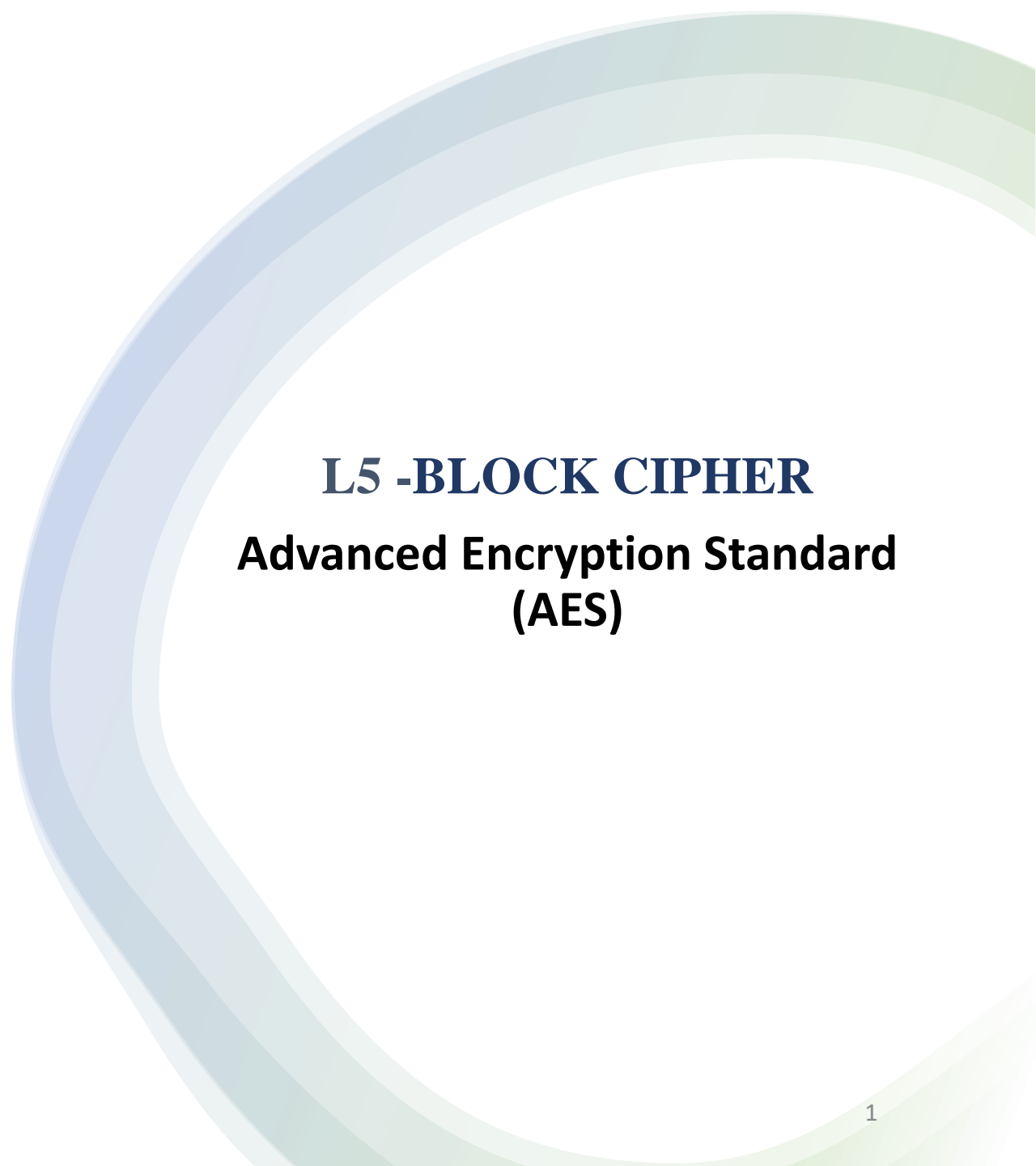




Data Security and Privacy

DSE 3258

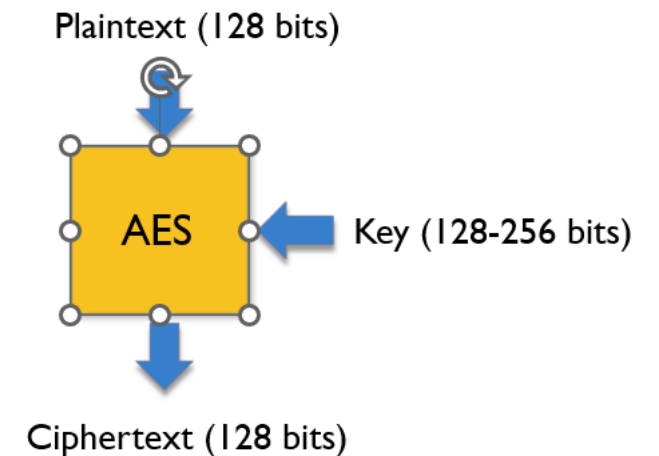


L5 -BLOCK CIPHER

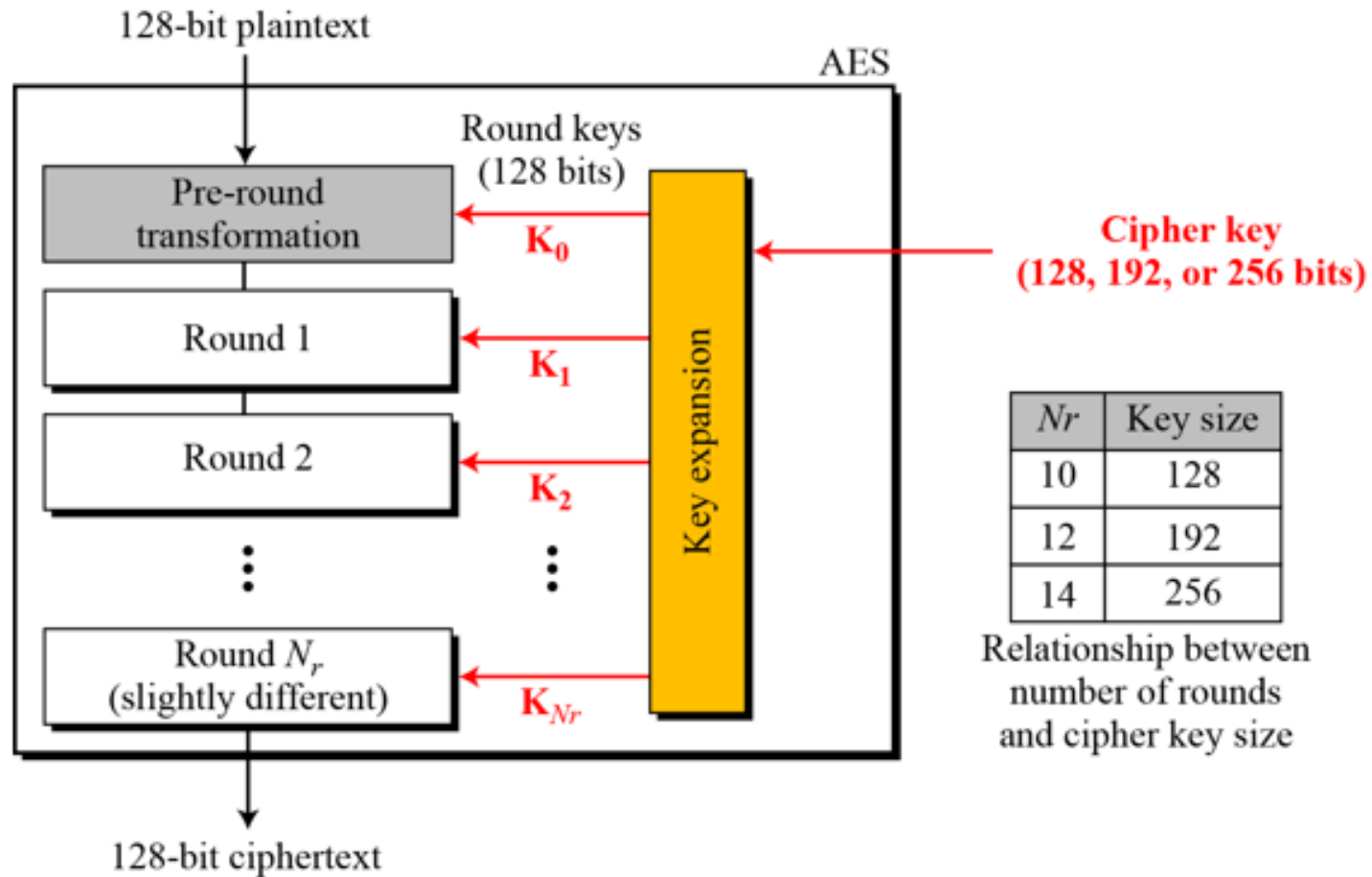
Advanced Encryption Standard (AES)

