TD 1 : Chiffrement et déchiffrement symétrique AES

Pour des raisons de temps nous ne considérerons qu'un seul round de chiffrement et de déchiffrement de l'AES qui se compose des étapes suivantes :

ROUND DE CHIFFREMENT AES
- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey

ROUND DE DECHIFFREMENT AES
- InvShiftRows
- InvSubBytes
- AddRoundKey
- InvMixColumns

Le message initial de 128 bits à transmettre est le suivant (chaque chiffre est codé en hexadécimal sur 4 bits)

00102030405060708090A0B0C0D0E0F0

La clé de chiffrement de 128 bits à utiliser dans ce round est la suivante

D6AA74FDD2AF72FADAA678F1D6AB76FE

ENTRÉE	**00102030405060708090A0B0C0D0E0F0**
SUBBYTES	**63CAB7040953D051CD60E0E7BA70E18C**
SHIFTROW	**6353E08C0960E104CD70B751BACAD0E7**
MIXCOLUMNS	**5F72641557F5BC92F7BE3B291DB9F91A**
KEY	**D6AA74FDD2AF72FADAA678F1D6AB76FE**
ADDROUNDKEY	**89D810E8855ACE682D1843D8CB128FE4**

ENTRÉE	**89D810E8855ACE682D1843D8CB128FE4**
KEY	**D6AA74FDD2AF72FADAA678F1D6AB76FE**
INVADDROUNDKEY	**5F72641557F5BC92F7BE3B291DB9F91A**
INVMIXCOLUMNS	**6353E08C0960E104CD70B751BACAD0E7**
INVSHIFTROW	**63CAB7040953D051CD60E0E7BA70E18C**
INVSUBBYTES	**00102030405060708090A0B0C0D0E0F0**

I. Chiffrement en bloc

Remplissez la matrice suivante, chaque case représente un octet. Par la suite, les opérations du chiffrement et du déchiffrement se font octet par octet.

00	40	80	C0
10	50	90	D0
20	60	A0	E0
30	70	B0	F0

II. Chiffrement AES – SubBytes

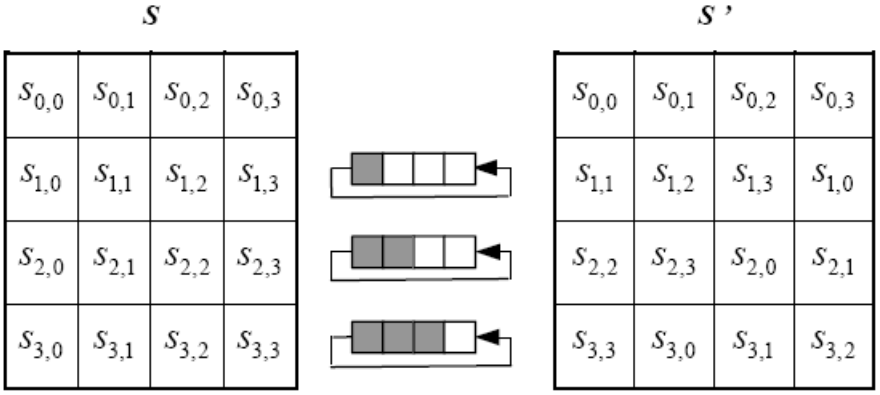
En utilisant la matrice Sbox suivante remplissez la matrice de résultat de l'opération SubBytes :

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

63	09	CD	BA
CA	53	60	70
B7	D0	E0	E1
04	51	E7	8C

III. Chiffrement AES – ShiftRows

En considérant la modification suivante pour ShiftRows remplissez la matrice de résultat de cette opération :



63	09	CD	BA
53	60	70	CA
E0	E1	B7	D0
8C	04	51	E7

IV. Chiffrement AES – MixColumns

En considérant la modification suivante pour MixColumns remplissez la matrice de résultat de cette opération :

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

5F	57	F7	1D
72	F5	BE	B9
64	BC	3B	F9
15	92	29	1A

MATRICE en entrée

63 = 0110 0011	09 = 0000 1001	CD = 1100 1101	BA = 1011 1010
53 = 0101 0011	60 = 0110 0000	70 = 0111 0000	CA = 1100 1010
E0 = 1110 0000	E1 =1110 0001	B7 = 1011 0111	D0 = 1101 0000
8C = 1000 1100	04 = 0000 0100	51 = 0101 0001	E7 = 1110 0111

