Data and Network Security

Course Code: IT-4542

AES: The Advanced Encryption Standard

The number of rounds is 10 for the case when the encryption key is 128 bit long. (the number of rounds is 12 when the key is 192 bits, and 14 when the key is 256.)

For encryption, each round consists of the following four steps:

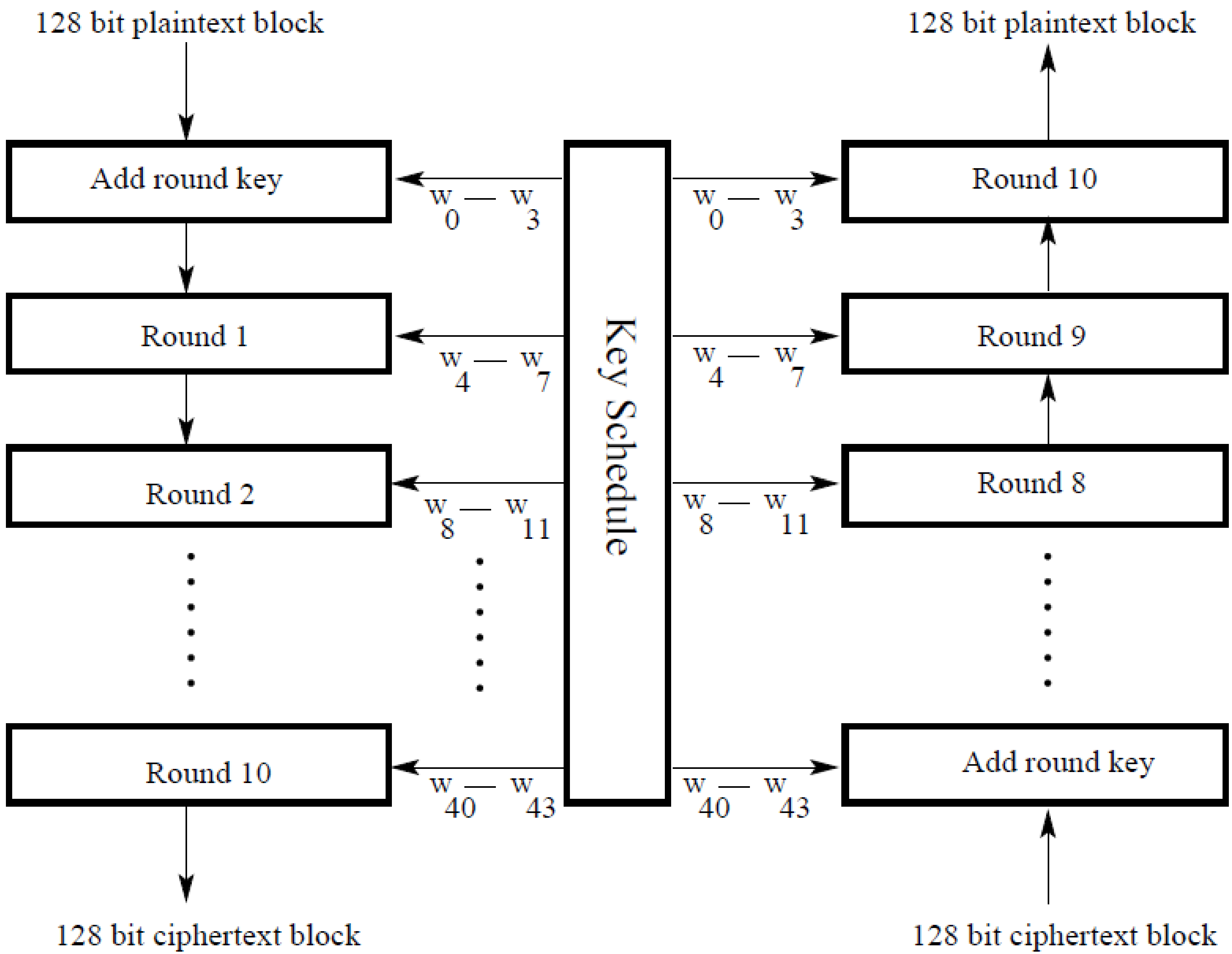
1) Substitute bytes,
2) Shift rows,
3) Mix columns
4) Add round key.