Introduction

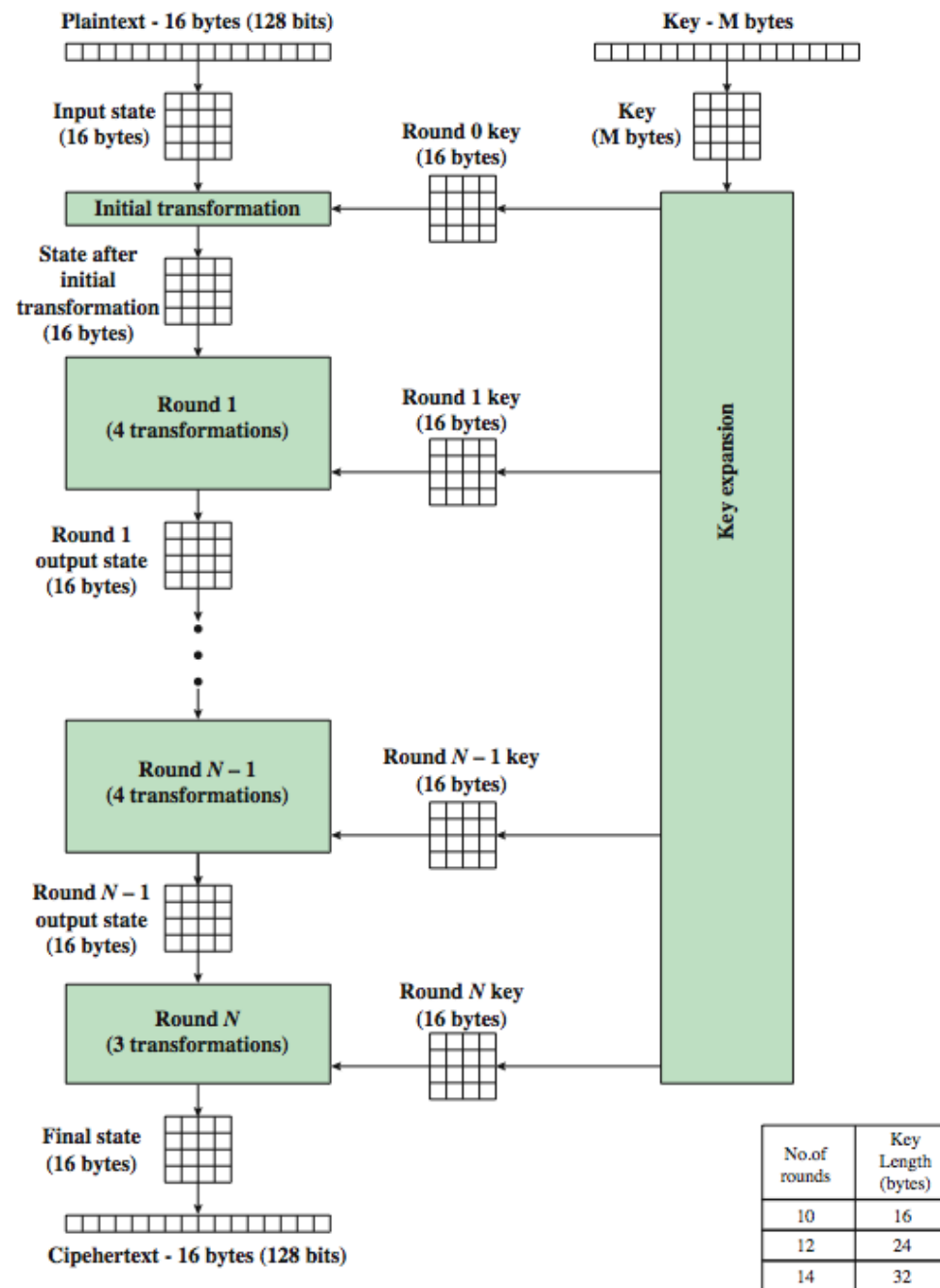
- Advanced Encryption Standard
- Symmetric block cipher
- Designed by Rijmen-Daemen in Belgium
- has 128/192/256 bit keys, 128 bit data
- The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length
- an iterative rather than Feistel cipher
 - processes data as block of 4 columns of 4 bytes
 - operates on entire data block in every round
- Designed to have:
 - resistance against known attacks
 - speed and code compactness on many CPUs
 - design simplicity



AES Encryption Process



AES Encryption Process (Detailed View)



High Level Description

Key Expansion

- Round keys are derived from the cipher key using Rijndael's key schedule

Initial Round

- AddRoundKey : Each byte of the state is combined with the round key using bitwise xor

Rounds

- SubBytes : non-linear substitution step
- ShiftRows : transposition step
- MixColumns : mixing operation of each column.
- AddRoundKey

Final Round

- SubBytes
- ShiftRows
- AddRoundKey

No MixColumns

AES Encryption Process (Cont..)

- The input to the encryption and decryption algorithms is a single 128-bit block which is depicted as a 4 * 4 square matrix of bytes.
- Input block is copied into the **State** array, which is modified at each stage of encryption or decryption. At the final stage, **State** is copied to an output matrix.



(a) Input, state array, and output

- The key is also depicted as a square matrix of bytes. Later, this key is expanded into an array of key schedule words.

AES Encryption Process (Cont..)

- The key is also depicted as a square matrix of bytes. Later, this key is expanded into an array of key schedule words.
- For 128 bit key, each word is four bytes, and the total key schedule is 44 words for the 128-bit key.



(b) Key and expanded key

AES Encryption Process (Cont..)

- The ordering of bytes within a matrix is by column.
- So, for example, the first four bytes of a 128-bit plaintext input to the encryption cipher occupy the first column of the in matrix, the second four bytes occupy the second column, and so on.
- Similarly, the first four bytes of the expanded key, which form a word, occupy the first column of the w matrix.
- The cipher consists of N rounds, where the number of rounds depends on the key length.
- The first N - 1 rounds consist of four distinct transformation functions: **SubBytes**, **ShiftRows**, **MixColumns**, and **AddRoundKey**.
- The final round contains only three transformations, and there is a initial single transformation (**AddRoundKey**) before the first round, which can be considered Round 0.
- Each transformation takes one or more 4×4 matrices as input and produces a 4×4 matrix as output.
- The key expansion function generates N + 1 round keys, each of which is a distinct 4×4 matrix. Each round key serves as one of the inputs to the **AddRoundKey transformation** in each round.

AES Encryption Process (Cont..)