Correction (tout les + sont des XOR) (tout les * sont modulo dans GF(2^8) 11B « 1 0001 1011 »)

2*(X) => 1 décalage à gauche
- si B7 = 0 => alors le résultat est bon
- si B7 = 1 => alors résultat = décalé à gauche + 0001 1011

Ligne n°0 ----------

$S'_{0,c} = 2* S_{0,c} + 3* S_{1,c} + S_{2,c} + S_{3,c} = 2* S_{0,c} + 2* S_{1,c} + S_{1,c} + S_{2,c} + S_{3,c}$
$S'_{0,c} = 2* (S_{0,c} + S_{1,c}) + S_{1,c} + S_{2,c} + S_{3,c}$

Calcul de $S'_{0,0}$
$2* (S_{0,0} + S_{1,0}) = 2*(0110\ 0011 + 0101\ 0011) = 2*(\mathbf{0}011\ 0000) = 0110\ 0000$
$S'_{0,0} = 0110\ 0000 + 0101\ 0011 + 1110\ 0000 + 1000\ 1100 = 0101\ 1111 = \mathbf{5F}$

Calcul de $S'_{0,1}$
$2* (S_{0,1} + S_{1,1}) = 2*(0000\ 1001 + 0110\ 0000) = 2*(\mathbf{0}110\ 1001) = 1101\ 0010$
$S'_{0,1} = 1101\ 0010 + 0110\ 0000 + 1110\ 0001 + 0000\ 0100 = 0101\ 0111 = \mathbf{57}$

Calcul de $S'_{0,2}$
$2* (S_{0,2} + S_{1,2}) = 2*(1100\ 1101 + 0111\ 0000) = 2*(\mathbf{1}011\ 1101) = 0111\ 1010 + 0001\ 1011$
$2* (S_{0,2} + S_{1,2}) = 0110\ 0001$
$S'_{0,2} = 0110\ 0001 + 0111\ 0000 + 1011\ 0111 + 0101\ 0001 = 1111\ 0111 = \mathbf{F7}$

Calcul de $S'_{0,3}$

$2*(S_{0,3} + S_{1,3}) = 2*(1011\ 1010 + 1100\ 1010) = 2*(\mathbf{0}111\ 0000) = 1110\ 0000$

$S'_{0,1} = 1110\ 0000 + 1100\ 1010 + 1101\ 0000 + 1110\ 0111 = 0001\ 1101 = \mathbf{1D}$

Ligne n°1 ----------

$S'_{1,c} = S_{0,c} + 2*S_{1,c} + 3*S_{2,c} + S_{3,c} = S_{0,c} + 2*S_{1,c} + 2*S_{2,c} + S_{2,c} + S_{3,c}$

$S'_{1,c} = 2*(S_{1,c} + S_{2,c}) + S_{0,c} + S_{2,c} + S_{3,c}$

Calcul de $S'_{1,0}$

$2*(S_{1,0} + S_{2,0}) = 2*(0101\ 0011 + 1110\ 0000) = 2*(\mathbf{1}011\ 0011) = 0110\ 0110 + 0001\ 1011$

$2*(S_{1,0} + S_{2,0}) = 0111\ 1101$

$S'_{1,0} = 0111\ 1101 + 0110\ 0011 + 1110\ 0000 + 1000\ 1100 = 0111\ 0010 = \mathbf{72}$

Calcul de $S'_{1,1}$

$2*(S_{1,1} + S_{2,1}) = 2*(0110\ 0000 + 1110\ 0001) = 2*(\mathbf{1}000\ 0001) = 0000\ 0010 + 0001\ 1011$

$2*(S_{1,1} + S_{2,1}) = 0001\ 1001$

$S'_{1,1} = 0001\ 1001 + 0000\ 1001 + 1110\ 0001 + 0000\ 0100 = 1111\ 0101 = \mathbf{F5}$

Calcul de $S'_{1,2}$

$2*(S_{1,2} + S_{2,2}) = 2*(0111\ 0000 + 1011\ 0111) = 2*(\mathbf{1}100\ 0111) = 1000\ 1110 + 0001\ 1011$

$2*(S_{1,2} + S_{2,2}) = 1001\ 0101$

$S'_{1,2} = 1001\ 0101 + 1100\ 1101 + 1011\ 0111 + 0101\ 0001 = 1011\ 1110 = \mathbf{BE}$