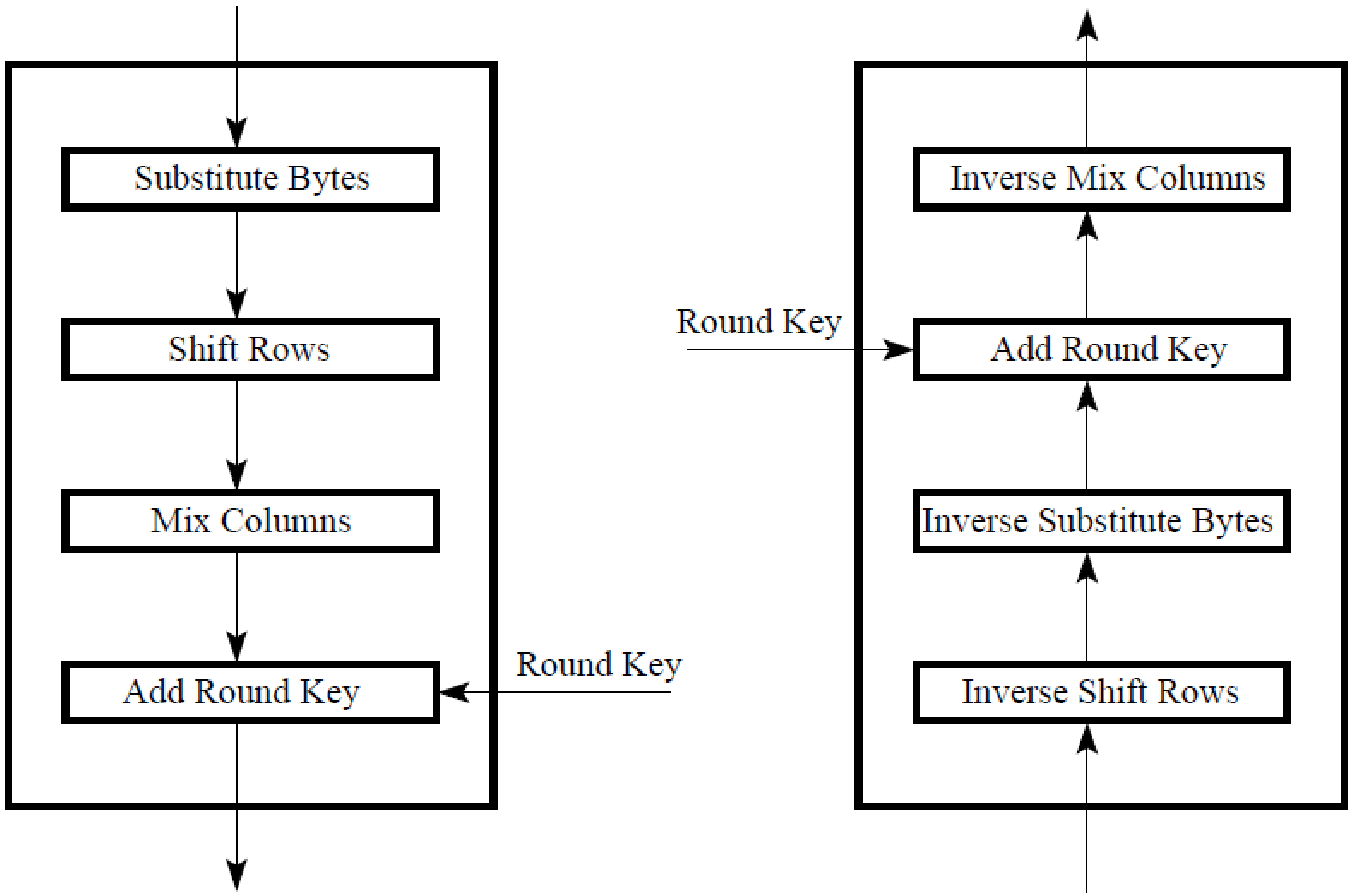
For decryption, each round consists of the following four steps:

1) Inverse shift rows
2) Inverse substitute bytes
3) Add round key
4) Inverse mix columns.