Table 6.1 AES Parameters

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

AES Detailed Structure

1. One noteworthy feature of this structure is that it is not a Feistel structure. AES processes the entire data block as a single matrix during each round using substitutions and permutation.
2. The key that is provided as input is expanded into an array of forty-four 32-bit words, $w[i]$. Four distinct words (128 bits) serve as a round key for each round.
3. Four different stages are used, one of permutation and three of substitution:
 - a. Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block.
 - b. ShiftRows: A simple permutation.
 - c. MixColumns: A substitution that makes use of matrix multiply of groups
 - d. AddRoundKey: A simple bitwise XOR of the current block with a portion of the expanded key
4. For both encryption and decryption, the cipher begins with an **AddRoundKey** stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.
5. Only the **AddRoundKey** stage makes use of the key. For this reason, the cipher begins and ends with an **AddRoundKey** stage.

AES Detailed Structure

6. The **AddRoundKey** stage is, in effect, a form of Vernam cipher and by itself would not be formidable. The other three stages together provide confusion, diffusion, and nonlinearity, but by themselves would provide no security because they do not use the key..
7. Each stage is easily reversible. For the **Substitute Byte**, **ShiftRows**, and **MixColumns** stages, an **inverse function** is used in the decryption algorithm.
8. As with most block ciphers, the decryption algorithm makes use of the expanded key in reverse order. However, the decryption algorithm is not identical to the encryption algorithm.
10. The final round of both encryption and decryption consists of only three stages. Again, this is a consequence of the particular structure of AES and is required to make the cipher reversible

AES Inner Workings of a Round

- The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages.
- This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm. The four stages are as follows:
 - 1. Substitute bytes
 - 2. Shift rows
 - 3. Mix Columns
 - 4. Add Round Key

AES Inner Workings of a Round

- **Substitute Bytes**
 - The forward substitute byte transformation, called SubBytes.
 - It is a table lookup using a 16×16 matrix of byte values called an s-box.
 - This matrix consists of all the possible combinations of an 8 bit sequence ($2^8 = 16 \times 16 = 256$). However, the s-box is not just a random permutation of these values and there is a well defined creating the s-box tables.
 - Again the matrix that gets operated upon throughout the encryption is known as **state**.
 - In a round each byte is mapped into a new byte in the following way: the leftmost nibble of the byte is used to specify a particular row of the s-box and the rightmost nibble specifies a column. For example, the byte {95} (curly brackets represent hex values selects row 9 column 5 which turns out to contain the value {2A}.
 - This is then used to update the state matrix.
 - The Inverse substitute byte transformation (known as InvSubBytes) makes use of an inverse s-box. In this case what is desired is to select the value {2A} and get the value {95}.

AES Inner Workings of a Round

- Substitute Bytes

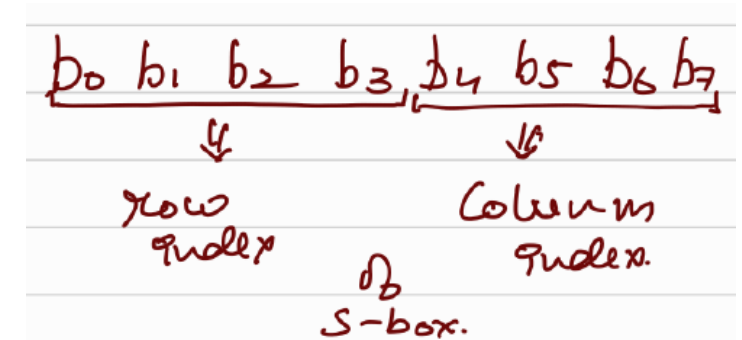
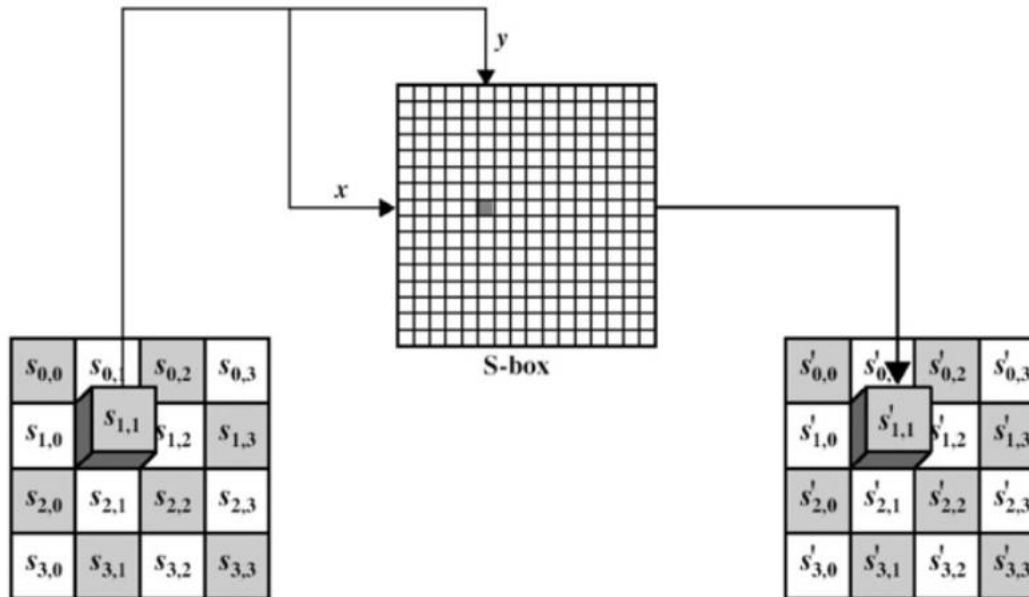


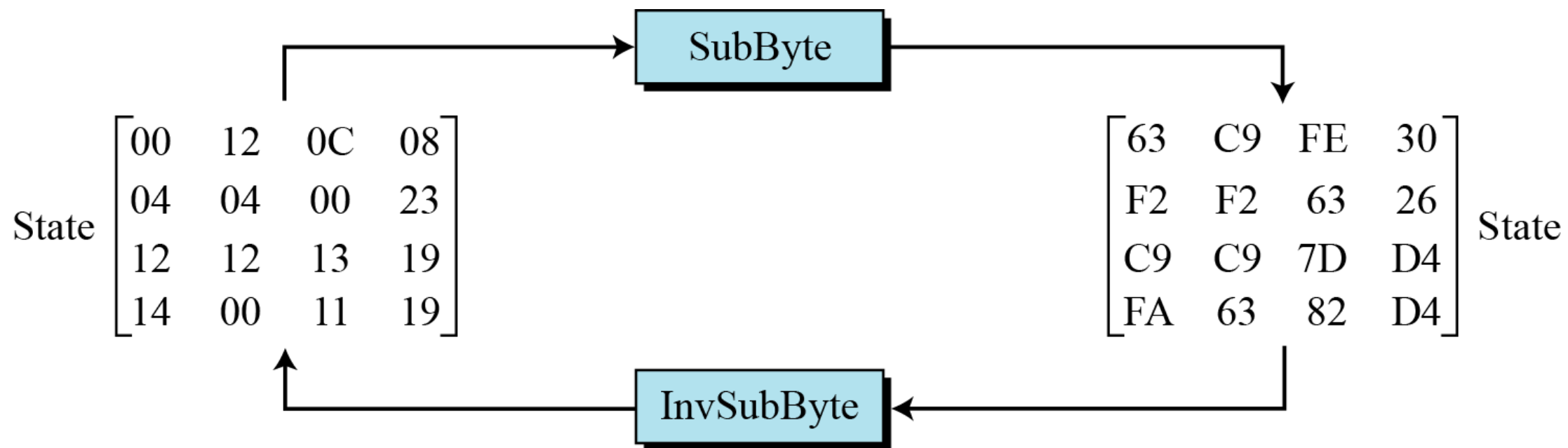
Figure 7.3: Substitute Bytes Stage of the AES algorithm.