Calcul de $S'_{1,3}$

$2*(S_{1,3} + S_{2,3}) = 2*(1100\ 1010 + 1101\ 0000) = 2*(\mathbf{0}001\ 1010) = 0011\ 0100$

$S'_{1,3} = 0011\ 0100 + 1011\ 1010 + 1101\ 0000 + 1110\ 0111 = 1011\ 1001 = \mathbf{B9}$

Ligne n°2 ----------

$S'_{2,c} = S_{0,c} + S_{1,c} + 2*S_{2,c} + 3*S_{3,c} = S_{0,c} + S_{1,c} + 2*S_{2,c} + 2*S_{3,c} + S_{3,c}$

$S'_{2,c} = 2*(S_{2,c} + S_{3,c}) + S_{0,c} + S_{1,c} + S_{3,c}$

Calcul de $S'_{2,0}$

$2*(S_{2,0} + S_{3,0}) = 2*(1110\ 0000 + 1000\ 1100) = 2*(\mathbf{0}110\ 1100) = 1101\ 1000$

$S'_{2,0} = 1101\ 1000 + 0110\ 0011 + 1000\ 1100 + 01010011 = 0110\ 0100 = \mathbf{64}$

Calcul de $S'_{2,1}$

$2*(S_{2,1} + S_{3,1}) = 2*(1110\ 0001 + 0000\ 0100) = 2*(\mathbf{1}110\ 0101) = 1100\ 1010 + 0001\ 1011$

$2*(S_{2,1} + S_{3,1}) = 1101\ 0001$

$S'_{2,1} = 1101\ 0001 + 0000\ 1001 + 0000\ 0100 + 0110\ 0000 = 1011\ 1100 = \mathbf{BC}$

Calcul de $S'_{2,2}$

$2*(S_{2,2} + S_{3,2}) = 2*(1011\ 0111 + 0101\ 0001) = 2*(\mathbf{1}110\ 0110) = 1100\ 1100 + 0001\ 1011$

$2*(S_{2,2} + S_{3,2}) = 1101\ 0111$

$S'_{2,2} = 1101\ 0111 + 1100\ 1101 + 0101\ 0001 + 0111\ 000 = 0011\ 1011 = \mathbf{3B}$

Calcul de $S'_{2,3}$

$2*(S_{2,3} + S_{3,3}) = 2*(1101\ 0000 + 1110\ 0111) = 2*(\mathbf{0}011\ 0111) = 0110\ 1110$

$S'_{2,3} = 0110\ 1110 + 1011\ 1010 + 1110\ 0111 + 1100\ 1010 = 1111\ 1001 = \mathbf{F9}$

Ligne n°3 ----------

$S'_{3,c} = 3*S_{0,c} + S_{1,c} + S_{2,c} + 2*S_{3,c} = 2*S_{0,c} + S_{0,c} + S_{1,c} + S_{2,c} + 2*S_{3,c}$

$S'_{3,c} = 2* (S_{0,c} + S_{3,c}) + S_{0,c} + S_{1,c} + S_{2,c}$

Calcul de $S'_{3,0}$

$2* (S_{0,0} + S_{3,0}) = 2*(0110\ 0011 + 1000\ 1100) = 2*(\mathbf{1}110\ 1111) = 1101\ 1110 + 0001\ 1011$

$2* (S_{0,0} + S_{3,0}) = 1100\ 0101$

$S'_{2,0} = 1100\ 0101 + 0110\ 0011 + 0101\ 0011 + 1110\ 0000 = 0001\ 0101 = \mathbf{15}$

Calcul de $S'_{3,1}$

$2* (S_{0,1} + S_{3,1}) = 2*(0000\ 1001 + 0000\ 0100) = 2*(\mathbf{0}000\ 1101) = 0001\ 1010$

$S'_{3,1} = 0001\ 1010 + 0000\ 1001 + 0110\ 0000 + 1110\ 0001 = 1001\ 0010 = \mathbf{92}$

Calcul de $S'_{3,2}$

$2* (S_{0,2} + S_{3,2}) = 2*(1100\ 1101 + 0101\ 0001) = 2*(\mathbf{1}001\ 1100) = 0011\ 1000 + 0001\ 1011$

$2* (S_{0,2} + S_{3,2}) = 0010\ 0011$

$S'_{3,2} = 0010\ 0011 + 1100\ 1101 + 0111\ 0000 + 1011\ 0111 = 0010\ 1001 = \mathbf{29}$

