Q2c – 2014

The details on the back page show how the AES algorithm operates for encryption and decryption. The input to each round is a 128-bit data block often represented as a 4x4 matrix, given below. The substitute bytes table, Shift rows and Mix Column matrix details are provided on the back pages.

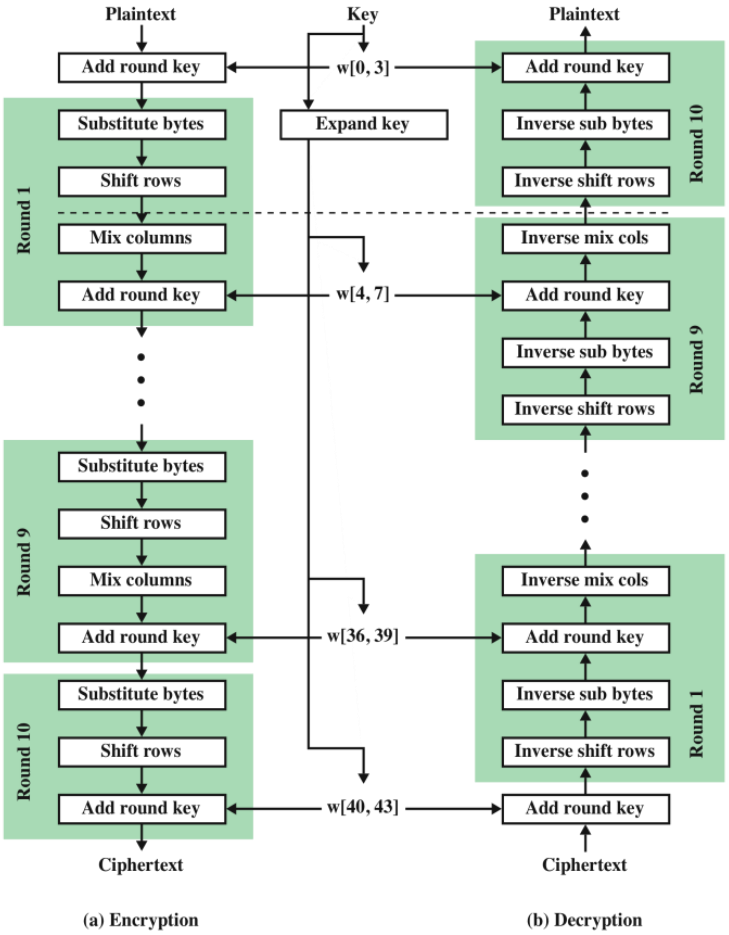
Using these details show what the input (to Sub Bytes operation) matrix/state below is transformed to after:

i) The Substitute Bytes operation. **(2%)**
ii) The Shift rows operation. **(2%)**
iii) Then show what the output of the Mix Columns operation is for **Column 1** of the resultant matrix from part (ii). **(6%)**

18	0A	B9	B5
64	68	6A	FB
5A	EF	D7	79
8E	B2	10	D4

Input State

Details for Q2.c.



Substitute Bytes S-Box

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

This example shows how the Substitute Bytes operation works

50	10	D0	81
60	20	4A	93
70	30	E1	A1
00	C0	F7	AF

→

53	CA	70	0C
D0	B7	D6	DC
51	04	F8	32
63	BA	68	79

Details for Q2.c. continued.

Shift Rows Operation

On encryption left rotate each row of State by 0,1,2,3 bytes respectively;
Example:

53	CA	70	0C
D0	B7	D6	DC
51	04	F8	32
63	BA	68	79

→

53	CA	70	0C
B7	D6	DC	D0
F8	32	51	04
79	63	BA	68

Mix Column Transformation

The Mix Column transformation uses the following Matrix:

2	3	1	1
1	2	3	1
1	1	2	3
3	1	1	2

This results in the following transformation

MixColumn

$$\text{State} \begin{bmatrix} 63 & C9 & FE & 30 \\ F2 & 63 & 26 & F2 \\ 7D & D4 & C9 & C9 \\ D4 & FA & 63 & 82 \end{bmatrix} \rightarrow \begin{bmatrix} 62 & 02 & 27 & 26 \\ CF & 92 & 91 & 0D \\ 0C & 0C & F4 & D6 \\ 99 & 18 & 30 & 74 \end{bmatrix} \text{State}$$

AES Polynomial P = 10001 1011

Needed if the result of the multiplication has an overflow.