SubBytes Table

		<i>y</i>															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
<i>x</i>	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

InvSubBytes Table

		<i>y</i>															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
<i>x</i>	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



AES Inner Workings of a Round

- **Shift Row Transformation**

It works as follow:

- The first row of state is not altered.
- The second row is shifted 1 bytes to the left in a circular manner.
- The third row is shifted 2 bytes to the left in a circular manner.
- The fourth row is shifted 3 bytes to the left in a circular manner

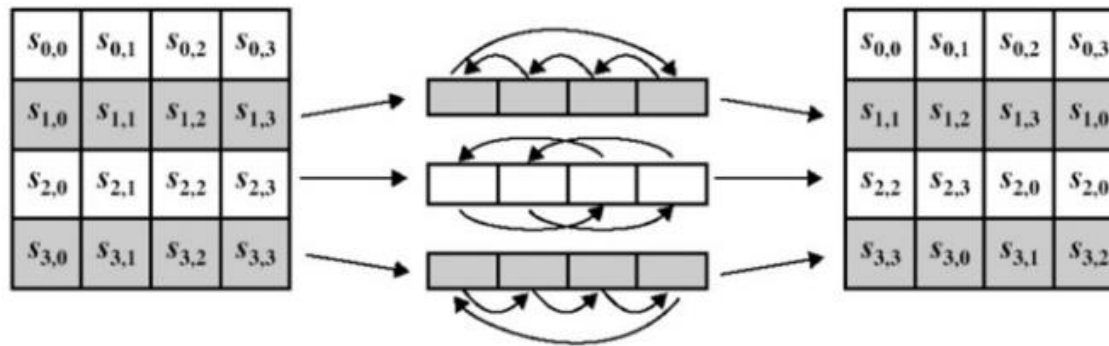
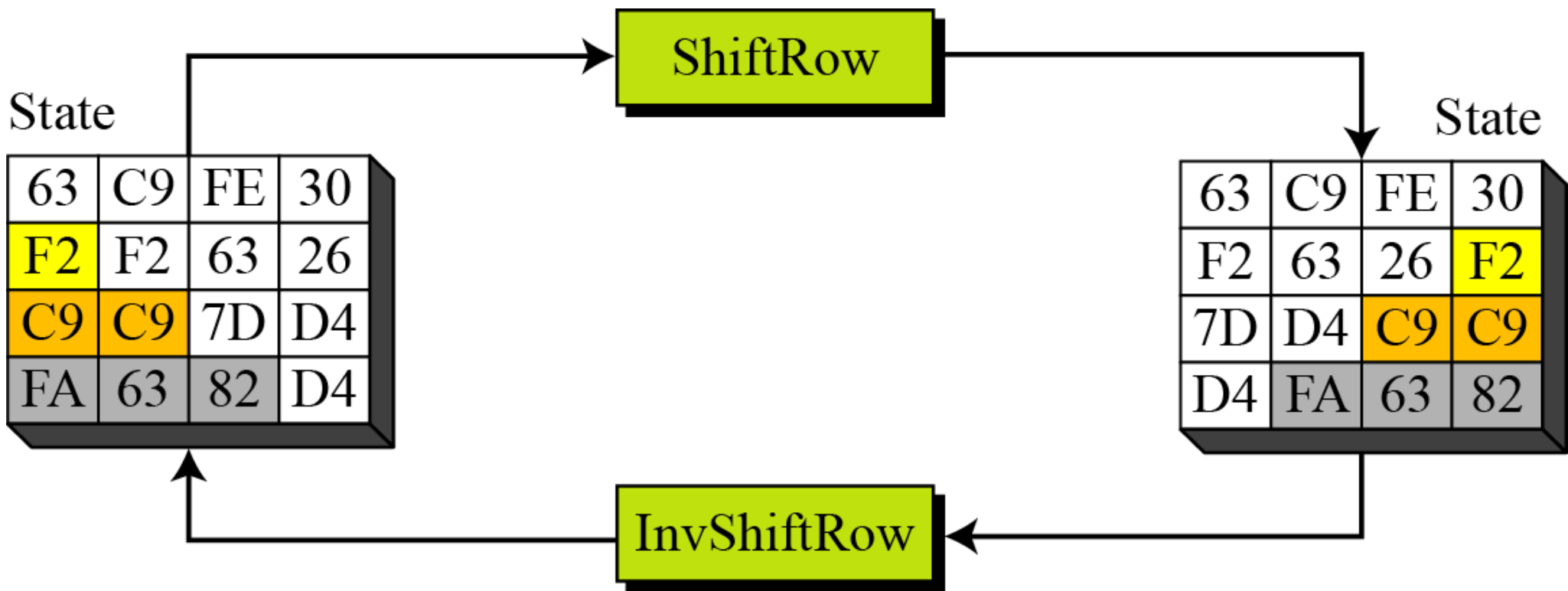


Figure 7.5: ShiftRows stage.

The **Inverse Shift Rows** transformation (known as InvShiftRows) performs these circular shifts in the opposite direction for each of the last three rows (the first row was unaltered to begin with)



AES Inner Workings of a Round

• Mix Column Transformation

This stage (known as MixColumn) is basically a substitution but it makes use of arithmetic of $GF(2^8)$. (Galois Field)

Each column is operated on individually.

Each byte of a column is mapped into a new value that is a **function of all four bytes** in the column.

Effectively a matrix multiplication in $GF(2^8)$ using prime poly $m(x) = x^8 + x^4 + x^3 + x + 1$

The transformation can be determined by the following matrix multiplication on state:

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

Each element of the product matrix is the sum of products of elements of one row and one column.

In this case the individual additions and multiplications are performed in $GF(2^8)$.

AES Inner Workings of a Round

- Mix Column Transformation

The MixColumns transformation of a single column j ($0 \leq j \leq 3$) of state can be expressed as:

$$s'_{0,j} = (2 \bullet s_{0,j}) \oplus (3 \bullet s_{1,j}) \oplus s_{2,j} \oplus s_{3,j}$$

$$s'_{1,j} = s_{0,j} \oplus (2 \bullet s_{1,j}) \oplus (3 \bullet s_{2,j}) \oplus s_{3,j}$$

$$s'_{2,j} = s_{0,j} \oplus s_{1,j} \oplus (2 \bullet s_{2,j}) \oplus (3 \bullet s_{3,j})$$

$$s'_{3,j} = (3 \bullet s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \bullet s_{3,j})$$

where \bullet denotes multiplication over the finite field $\text{GF}(2^8)$.

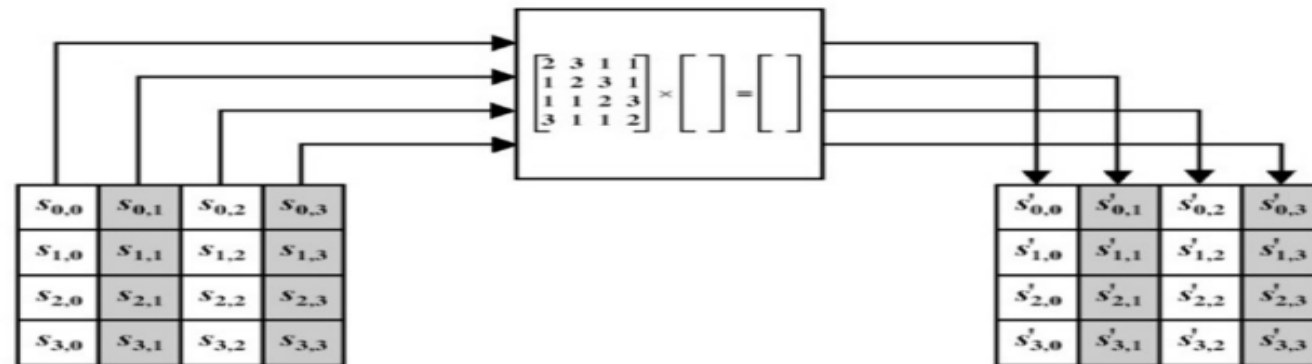


Figure 7.6: MixColumns stage.