The last round for encryption does not involve the “Mix columns” step. The last round for decryption does not involve the “Inverse mix columns” step.

$$\begin{bmatrix} byte_0 & byte_4 & byte_8 & byte_{12} \\ byte_1 & byte_5 & byte_9 & byte_{13} \\ byte_2 & byte_6 & byte_{10} & byte_{14} \\ byte_3 & byte_7 & byte_{11} & byte_{15} \end{bmatrix}$$


128 bit plaintext block
128 bit plaintext block
Add round key
Round 1
Round 2
Round 10
Key Schedule
Round 10
Round 9
Round 8
Add round key
w0 — w3
w4 — w7
w8 — w11
w40 — w43
w0 — w3
w4 — w7
w8 — w11
w40 — w43
128 bit ciphertext block
128 bit ciphertext block



Encryption Round

Decryption Round

STEP 1: Bytes substitution

- The corresponding substitution step used during decryption is called Inverse substitution Bytes.
- This step consists of using a 16 × 16 lookup table to find a replacement byte for a given byte in the input state array.
- The entries in the lookup table are created by using the notions of multiplicative inverses in $GF(2^8)$ and bit scrambling to destroy the bit-level correlations inside each byte.

```
         0     1     2     3     4     5     6     7     8     9 ....
      ----------------------------------------------------------
0   | 00    01    02    03    04    05    06    07    08    09    ....
    |
1   | 10    11    12    13    14    15    16    17    18    19    ....
    |
2   | 20    21    22    23    24    25    26    27    28    29    ....
    |
          .........
          .........
```

STEP 2: Shift Rows - shifting the rows of the state array

- The corresponding transformation during decryption is Inverse Shift Rows
- The goal of this transformation is to scramble the byte order inside each 128-bit block.