Q2c 2014 EE6011

This is After Round Key Addition

14	0A	B9	B5
64	68	6A	FB
5A	EF	D7	79
8E	B2	10	D4

After Substitute bytes

AD	67	56	D5
43	45	02	0F
BE	DF	0E	B6
19	37	CA	48

After Shift Rows

No shift
shift left by 1 (Rotate)
Rotate " by 2
" " " 3

AD	67	56	D5
45	02	0F	43
0E	B6	BE	DF
48	19	37	CA

Mix Columns

AD		2	3	1	1		
45	*	1	2	3	1		
0E		1	1	2	3		
48		3	1	1	2		

Replace AD with 02 * AD ⊕ 03 * 45 ⊕ 01 * 0E ⊕ 01 * 48
Replace 45 with 01 * AD ⊕ 02 * 45 ⊕ 03 * 0E ⊕ 01 * 48
Replace 0E with 01 * AD ⊕ 01 * 45 ⊕ 02 * 0E ⊕ 03 * 48
Replace 48 with 03 * AD ⊕ 01 * 45 ⊕ 01 * 0E ⊕ 02 * 48

AD

AD * 02

AD = 1010 1101

*02 ⇒ 1010 1010 — bit 9 set so perform XOR with P (10001 1011)

XOR P = 10001 1011

0100 0001 = 41

45 * 03 = (45 * 2) XOR 45

45 = 0100 0101

*02 ⇒ 1000 1010

XOR 45 0100 0101

1100 1111 = CF

OE * 01 = OE

48 * 01 = 48

Now Perform XOR

```
  0100 0001   41
⊕ 1100 1111   CF
  ---------
  1000 1110
⊕ 0000 1110   OE
  ---------
  1000 0000
⊕ 0100 1000   48
  ---------
  1100 1000
     C    8
```

Replace AD with C8.

45

[AD * 01 = AD

45 * 02

45 = 0100 0101
*02 = 1000 1010 = 8A

0E * 03 = (0E * 02) ⊕ 0E

0E = 0000 1110
*02 = 0001 1100
⊕ 0E = 0000 1110
0001 0010 = 12

[46 * 01 = 46

Now XOR Them.

AD ⊕ 8A
1010 1101
1000 1010
0010 0111

⊕ 12
0001 0010
0011 0101

⊕ 46
0100 1000
0111 1101 = 7D

Replace **45** with 7D

~~0E~~

$[AD * 01 = AD$

$[45 * 01] = 45$

$[0E * 02$

$0E = 0000\ 1110$

$*02 = 0001\ 1100 = 1C$

$[48 * 03 = (48 * 02) \text{ XOR } 48$

$48 = 0100\ 1000$

$*02 = 1001\ 0000$

$\oplus 48 = 0100\ 1000$

$1101\ 1000 = D8$

Now XOR Them

$AD = 1010\ 1101$

$\oplus 45 = 0100\ 0101$

$1110\ 1000$

$\oplus 1C = 0001\ 1100$

$1111\ 0100$

$\oplus D8 = 1101\ 1000$

$0010\ 1100 = 2C$

Replace ~~0D~~ 0E with 2C

48

AD * 03 = (AD * 02) XOR AD

AD = 1010 1101

*02 = 10101 1010 — bit 9 set to 1 so XOR with Polynomial P (100011011)

⊕ 10001 1011

00100 0001

⊕ AD 1010 1101

1110 1100 = EC

[45 * 01 = 45

[0E * 01 = 0E

[48 * 02

48 = 0100 1000

*02 = 1001 0000 = 90

Now XOR Them

EC = 1110 1100

⊕ 45 0100 0101

1010 1001

⊕ 0E = 0000 1110

1010 0111

⊕ 90 = 1001 0000

0011 0111 = 37

Replace 48 with 37

column 1 becomes