AES Inner Workings of a Round

MixColumn and InvMixColumn

$$\begin{array}{ccc}
 \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} & \xleftrightarrow{\text{Inverse}} & \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \\
 C & & C^{-1}
 \end{array}$$

The **inverse mix column transformation**, called **InvMixColumns**, is defined by the following matrix multiplication:

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix} \quad (6.5)$$

Example

$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$	87	F2	4D	97
	6E	4C	90	EC
	46	E7	4A	C3
	A6	8C	D8	95

 \rightarrow

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

$$\begin{aligned}
 (\{02\} \cdot \{87\}) \oplus (\{03\} \cdot \{6E\}) \oplus \{46\} \oplus \{A6\} &= \{47\} \\
 \{87\} \oplus (\{02\} \cdot \{6E\}) \oplus (\{03\} \cdot \{46\}) \oplus \{A6\} &= \{37\} \\
 \{87\} \oplus \{6E\} \oplus (\{02\} \cdot \{46\}) \oplus (\{03\} \cdot \{A6\}) &= \{94\} \\
 (\{03\} \cdot \{87\}) \oplus \{6E\} \oplus \{46\} \oplus (\{02\} \cdot \{A6\}) &= \{ED\}
 \end{aligned}$$

For the first equation, we have $\{02\} \cdot \{87\} = (0000\ 1110) \oplus (0001\ 1011) = (0001\ 0101)$ and $\{03\} \cdot \{6E\} = \{6E\} \oplus (\{02\} \cdot \{6E\}) = (0110\ 1110) \oplus (1101\ 1100) = (1011\ 0010)$. Then,

$$\begin{aligned}
 \{02\} \cdot \{87\} &= 0001\ 0101 \\
 \{03\} \cdot \{6E\} &= 1011\ 0010 \\
 \{46\} &= 0100\ 0110 \\
 \{A6\} &= \underline{1010\ 0110} \\
 &0100\ 0111 = \{47\}
 \end{aligned}$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \underbrace{\begin{bmatrix} S_{00} \\ S_{01} \\ S_{02} \\ S_{03} \end{bmatrix}}_{w_1} = \begin{bmatrix} S'_{00} & S'_{10} & S'_{20} & S'_{30} \\ S'_{01} & S'_{11} & S'_{21} & S'_{31} \\ S'_{02} & S'_{12} & S'_{22} & S'_{32} \\ S'_{03} & S'_{13} & S'_{23} & S'_{33} \end{bmatrix}$$

$$\Downarrow$$

$$(02 \cdot S_{00}) \oplus (03 \cdot S_{01}) \oplus (01 \cdot S_{02}) \oplus (01 \cdot S_{03})$$

'.' \rightarrow Galois Field based multiplication

$$GF(2^8)$$

\Downarrow

$$1 = 1$$

$$2 = x$$

$$3 = x + 1$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} 87 \\ 6E \\ 46 \\ A6 \end{bmatrix} = \begin{bmatrix} \end{bmatrix}$$

$$\underline{(02 \cdot 87)} \oplus (03 \cdot 6E) \oplus (01 \cdot 46) \oplus (01 \cdot A6)$$

$$\begin{aligned} (02 \cdot 87) &= x(1000 \ 0111) \\ &= x(x^7 + x^2 + x' + 1) \\ &= \underline{x^8} + x^3 + x^2 + x \end{aligned}$$

$x^8 \rightarrow$ not possible
as we have
 x^0 to x^7
bits

So x^8 should be reduced.

By factorizing we get

$$x^8 = x^4 + x^3 + x + 1$$

So replace x^8 \rightarrow

$$x^4 + \cancel{x^3} + \cancel{x} + 1 + \cancel{x^3} + x^2 + \cancel{x}$$

$$= x^4 + x^2 + 1$$

$$= 00010101$$

$$\begin{aligned}
 (03 \cdot 6E) &= (x+1)(01101110) \\
 &= (x+1)(x^6+x^5+x^3+x^2+x) \\
 &= x^7 + \cancel{x^6} + x^4 + \cancel{x^3} + \cancel{x^2} + \\
 &\quad \cancel{x^6} + x^5 + \cancel{x^3} + \cancel{x^2} + x \\
 &= x^7 + x^5 + x^4 + x \\
 &\rightarrow = \underline{10110010}
 \end{aligned}$$

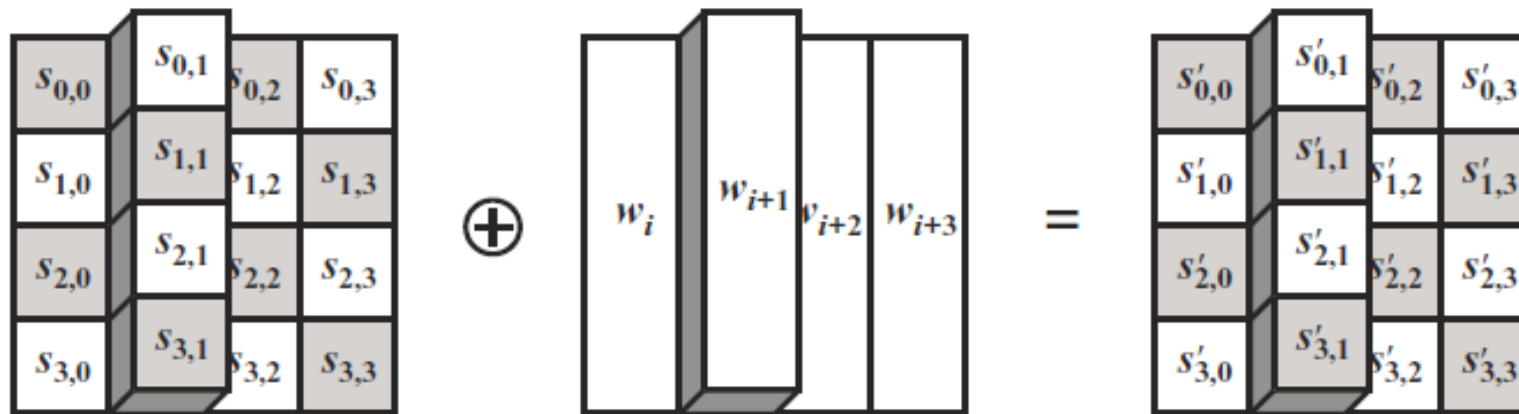
$$\begin{aligned}
 (01 \cdot 46) &= (1)(01000110) \\
 (01 \cdot A6) &= (1)(10100110)
 \end{aligned}$$

$$\begin{array}{r}
 00010101 \\
 10110010 \\
 \oplus 01000110 \\
 10100110 \\
 \hline
 01000111 \\
 \hline
 \underline{\quad 4 \quad 7 \quad}
 \end{array}$$