STEP 3: Mix Columns – mixing up of the bytes in each column

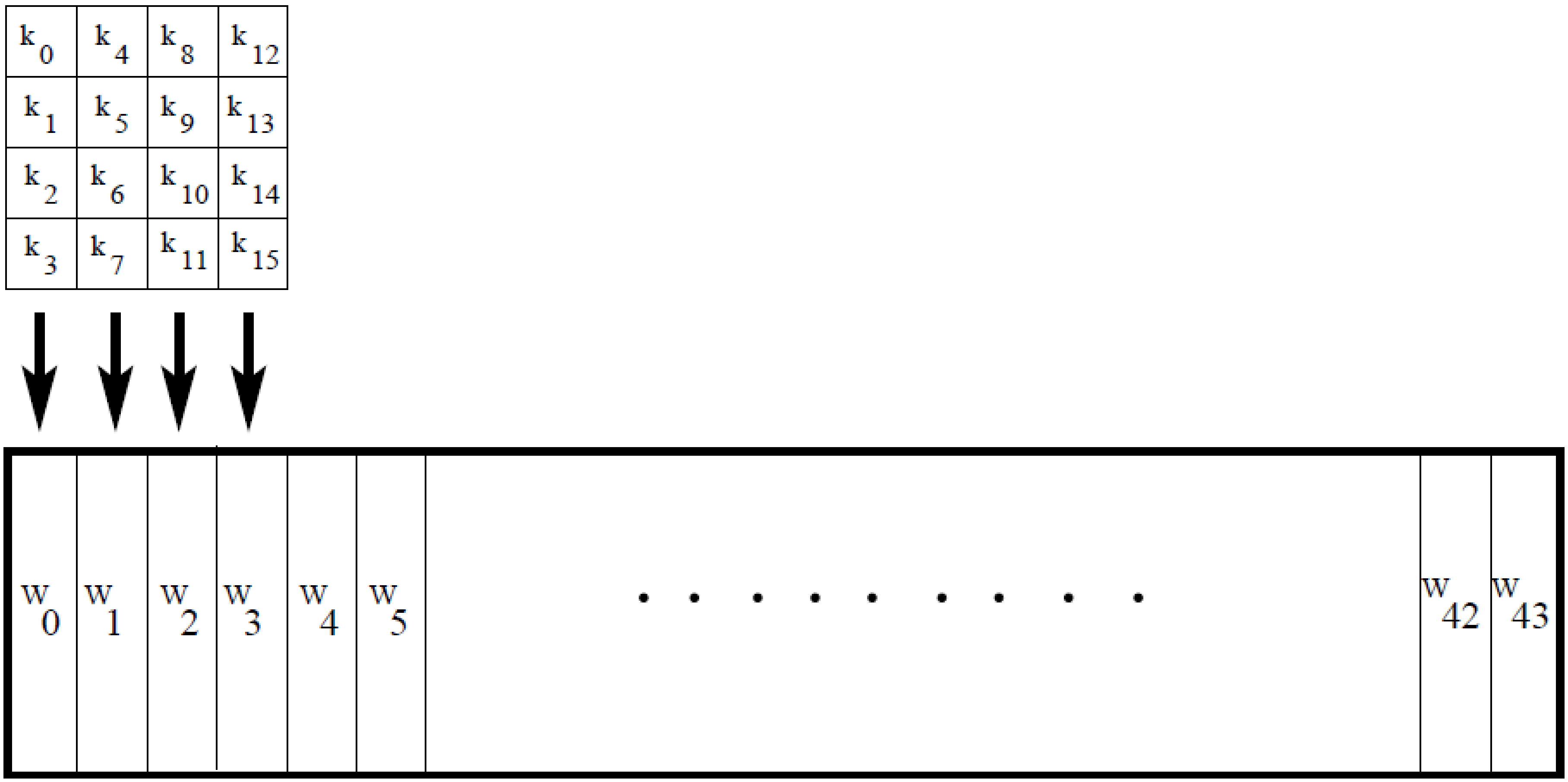
- The corresponding transformation during decryption is inverse mix column transformation.
- The goal is to further scramble up the 128-bit input block.
- The shift-rows step along with the mix-column step causes each bit of the cipher text to depend on every bit of the plaintext after 10 rounds of processing.

STEP 4: Add Round Key

- The corresponding step during decryption is Inverse Add Round Key.

The Encryption Key and its Expansion

- Assuming a 128-bit key, the key is also arranged in the form of an array of 4×4 bytes. As with the input block, the first word from the key fills the first column of the array, and so on.
- The four column words of the key array are expanded into a schedule of 44 words.
- Each round consumes four words from the key schedule.
- The key is expanded into a key schedule consisting of 44 4-byte words.


k0 k4 k8 k12
k1 k5 k9 k13
k2 k6 k10 k14
k3 k7 k11 k15
w0 w1 w2 w3 w4 w5
w42 w43

Modern way of Byte Substitution

Let x_{in} be a byte of the state array for which we seek a substitute byte x_{out}. We can write $x_{out} = f(x_{in})$. The function $f()$ involves two nonlinear operations:

(i) We first find the multiplicative inverse x' of x_{in} in $GF(2^8)$

(ii) Then we scramble the bits of x' by XORing x' with four different circularly rotated versions of itself and with a special constant byte c = 0x63.

The four circular rotations are through 4, 5, 6, and 7 bit positions to the right.

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

82	9	106	213	48	54	165	56	191	64	163	158	129	243	215	251
124	227	57	130	155	47	255	135	52	142	67	68	196	222	233	203
84	123	148	50	166	194	35	61	238	76	149	11	66	250	195	78
8	46	161	102	40	217	36	178	118	91	162	73	109	139	209	37
114	248	246	100	134	104	152	22	212	164	92	204	93	101	182	146
108	112	72	80	253	237	185	218	94	21	70	87	167	141	157	132
144	216	171	0	140	188	211	10	247	228	88	5	184	179	69	6
208	44	30	143	202	63	15	2	193	175	189	3	1	19	138	107
58	145	17	65	79	103	220	234	151	242	207	206	240	180	230	115
150	172	116	34	231	173	53	133	226	249	55	232	28	117	223	110
71	241	26	113	29	41	197	137	111	183	98	14	170	24	190	27
252	86	62	75	198	210	121	32	154	219	192	254	120	205	90	244
31	221	168	51	136	7	199	49	177	18	16	89	39	128	236	95
96	81	127	169	25	181	74	13	45	229	122	159	147	201	156	239
160	224	59	77	174	42	245	176	200	235	187	60	131	83	153	97
23	43	4	126	186	119	214	38	225	105	20	99	85	33	12	125