Calcul de $S'_{3,3}$

$2* (S_{0,3} + S_{3,3}) = 2*(1011\ 1010 + 1110\ 0111) = 2*(\mathbf{0}101\ 1101) = 1011\ 1010$

$S'_{3,3} = 1011\ 1010 + 1011\ 1010 + 1100\ 1010 + 1101\ 0000 = 0001\ 1010 = \mathbf{1A}$

V. Chiffrement AES – AddRoundKey

En utilisant la clé donnée remplissez la matrice de résultat de l'opération AddRoundKey :

89	85	2D	CB
D8	5A	18	12
10	CE	43	8F
E8	68	D8	E4

VI. Déchiffrement AES – AddRoundKey

En utilisant la clé donnée remplissez la matrice de résultat de l'opération AddRoundKey :

5F	57	F7	1D
72	F5	BE	B9
64	BC	3B	F9
15	92	29	1A

VII. Déchiffrement AES –Inv MixColumns

En considérant la modification suivante pour InvMixColumns remplissez la matrice de résultat de cette opération :

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

63	09	CD	BA
53	60	70	CA
E0	E1	B7	D0
8C	04	51	E7

MATRICE en entrée

5F = 0101 1111	57 = 0101 0111	F7 = 1111 0111	1D = 0001 1101
72 = 0111 0010	F5 = 1111 0101	BE = 1011 1110	B9 = 1011 1001
64 = 0110 0100	BC =1011 1100	3B = 0011 1011	F9 = 1111 1001
15 = 0001 0101	92 = 1001 0010	29 = 0010 1001	1A = 0001 1010

Correction (tout les + sont des XOR) (tout les * sont modulo dans GF(2^8) 11B « 1 0001 1011 »)

2*(X) => 1 décalage à gauche
- si B7 = 0 => alors le résultat est bon
- si B7 = 1 => alors résultat = décalé à gauche + 0001 1011

Ligne n°0 ----------

$S'_{0,c} = E^* S_{0,c} + B^* S_{1,c} + D^* S_{2,c} + 9^* S_{3,c} = 8^* S_{0,c} + 4^* S_{0,c} + 2^* S_{0,c} + 8^* S_{1,c} + 2^* S_{1,c} + S_{1,c} + 8^* S_{2,c} + 4^* S_{2,c} + S_{2,c} + 8^* S_{3,c} + S_{3,c}$

$S'_{0,c} = 8^* (S_{0,c} + S_{1,c} + S_{2,c} + S_{3,c}) + 4^* (S_{0,c} + S_{2,c}) + 2^* (S_{0,c} + S_{1,c}) + S_{1,c} + S_{2,c} + S_{3,c}$

Calcul de $S'_{0,0}$

$8^* (S_{0,0} + S_{1,0} + S_{2,0} + S_{3,0}) = 8^*(0101\ 1111 + 0111\ 0010 + 0110\ 0100 + 0001\ 0101)$
$8^* (S_{0,0} + S_{1,0} + S_{2,0} + S_{3,0}) = 8^*(\mathbf{0}101\ 1100) = 4^*(\mathbf{1}011\ 1000) = 2^*(0111\ 0000 + 0001\ 1011)$
$8^* (S_{0,0} + S_{1,0} + S_{2,0} + S_{3,0}) = 2^*(\mathbf{0}110\ 1011) = \underline{1101\ 0110}$

$4^* (S_{0,0} + S_{2,0}) = 4^*(0101\ 1111 + 0110\ 0100) = 4^*(\mathbf{0}011\ 1011) = 2^*(\mathbf{0}111\ 0110) = \underline{1110\ 1100}$

$2^* (S_{0,0} + S_{1,0}) = 2^*(0101\ 1111 + 0111\ 0010) = 2^*(\mathbf{0}010\ 1101) = \underline{0101\ 1010}$

$S'_{0,0} = 1101\ 0110 + 1110\ 1100 + 0101\ 1010 + 0111\ 0010 + 0110\ 0100 + 0001\ 0101$
$S'_{0,0} = 0110\ 0011 = \mathbf{63}$