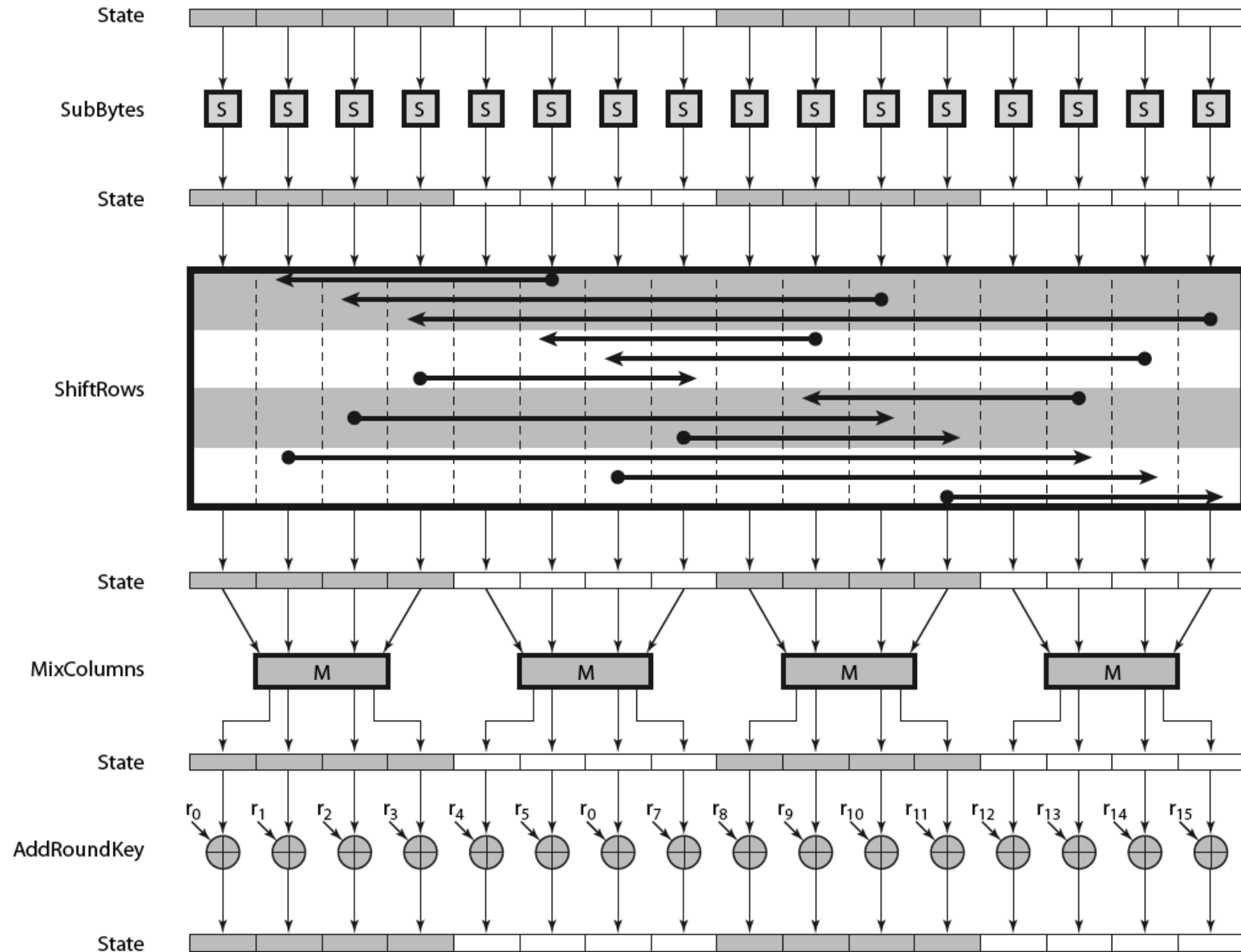
$$\begin{array}{lclclclcl}
 (\{02\} \cdot \{87\}) & \oplus & (\{03\} \cdot \{6E\}) & \oplus & \{46\} & \oplus & \{A6\} & = & \{47\} \\
 \{87\} & \oplus & (\{02\} \cdot \{6E\}) & \oplus & (\{03\} \cdot \{46\}) & \oplus & \{A6\} & = & \{37\} \\
 \{87\} & \oplus & \{6E\} & \oplus & (\{02\} \cdot \{46\}) & \oplus & (\{03\} \cdot \{A6\}) & = & \{94\} \\
 (\{03\} \cdot \{87\}) & \oplus & \{6E\} & \oplus & \{46\} & \oplus & (\{02\} \cdot \{A6\}) & = & \{ED\}
 \end{array}$$

Add Round Key Transformation

- In this stage (known as AddRoundKey) the 128 bits of state are bitwise XORed with the 128 bits of the round key. The operation is viewed as a column-wise operation between the 4 bytes of a state column and one word of the round key.



(b) Add round key transformation



Add Round Key Transformation

AES Key Expansion

Table 7.3 Words for each round

Round	Words			
Pre-round	w_0	w_1	w_2	w_3
1	w_4	w_5	w_6	w_7
2	w_8	w_9	w_{10}	w_{11}
...	...			
N_r	w_{4N_r}	w_{4N_r+1}	w_{4N_r+2}	w_{4N_r+3}

Table 7.4 RCon constants

Round	Constant (RCon)	Round	Constant (RCon)
1	(<u>01</u> 00 00 00) ₁₆	6	(<u>20</u> 00 00 00) ₁₆
2	(<u>02</u> 00 00 00) ₁₆	7	(<u>40</u> 00 00 00) ₁₆
3	(<u>04</u> 00 00 00) ₁₆	8	(<u>80</u> 00 00 00) ₁₆
4	(<u>08</u> 00 00 00) ₁₆	9	(<u>1B</u> 00 00 00) ₁₆
5	(<u>10</u> 00 00 00) ₁₆	10	(<u>36</u> 00 00 00) ₁₆

The key expansion was designed to be resistant to known cryptanalytic attacks. The inclusion of a round-dependent round constant eliminates the symmetry, or similarity, between the way in which round keys are generated in different rounds.

AES Key Expansion

- The key is copied into the first four words of the expanded key.
- The remainder of the expanded key is filled in four words at a time.
- Each added word $w[i]$ depends on the immediately preceding word, $w[i - 1]$, and the word four positions back $w[i - 4]$.
- In three out of four cases, a simple XOR is used.
- For a word whose position in the w array is a multiple of 4, a more complex function is used.
- The function g consists of the following subfunctions:
 1. **RotWord** performs a one-byte circular left shift on a word. This means that an input word $[b0, b1, b2, b3]$ is transformed into $[b1, b2, b3, b0]$.
 2. **SubWord** performs a byte substitution on each byte of its input word, using the s-box described earlier.
 3. The result of steps 1 and 2 is XORed with round constant, $Rcon[j]$

Add Round Key Transformation

AES Key Expansion

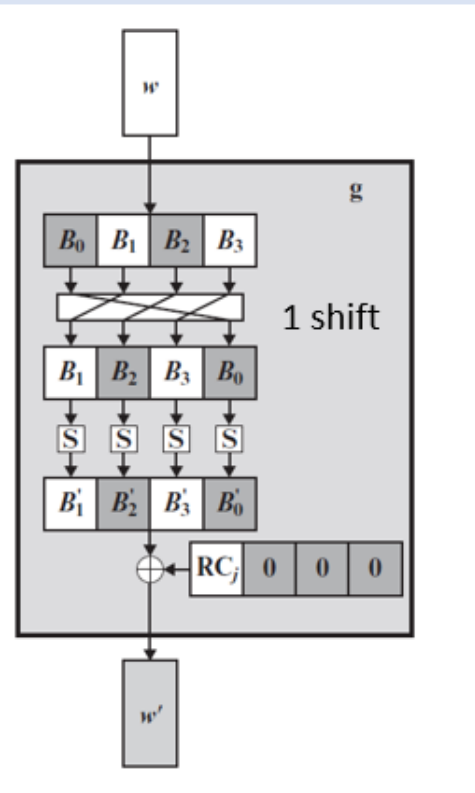
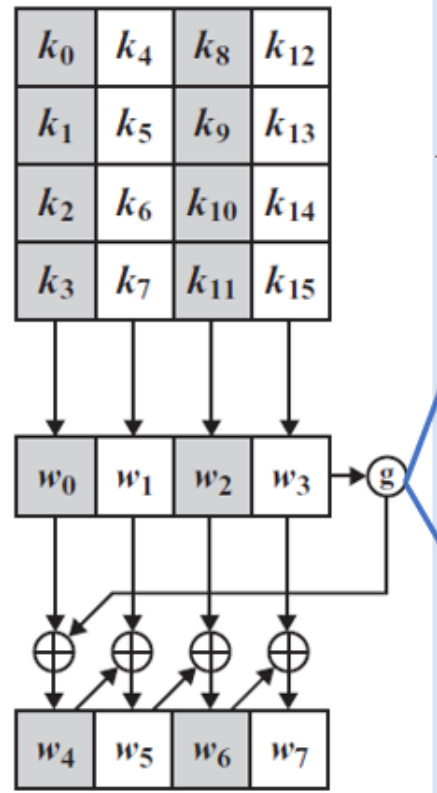


