Perform the following matrix calculations

1. $\begin{bmatrix} 2 & 3 & -1 \\ 1 & 0 & 4 \\ -1 & 2 & 0 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ 2 & 1 \\ 1 & 4 \end{bmatrix}$

2. $\begin{bmatrix} 3 & 7 & 1 \\ 3 & 4 & 0 \\ 2 & 7 & 5 \end{bmatrix} \begin{bmatrix} 5 & 0 & 1 \\ 2 & 1 & 0 \\ 3 & 1 & 4 \end{bmatrix}$ in $\mathbb{Z}_8$

3. $\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$ in $\mathbb{Z}_2$

Details of AES round structure

From Paar, Pelzl, and Güneysu

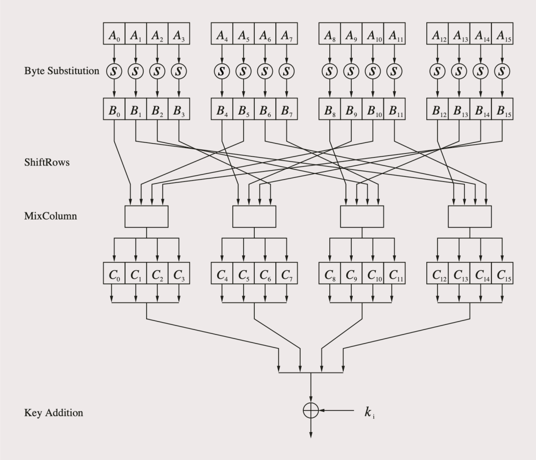
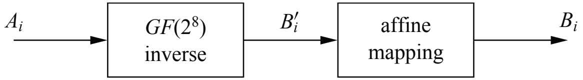


Fig. 4.3 AES round function for rounds $1, 2, \ldots, n_r - 1$

The Byte Substitution Layer / AES S-box

From Paar, Pelzl, and Güneysu



where the affine mapping is

$$MB'_i + v \mod 2$$

with matrix M and vector v

$$\underset{\textbf{B\_i}}{\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix}} \equiv \underset{\textbf{M}}{\begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix}} \underset{\textbf{B'\_i}}{\begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix}} + \underset{\textbf{v}}{\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}} \mod 2$$

Multiplicative inverses in $GF(2^8)$

From Paar, Pelzl, and Güneysu

Table 4.2 Multiplicative inverse table in $GF(2^8)$ for bytes xy used within the AES S-box, with the irreducible polynomial $P(x) = x^8 + x^4 + x^3 + x + 1$

X \ Y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	8D	F6	CB	52	7B	D1	E8	4F	29	C0	B0	E1	E5	C7
1	74	B4	AA	4B	99	2B	60	5F	58	3F	FD	CC	FF	40	EE	B2
2	3A	6E	5A	F1	55	4D	A8	C9	C1	0A	98	15	30	44	A2	C2
3	2C	45	92	6C	F3	39	66	42	F2	35	20	6F	77	BB	59	19
4	1D	FE	37	67	2D	31	F5	69	A7	64	AB	13	54	25	E9	09
5	ED	5C	05	CA	4C	24	87	BF	18	3E	22	F0	51	EC	61	17
6	16	5E	AF	D3	49	A6	36	43	F4	47	91	DF	33	93	21	3B
7	79	B7	97	85	10	B5	BA	3C	B6	70	D0	06	A1	FA	81	82
8	83	7E	7F	80	96	73	BE	56	9B	9E	95	D9	F7	02	B9	A4
9	DE	6A	32	6D	D8	8A	84	72	2A	14	9F	88	F9	DC	89	9A
A	FB	7C	2E	C3	8F	B8	65	48	26	C8	12	4A	CE	E7	D2	62
B	0C	E0	1F	EF	11	75	78	71	A5	8E	76	3D	BD	BC	86	57
C	0B	28	2F	A3	DA	D4	E4	0F	A9	27	53	04	1B	FC	AC	E6
D	7A	07	AE	63	C5	DB	E2	EA	94	8B	C4	D5	9D	F8	90	6B
E	B1	0D	D6	EB	C6	0E	CF	AD	08	4E	D7	E3	5D	50	1E	B3
F	5B	23	38	34	68	46	03	8C	DD	9C	7D	A0	CD	1A	41	1C

Table 4.3 AES S-Box: Substitution values in hexadecimal notation for input byte (xy)

									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
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

The ShiftRows Layer

From Paar, Pelzl, and Güneysu

Place output from byte substitution in a matrix

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

Perform the ShiftRows

B_0	B_4	B_8	B_{12}	no shift
B_5	B_9	B_{13}	B_1	$\longleftarrow$ one position left shift
B_{10}	B_{14}	B_2	B_6	$\longleftarrow$ two positions left shift
B_{15}	B_3	B_7	B_{11}	$\longleftarrow$ three positions left shift