Calcul de $S'_{0,1}$

$8^* (S_{0,1} + S_{1,1} + S_{2,1} + S_{3,1}) = 8^*(0101\ 0111 + 1111\ 0101 + 1011\ 1100 + 1001\ 0010)$
$8^* (S_{0,1} + S_{1,1} + S_{2,1} + S_{3,1}) = 8^*(\mathbf{1}000\ 1100) = 4^*(0001\ 1000 + 0001\ 1011) = 4^*(\mathbf{0}000\ 0011)$
$8^* (S_{0,1} + S_{1,1} + S_{2,1} + S_{3,1}) = 2^*(\mathbf{0}000\ 0110) = \underline{0000\ 1100}$

$4^* (S_{0,1} + S_{2,1}) = 4^*(0101\ 0111 + 1011\ 1100) = 4^*(\mathbf{1}110\ 1011) = 2^*(1101\ 0110 + 0001\ 1011)$
$4^* (S_{0,1} + S_{2,1}) = 2^*(\mathbf{1}100\ 1101) = 1001\ 1010 + 0001\ 1011 = \underline{1000\ 0001}$

$2^* (S_{0,1} + S_{1,1}) = 2^*(0101\ 0111 + 1111\ 0101\ ) = 2^*(\mathbf{1}010\ 0010)$
$2^* (S_{0,1} + S_{1,1}) = 0100\ 0100 + 0001\ 1011 = \underline{0101\ 1111}$

$S'_{0,1} = 0000\ 1100 + 1000\ 0001 + 0101\ 1111 + 1111\ 0101 + 1011\ 1100 + 1001\ 0010$
$S'_{0,1} = 0000\ 1001 = \mathbf{09}$

Calcul de $S'_{0,2}$

$8^* (S_{0,2} + S_{1,2} + S_{2,2} + S_{3,2}) = 8^*(1111\ 0111 + 1011\ 1110 + 0011\ 1011 + 0010\ 1001)$
$8^* (S_{0,2} + S_{1,2} + S_{2,2} + S_{3,2}) = 8^*(\mathbf{0}101\ 1011) = 4^*(\mathbf{1}011\ 0110) = 2^*(0110\ 1100 + 0001\ 1011)$
$8^* (S_{0,2} + S_{1,2} + S_{2,2} + S_{3,2}) = 2^*(\mathbf{0}111\ 0111) = \underline{1110\ 1110}$

$4^* (S_{0,2} + S_{2,2}) = 4^*(1111\ 0111 + 0011\ 1011) = 4^*(\mathbf{1}100\ 1100) = 2^*(1001\ 1000 + 0001\ 1011)$
$4^* (S_{0,2} + S_{2,2}) = 2^*(\mathbf{1}000\ 0011) = 0000\ 0110 + 0001\ 1011 = \underline{0001\ 1101}$

$2^* (S_{0,2} + S_{1,2}) = 2^*(1111\ 0111 + 1011\ 1110) = 2^*(\mathbf{0}100\ 1001) = \underline{1001\ 0010}$

$S'_{0,1} = 1110\ 1110 + 0001\ 1101 + 1001\ 0010 + 1011\ 1110 + 0011\ 1011 + 0010\ 1001$
$S'_{0,1} = 1100\ 1101 = \mathbf{CD}$

Calcul de $S'_{0,3}$

$8^* (S_{0,3} + S_{1,3} + S_{2,3} + S_{3,3}) = 8^*(0001\ 1101 + 1011\ 1001 + 1111\ 1001 + 0001\ 1010)$
$8^* (S_{0,3} + S_{1,3} + S_{2,3} + S_{3,3}) = 8^*(\mathbf{0}100\ 0111) = 4^*(\mathbf{1}000\ 1110) = 2^*(0001\ 1100 + 0001\ 1011)$
$8^* (S_{0,3} + S_{1,3} + S_{2,3} + S_{3,3}) = 2^*(\mathbf{0}000\ 0111) = \underline{0000\ 1110}$

$4*(S_{0,3} + S_{2,3}) = 4*(0001\ 1101 + 1111\ 1001) = 4*(\mathbf{1}110\ 0100) = 2*(1100\ 1000 + 0001\ 1011)$
$4*(S_{0,3} + S_{2,3}) = 2*(\mathbf{1}101\ 0011) = 1010\ 0110 + 0001\ 1011 = \underline{1011\ 1101}$

$2*(S_{0,3} + S_{1,3}) = 2*(0001\ 1101 + 1011\ 1001) = 2*(\mathbf{1}010\ 0100)$
$2*(S_{0,3} + S_{1,3}) = 0100\ 1000 + 0001\ 1011 = \underline{0101\ 0011}$