The Shift Rows Step

$$\begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2.0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3.0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} ===> \begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.1} & s_{1,2} & s_{1,3} & s_{1,0} \\ s_{2.2} & s_{2,3} & s_{2,0} & s_{2,1} \\ s_{3.3} & s_{3,0} & s_{3,1} & s_{3,2} \end{bmatrix}$$

$$\begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2.0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3.0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} ===> \begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.3} & s_{1,0} & s_{1,1} & s_{1,2} \\ s_{2.2} & s_{2,3} & s_{2,0} & s_{2,1} \\ s_{3.1} & s_{3,2} & s_{3,3} & s_{3,0} \end{bmatrix}$$

The Mix Columns Step

$$
\begin{aligned}
s'_{0,j} &= (0\text{x}02 \times s_{0,j}) \otimes (0\text{x}03 \times s_{1,j}) \otimes s_{2,j} \otimes s_{3,j} \\
s'_{1,j} &= s_{0,j} \otimes (0\text{x}02 \times s_{1,j}) \otimes (0\text{x}03 \times s_{2,j}) \otimes s_{3,j} \\
s'_{2,j} &= s_{0,j} \otimes s_{1,j} \otimes (0\text{x}02 \times s_{2,j}) \otimes (0\text{x}03 \times s_{3,j}) \\
s'_{3,j} &= (0\text{x}03 \times s_{0,j}) \otimes s_{1,j} \otimes s_{2,j} \otimes (0\text{x}02 \times s_{3,j})
\end{aligned}
$$

$$
\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}
\times
\begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2.0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3.0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}
=
\begin{bmatrix} s'_{0.0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1.0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2.0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3.0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}
$$

Inverse of Mix Columns Step

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \times \begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2.0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3.0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0.0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1.0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2.0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3.0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