Table 7.4 *RCon constants*

Round	Constant (RCon)	Round	Constant (RCon)
1	(<u>01</u> 00 00 00) ₁₆	6	(<u>20</u> 00 00 00) ₁₆
2	(<u>02</u> 00 00 00) ₁₆	7	(<u>40</u> 00 00 00) ₁₆
3	(<u>04</u> 00 00 00) ₁₆	8	(<u>80</u> 00 00 00) ₁₆
4	(<u>08</u> 00 00 00) ₁₆	9	(<u>1B</u> 00 00 00) ₁₆
5	(<u>10</u> 00 00 00) ₁₆	10	(<u>36</u> 00 00 00) ₁₆

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

Key Words	Auxiliary Function
w0 = 0f 15 71 c9 w1 = 47 d9 e8 59 w2 = 0c b7 ad w3 = af 7f 67 98	RotWord(w3)= 7f 67 98 af = x1 SubWord(x1)= d2 85 46 79 = y1 Rcon(1)= 01 00 00 00 y1 \oplus Rcon(1)= d3 85 46 79 = z1
w4 = w0 \oplus z1 = dc 90 37 b0 w5 = w4 \oplus w1 = 9b 49 df e9 w6 = w5 \oplus w2 = 97 fe 72 3f w7 = w6 \oplus w3 = 38 81 15 a7	RotWord(w7)= 81 15 a7 38 = x2 SubWord(x2)= 0c 59 5c 07 = y2 Rcon(2)= 02 00 00 00 y2 \oplus Rcon(2)= 0e 59 5c 07 = z2
w8 = w4 \oplus z2 = d2 c9 6b b7 w9 = w8 \oplus w5 = 49 80 b4 5e w10 = w9 \oplus w6 = de 7e c6 61 w11 = w10 \oplus w7 = e6 ff d3 c6	RotWord(w11)= ff d3 c6 e6 = x3 SubWord(x3)= 16 66 b4 8e = y3 Rcon(3)= 04 00 00 00 y3 \oplus Rcon(3)= 12 66 b4 8e = z3
w12 = w8 \oplus z3 = c0 af df 39 w13 = w12 \oplus w9 = 89 2f 6b 67 w14 = w13 \oplus w10 = 57 51 ad 06 w15 = w14 \oplus w11 = b1 ae 7e c0	RotWord(w15)= ae 7e c0 b1 = x4 SubWord(x4)= e4 f3 ba c8 = y4 Rcon(4)= 08 00 00 00 y4 \oplus Rcon(4)= ec f3 ba c8 = 4
w16 = w12 \oplus z4 = 2c 5c 65 f1 w17 = w16 \oplus w13 = a5 73 0e 96 w18 = w17 \oplus w14 = f2 22 a3 90 w19 = w18 \oplus w15 = 43 8c dd 50	RotWord(w19)= 8c dd 50 43 = x5 SubWord(x5)= 64 c1 53 1a = y5 Rcon(5)= 10 00 00 00 y5 \oplus Rcon(5)= 74 c1 53 1a = z5

$w_{20} = w_{16} \oplus z_5 = 58\ 9d\ 36\ eb$ $w_{21} = w_{20} \oplus w_{17} = fd\ ee\ 38\ 7d$ $w_{22} = w_{21} \oplus w_{18} = 0f\ cc\ 9b\ ed$ $w_{23} = w_{22} \oplus w_{19} = 4c\ 40\ 46\ bd$	$RotWord(w_{23}) = 40\ 46\ bd\ 4c = x_6$ $SubWord(x_5) = 09\ 5a\ 7a\ 29 = y_6$ $Rcon(6) = 20\ 00\ 00\ 00$ $y_6 \oplus Rcon(6) = 29\ 5a\ 7a\ 29 = z_6$
$w_{24} = w_{20} \oplus z_6 = 71\ c7\ 4c\ c2$ $w_{25} = w_{24} \oplus w_{21} = 8c\ 29\ 74\ bf$ $w_{26} = w_{25} \oplus w_{22} = 83\ e5\ ef\ 52$ $w_{27} = w_{26} \oplus w_{23} = cf\ a5\ a9\ ef$	$RotWord(w_{27}) = a5\ a9\ ef\ cf = x_7$ $SubWord(x_6) = 06\ d3\ df\ 8a = y_7$ $Rcon(7) = 40\ 00\ 00\ 00$ $y_7 \oplus Rcon(7) = 46\ d3\ df\ 8a = z_7$
$w_{28} = w_{24} \oplus z_7 = 37\ 14\ 93\ 48$ $w_{29} = w_{28} \oplus w_{25} = bb\ 3d\ e7\ f7$ $w_{30} = w_{29} \oplus w_{26} = 38\ d8\ 08\ a5$ $w_{31} = w_{30} \oplus w_{27} = f7\ 7d\ a1\ 4a$	$RotWord(w_{31}) = 7d\ a1\ 4a\ f7 = x_8$ $SubWord(x_7) = ff\ 32\ d6\ 68 = y_8$ $Rcon(8) = 80\ 00\ 00\ 00$ $y_8 \oplus Rcon(8) = 7f\ 32\ d6\ 68 = z_8$
$w_{32} = w_{28} \oplus z_8 = 48\ 26\ 45\ 20$ $w_{33} = w_{32} \oplus w_{29} = f3\ 1b\ a2\ d7$ $w_{34} = w_{33} \oplus w_{30} = cb\ c3\ aa\ 72$ $w_{35} = w_{34} \oplus w_{32} = 3c\ be\ 0b\ 38$	$RotWord(w_{35}) = be\ 0b\ 38\ 3c = x_9$ $SubWord(x_8) = ae\ 2b\ 07\ eb = y_9$ $Rcon(9) = 1b\ 00\ 00\ 00$ $y_9 \oplus Rcon(9) = b5\ 2b\ 07\ eb = z_9$
$w_{36} = w_{32} \oplus z_9 = fd\ 0d\ 42\ cb$ $w_{37} = w_{36} \oplus w_{33} = 0e\ 16\ e0\ 1c$ $w_{38} = w_{37} \oplus w_{34} = c5\ d5\ 4a\ 6e$ $w_{39} = w_{38} \oplus w_{35} = f9\ 6b\ 41\ 56$	$RotWord(w_{39}) = 6b\ 41\ 56\ f9 = x_{10}$ $SubWord(x_9) = 7f\ 83\ b1\ 99 = y_{10}$ $Rcon(10) = 36\ 00\ 00\ 00$ $y_{10} \oplus Rcon(10) = 49\ 83\ b1\ 99 = z_{10}$
$w_{40} = w_{36} \oplus z_{10} = b4\ 8e\ f3\ 52$ $w_{41} = w_{40} \oplus w_{37} = ba\ 98\ 13\ 4e$ $w_{42} = w_{41} \oplus w_{38} = 7f\ 4d\ 59\ 20$ $w_{43} = w_{42} \oplus w_{39} = 86\ 26\ 18\ 76$	