$S'_{0,3} = 0000\ 1110 + 1011\ 1101 + 0101\ 0011 + 1011\ 1001 + 1111\ 1001 + 0001\ 1010$
$S'_{0,3} = 1011\ 1010 = \mathbf{BA}$

Ligne n°1 ----------

$S'_{1,c} = 9*S_{0,c} + E*S_{1,c} + B*S_{2,c} + D*S_{3,c}$

$S'_{1,c} = 8*(S_{0,c} + S_{1,c} + S_{2,c} + S_{3,c}) + 4*(S_{1,c} + S_{3,c}) + 2*(S_{1,c} + S_{2,c}) + S_{0,c} + S_{2,c} + S_{3,c}$

Calcul de $S'_{1,0}$
$8*(S_{0,0} + S_{1,0} + S_{2,0} + S_{3,0}) = \underline{1101\ 0110}$

$4*(S_{1,0} + S_{3,0}) = 4*(0111\ 0010 + 0001\ 0101) = 4*(\mathbf{0}110\ 0111) = 2*(\mathbf{1}100\ 1110)$
$4*(S_{1,0} + S_{3,0}) = 1001\ 1100 + 0001\ 1011 = \underline{1000\ 0111}$

$2*(S_{1,0} + S_{2,0}) = 2*(0111\ 0010 + 0110\ 0100) = 2*(\mathbf{0}001\ 0110) = \underline{0010\ 1100}$

$S'_{0,0} = 1101\ 0110 + 1000\ 0111 + 0010\ 1100 + 0101\ 1111 + 0110\ 0100 + 0001\ 0101$
$S'_{0,0} = 0101\ 0011 = \mathbf{53}$

Calcul de $S'_{1,1}$
$8*(S_{0,1} + S_{1,1} + S_{2,1} + S_{3,1}) = \underline{0000\ 1100}$

$4*(S_{1,1} + S_{3,1}) = 4*(1111\ 0101 + 1001\ 0010) = 4*(\mathbf{0}110\ 0111) = 2*(\mathbf{1}100\ 1110)$
$4*(S_{1,1} + S_{3,1}) = 1001\ 1100 + 0001\ 1011 = \underline{1000\ 0111}$

$2*(S_{1,1} + S_{2,1}) = 2*(1111\ 0101 + 1011\ 1100) = 2*(\mathbf{0}100\ 1001) = \underline{1001\ 0010}$

$S'_{0,1} = 0000\ 1100 + 1000\ 0111 + 1001\ 0010 + 0101\ 0111 + 1011\ 1100 + 1001\ 0010$
$S'_{0,1} = 0110\ 0000 = \mathbf{60}$

Calcul de $S'_{1,2}$
$8*(S_{0,2} + S_{1,2} + S_{2,2} + S_{3,2}) = \underline{1110\ 1110}$

$4*(S_{1,2} + S_{3,2}) = 4*(1011\ 1110 + 0010\ 1001) = 4*(\mathbf{1}001\ 0111) = 2*(0010\ 1110 + 0001\ 1011)$
$4*(S_{1,2} + S_{3,2}) = 2*(\mathbf{0}011\ 0101) = \underline{0110\ 1010}$

$2*(S_{1,2} + S_{2,1}) = 2*(1011\ 1110 + 0011\ 1011) = 2*(\mathbf{1}000\ 0101)$
$2*(S_{1,2} + S_{2,1}) = 0000\ 1010 + 0001\ 1011 = \underline{0001\ 0001}$

$S'_{0,2} = 1110\ 1110 + 0110\ 1010 + 0001\ 0101 + 1111\ 0111 + 0011\ 1011 + 0010\ 1001$
$S'_{0,2} = 0111\ 0000 = \mathbf{70}$

Calcul de $S'_{1,3}$
$8*(S_{0,3} + S_{1,3} + S_{2,3} + S_{3,3}) = \underline{0000\ 1110}$

$4*(S_{1,3} + S_{3,3}) = 4*(1011\ 1001 + 0001\ 1010) = 4*(\mathbf{1}010\ 0011) = 2*(0100\ 0110 + 0001\ 1011)$
$4*(S_{1,3} + S_{3,3}) = 2*(\mathbf{0}101\ 1101) = \underline{1011\ 1010}$

$2*(S_{1,3} + S_{2,3}) = 2*(1011\ 1001 + 1111\ 1001) = 2*(\mathbf{0}100\ 0000) = \underline{1000\ 0000}$