Compare to diagram

B_0	B_5	B_{10}	B_{15}	B_4	B_9	B_{14}	B_3	B_8	B_{13}	B_2	B_7	B_{12}	B_1	B_6	B_{11}

The MixColumns Layer

$$\begin{bmatrix} C_0 & C_4 & C_8 & C_{12} \\ C_1 & C_5 & C_9 & C_{13} \\ C_2 & C_6 & C_{10} & C_{14} \\ C_3 & C_7 & C_{11} & C_{15} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} B_0 & B_4 & B_8 & B_{12} \\ B_5 & B_9 & B_{13} & B_1 \\ B_{10} & B_{14} & B_2 & B_6 \\ B_{15} & B_3 & B_7 & B_{11} \end{bmatrix}$$

Notice that all operations in the matrix multiplication are taking place in $GF(2^8)$!

The MixColumns Layer

From Paar, Pelzl, and Güneysu

$$\begin{bmatrix} C_0 & C_4 & C_8 & C_{12} \\ C_1 & C_5 & C_9 & C_{13} \\ C_2 & C_6 & C_{10} & C_{14} \\ C_3 & C_7 & C_{11} & C_{15} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} B_0 & B_4 & B_8 & B_{12} \\ B_5 & B_9 & B_{13} & B_1 \\ B_{10} & B_{14} & B_2 & B_6 \\ B_{15} & B_3 & B_7 & B_{11} \end{bmatrix}$$

Notice that all operations in the matrix multiplication are taking place in $GF(2^8)$!

If the output from the Byte Substitution Layer is

B_0	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}	B_{13}	B_{14}	B_{15}
$2A$	$C2$	$1F$	43	$8A$	03	17	02	41	32	18	CB	$A4$	20	$9B$	37

What is the output byte C_0 from the MixColumns layer?

The 128-bit AES Key Schedule (10 rounds)

From Paar, Pelzl, and Güneysu

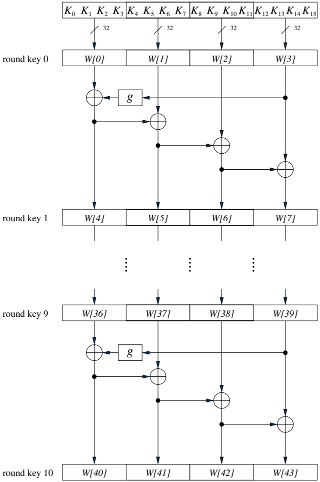
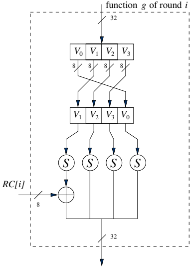


Fig. 4.5 AES key schedule for 128-bit key size



$$RC[i] = x^i$$

$\boxed{\text{Need to generate 44 words of 32-bits each}}$

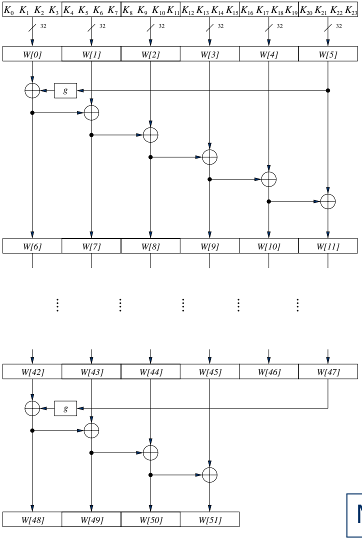
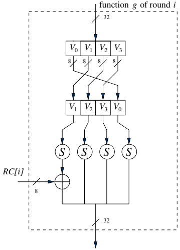


Fig. 4.6 AES key schedule for 192-bit key sizes



$$RC[i] = x^i$$

Need to generate 52 words of 32-bits each

The 256-bit AES Key Schedule (14 rounds)

From Paar, Pelzl, and Güneysu

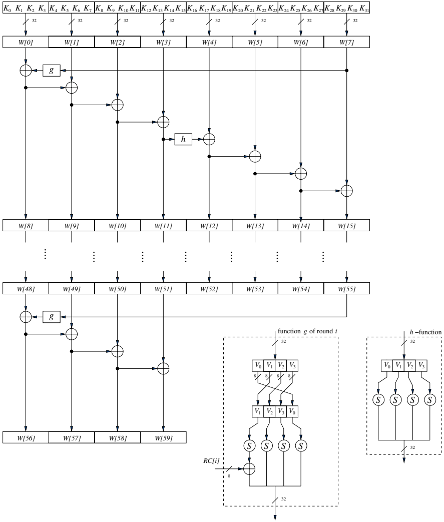


Fig. 4.7 AES key schedule for 256-bit key size

$$RC[i] = x^i$$

Need to generate 60 words of 32-bits each