_{i,j} = \underbrace{\sum_{k=0}^{n-1} a_{i,k} b_k}$$

où fait on cette opération ?

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