$S'_{0,2} = 0000\ 1110 + 1011\ 1010 + 1000\ 0000 + 0001\ 1101 + 1111\ 1001 + 0001\ 1010$
$S'_{0,2} = 1100\ 1010 = \mathbf{CA}$

Ligne n°2 ----------

$S'_{2,c} = D*S_{0,c} + 9*S_{1,c} + E*S_{2,c} + B*S_{3,c}$

$S'_{2,c} = 8*(S_{0,c} + S_{1,c} + S_{2,c} + S_{3,c}) + 4*(S_{2,c} + S_{0,c}) + 2*(S_{2,c} + S_{3,c}) + S_{0,c} + S_{1,c} + S_{3,c}$

Calcul de $S'_{2,0}$
$8*(S_{0,0} + S_{1,0} + S_{2,0} + S_{3,0}) = \underline{1101\ 0110}$

$4*(S_{2,0} + S_{0,0}) = \underline{1110\ 1100}$

$2*(S_{2,0} + S_{3,0}) = 2*(0110\ 0100 + 0001\ 0101) = 2*(\mathbf{0}111\ 0001) = \underline{1110\ 0010}$

$S'_{2,0} = 1101\ 0110 + 1110\ 1100 + 1110\ 0010 + 0101\ 1111 + 0111\ 0010 + 0001\ 0101$
$S'_{2,0} = 1110\ 0000 = \mathbf{E0}$

Calcul de $S'_{2,1}$
$8*(S_{0,1} + S_{1,1} + S_{2,1} + S_{3,1}) = \underline{0000\ 1100}$

$4*(S_{2,1} + S_{0,1}) = \underline{1000\ 0001}$

$2*(S_{2,1} + S_{3,1}) = 2*(1011\ 1100 + 1001\ 0010) = 2*(\mathbf{0}010\ 1110) = \underline{0101\ 1100}$

$S'_{2,1} = 0000\ 1100 + 1000\ 0001 + 0101\ 1100 + 0101\ 0111 + 1111\ 0101 + 1001\ 0010$
$S'_{2,1} = 1110\ 0001 = \mathbf{E1}$

Calcul de $S'_{2,2}$
$8*(S_{0,2} + S_{1,2} + S_{2,2} + S_{3,2}) = \underline{1110\ 1110}$

$4*(S_{2,2} + S_{0,2}) = \underline{0001\ 1101}$

$2*(S_{2,2} + S_{3,1}) = 2*(0011\ 1011 + 0010\ 1001) = 2*(\mathbf{0}001\ 0010) = \underline{0010\ 0100}$

$S'_{2,2} = 1110\ 1110 + 0001\ 1101 + 0010\ 0100 + 1111\ 0111 + 1011\ 1110 + 0010\ 1001$
$S'_{2,2} = 1011\ 0111 = \mathbf{B7}$

Calcul de $S'_{2,3}$
$8*(S_{0,3} + S_{1,3} + S_{2,3} + S_{3,3}) = \underline{0000\ 1110}$

$4*(S_{2,3} + S_{0,3}) = \underline{1011\ 1101}$

$2*(S_{2,3} + S_{3,3}) = 2*(1111\ 1001 + 0001\ 1010) = 2*(\mathbf{1}110\ 0011)$

$2^* (S_{2,3} + S_{3,3}) = 1100\ 0110 + 0001\ 1011 = \underline{1101\ 1101}$

$S'_{2,3} = 0000\ 1110 + 1011\ 1101 + 1101\ 1101 + 0001\ 1101 + 1011\ 1001 + 0001\ 1010$
$S'_{2,3} = 1101\ 0000 = \mathbf{D0}$

Ligne n°3 ----------

$S'_{3,c} = B^* S_{0,c} + D^* S_{1,c} + 9^* S_{2,c} + E^* S_{3,c}$

$S'_{3,c} = 8^* (S_{0,c} + S_{1,c} + S_{2,c} + S_{3,c}) + 4^* (S_{3,c} + S_{1,c}) + 2^* (S_{3,c} + S_{0,c}) + S_{0,c} + S_{1,c} + S_{2,c}$

Calcul de $S'_{3,0}$
$8^* (S_{0,0} + S_{1,0} + S_{2,0} + S_{3,0}) = \underline{1101\ 0110}$