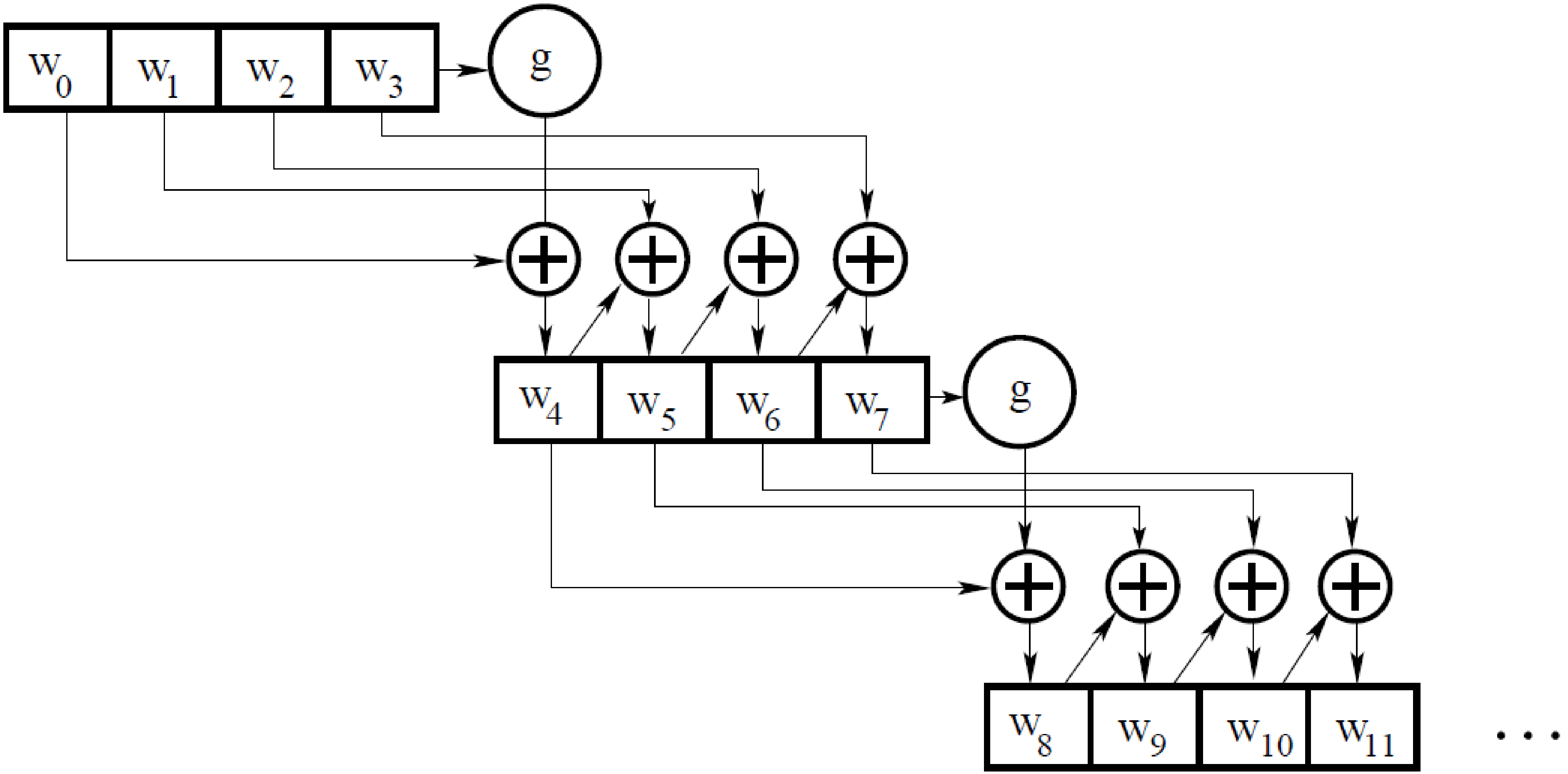
The Key Expansion Algorithm

$$\begin{bmatrix} k_0 & k_4 & k_8 & k_{12} \\ k_1 & k_5 & k_9 & k_{13} \\ k_2 & k_6 & k_{10} & k_{14} \\ k_3 & k_7 & k_{11} & k_{15} \end{bmatrix}$$

$$\Downarrow$$

$$\begin{bmatrix} w_0 & w_1 & w_2 & w_3 \end{bmatrix}$$

The Key Expansion Algorithm



How to find *g*

- Perform a one-byte left circular rotation on the argument 4-byte word.
- Perform a byte substitution for each byte of the word returned by the previous step by using the same 16×16 lookup table as used in the Substitute Bytes step of the encryption rounds.
- XOR the bytes obtained from the previous step with what is known as a round constant. The round constant is a word whose three rightmost bytes are always zero.

Round Constant

- The addition of the round constants is for the purpose of destroying any symmetries that may have been introduced by the other steps in the key expansion algorithm.

$$Rcon[i] = (RC[i],\ 0\text{x}00,\ 0\text{x}00,\ 0\text{x}00)$$

$$\begin{aligned} RC[1] &= 0\text{x}01 \\ RC[j] &= 0\text{x}02 \times RC[j-1] \end{aligned}$$

Key: hello

```
word 0:  [104, 101, 108, 108]
word 1:  [111, 48, 48, 48]
word 2:  [48, 48, 48, 48]
word 3:  [48, 48, 48, 48]

word 4:  [109, 97, 104, 104]
word 5:  [2, 81, 88, 88]
word 6:  [50, 97, 104, 104]
word 7:  [2, 81, 88, 88]

word 8:  [190, 11, 2, 31]
word 9:  [188, 90, 90, 71]
word 10:  [142, 59, 50, 47]
word 11:  [140, 106, 106, 119]
```