$4^* (S_{3,0} + S_{1,0}) = \underline{1000\ 0111}$

$2^* (S_{3,0} + S_{0,0}) = 2^*(0001\ 0101 + 0101\ 1111) = 2^*(\mathbf{0}100\ 1010) = \underline{1001\ 0100}$

$S'_{3,0} = 1101\ 0110 + 1000\ 0111 + 1001\ 0100 + 0101\ 1111 + 0111\ 0010 + 0110\ 0100$
$S'_{3,0} = 1000\ 1100 = \mathbf{8C}$

Calcul de $S'_{3,1}$
$8^* (S_{0,1} + S_{1,1} + S_{2,1} + S_{3,1}) = \underline{0000\ 1100}$

$4^* (S_{3,1} + S_{1,1}) = \underline{1000\ 0111}$

$2^* (S_{3,1} + S_{0,1}) = 2^*(1001\ 0010 + 0101\ 0111) = 2^*(\mathbf{1}100\ 0101)$
$2^* (S_{3,1} + S_{0,1}) = 1000\ 1010 + 0001\ 1011 = \underline{1001\ 0001}$

$S'_{3,1} = 0000\ 1100 + 1000\ 0111 + 1001\ 0001 + 0101\ 0111 + 1111\ 0101 + 1011\ 1100$
$S'_{3,1} = 0000\ 0100 = \mathbf{04}$

Calcul de $S'_{3,2}$
$8^* (S_{0,2} + S_{1,2} + S_{2,2} + S_{3,2}) = \underline{1110\ 1110}$

$4^* (S_{3,2} + S_{1,2}) = \underline{0110\ 1010}$

$2^* (S_{3,2} + S_{0,2}) = 2^*(0010\ 1001 + 1111\ 0111) = 2^*(\mathbf{1}101\ 1110)$
$2^* (S_{3,2} + S_{0,2}) = 1011\ 1100 + 0001\ 1011 = \underline{1010\ 0111}$

$S'_{3,2} = 1110\ 1110 + 0110\ 1010 + 1010\ 0111 + 1111\ 0111 + 1011\ 1110 + 0011\ 1011$
$S'_{3,2} = 0101\ 0001 = \mathbf{51}$

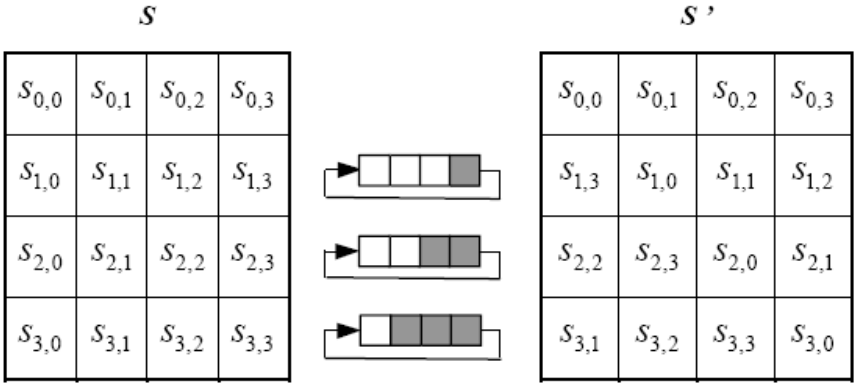
Calcul de $S'_{3,3}$
$8^* (S_{0,3} + S_{1,3} + S_{2,3} + S_{3,3}) = \underline{0000\ 1110}$
$4^* (S_{3,3} + S_{1,3}) = \underline{1011\ 1010}$

$2^* (S_{3,3} + S_{0,3}) = 2^*(0001\ 1010 + 0001\ 1101) = 2^*(\mathbf{0}000\ 0110) = \underline{0000\ 1100}$

$S'_{3,3} = 0000\ 1110 + 1011\ 1010 + 0000\ 1100 + 0001\ 1101 + 1011\ 1001 + 1111\ 1001$
$S'_{3,3} = 1110\ 0101 = \mathbf{E7}$

VIII. Déchiffrement AES – InvShiftRows

En considérant la modification suivante pour InvShiftRows remplissez la matrice de résultat de cette opération :



63	09	CD	BA
CA	53	60	70
B7	D0	E0	E1
04	51	E7	8C

IX. Déchiffrement AES – InvSubBytes

En utilisant la matrice Sbox suivante remplissez la matrice de résultat de l'opération SubBytes :

x \ 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
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

00	40	80	C0
10	50	90	D0
20	60	A0	E0
30	70	B0	F0