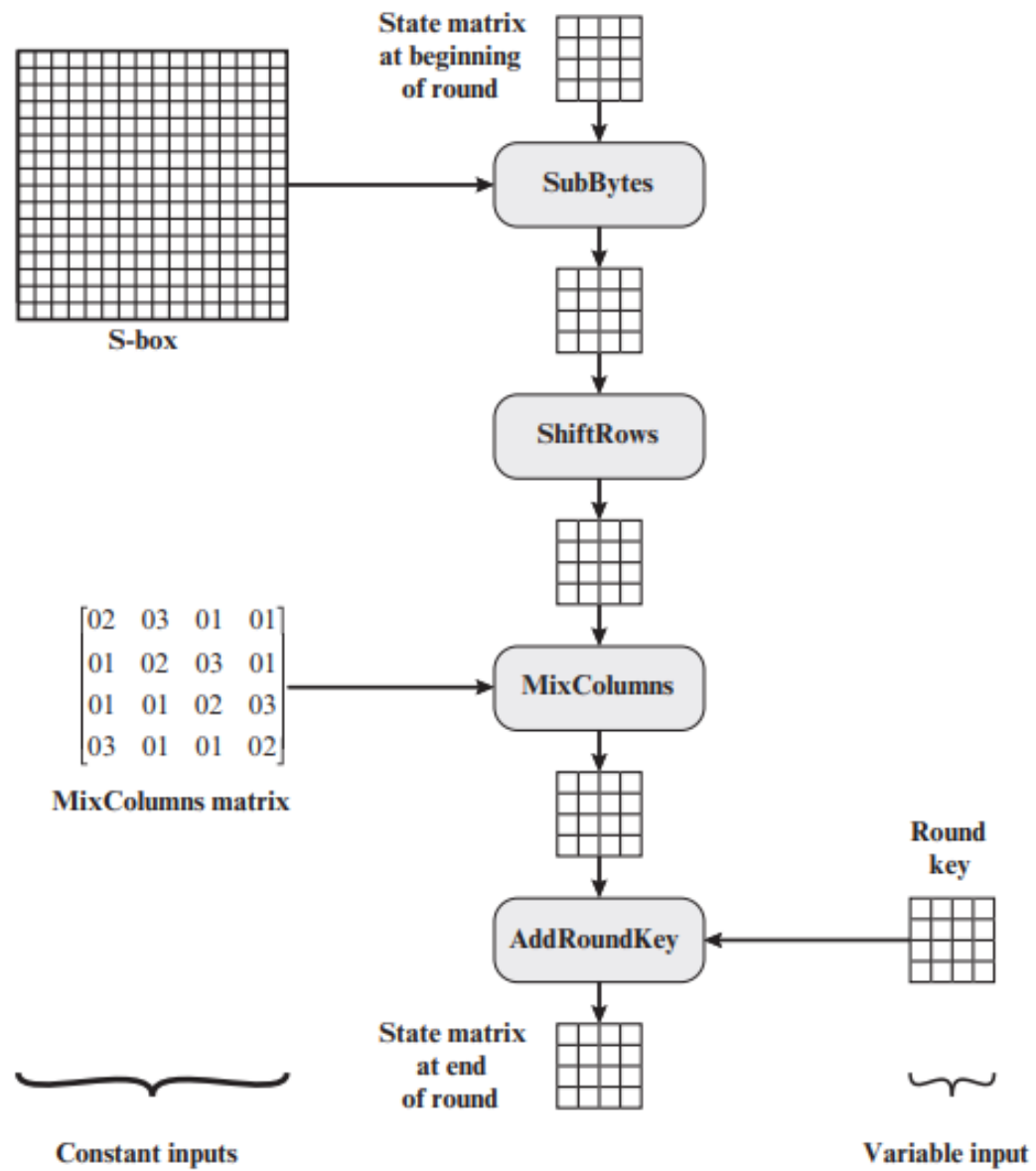


Figure 6.8 Inputs for Single AES Round

AES Example - Input (128 bit key and message)

- Key in English: **Thats my Kung Fu** (16 ASCII characters, 1 byte each)

Translation into Hex:

T	h	a	t	s		m	y		K	u	n	g		F	u
54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

Key in Hex (128 bits): **54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75**

- **The first Roundkey:**

AES Example - Input (128 bit key and message)

• The first Roundkey:

- Key in Hex (128 bits): 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
- $w[0] = (54, 68, 61, 74)$, $w[1] = (73, 20, 6D, 79)$, $w[2] = (20, 4B, 75, 6E)$, $w[3] = (67, 20, 46, 75)$
- $g(w[3])$:
 - circular byte left shift of $w[3]$: $(20, 46, 75, 67)$
 - Byte Substitution (S-Box): $(B7, 5A, 9D, 85)$
 - Adding round constant $(01, 00, 00, 00)$ gives: $g(w[3]) = (B6, 5A, 9D, 85)$
- $w[4] = w[0] \oplus g(w[3]) = (E2, 32, FC, F1)$:

$$\begin{array}{r}
 10110111 \\
 00000001 \\
 \hline
 10110110 \\
 \text{B} \quad 6
 \end{array}
 \quad \times 01$$

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	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

- $w[4] = w[0] \oplus g(w[3]) = (E2, 32, FC, F1)$:

0101 0100	0110 1000	0110 0001	0111 0100
1011 0110	0101 1010	1001 1101	1000 0101
1110 0010	0011 0010	1111 1100	1111 0001
E2	32	FC	F1

- $w[5] = w[4] \oplus w[1] = (91, 12, 91, 88)$, $w[6] = w[5] \oplus w[2] = (B1, 59, E4, E6)$,
 $w[7] = w[6] \oplus w[3] = (D6, 79, A2, 93)$
- first roundkey: E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

- Round 0: 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
- Round 1: E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93
- Round 2: 56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA

Plaintext in English: **Two One Nine Two** (16 ASCII characters, 1 byte each)

Translation into Hex:

T	w	o		O	n	e		N	i	n	e		T	w	o
54	77	6F	20	4F	6E	65	20	4E	69	6E	65	20	54	77	6F

AES Example - Add Roundkey, Round 0

- State Matrix and Roundkey No.0 Matrix:

$$\begin{pmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{pmatrix} \quad \begin{pmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{pmatrix}$$

- XOR the corresponding entries, e.g., $69 \oplus 4B = 22$

$$\begin{array}{r} 0110 \ 1001 \\ 0100 \ 1011 \\ \hline 0010 \ 0010 \end{array}$$

- the new State Matrix is

$$\begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

AES Example - Round 1, Substitution Bytes

- current State Matrix is

$$\begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

- substitute each entry (byte) of current state matrix by corresponding entry in AES S-Box
- for instance: byte 6E is substituted by entry of S-Box in row 6 and column E, i.e., by 9F
- this leads to new State Matrix

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

- this non-linear layer is for resistance to differential and linear cryptanalysis attacks

AES Example - Round 1, Shift Row

- the current State Matrix is

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

- four rows are shifted cyclically to the left by offsets of 0,1,2, and 3
- the new State Matrix is

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix}$$

- this linear mixing step causes diffusion of the bits over multiple rounds

AES Example - Round 1, Mix Column

- Mix Column multiplies fixed matrix against current State Matrix:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix} = \begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix}$$

- entry BA is result of $(02 \bullet 63) \oplus (03 \bullet 2F) \oplus (01 \bullet AF) \oplus (01 \bullet A2)$:
 - $02 \bullet 63 = 00000010 \bullet 01100011 = 11000110$
 - $03 \bullet 2F = (02 \bullet 2F) \oplus 2F = (00000010 \bullet 00101111) \oplus 00101111 = 01110001$
 - $01 \bullet AF = AF = 10101111$ and $01 \bullet A2 = A2 = 10100010$
 - hence

$$\begin{array}{r} 11000110 \\ 01110001 \\ 10101111 \\ 10100010 \\ \hline 10111010 \end{array}$$

AES Example - Add Roundkey, Round 1

- State Matrix and Roundkey No.1 Matrix:

$$\begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix} \quad \begin{pmatrix} E2 & 91 & B1 & D6 \\ 32 & 12 & 59 & 79 \\ FC & 91 & E4 & A2 \\ F1 & 88 & E6 & 93 \end{pmatrix}$$

- XOR yields new State Matrix

$$\begin{pmatrix} 58 & 15 & 59 & CD \\ 47 & B6 & D4 & 39 \\ 08 & 1C & E2 & DF \\ 8B & BA & E8 & CE \end{pmatrix}$$

- AES output after Round 1: 58 47 08 8B 15 B6 1C BA 59 D4 E2 E8 CD 39 DF CE

- Continue with next 9 rounds: (in 10th round no mixcolumn operation)

Additional Materials

So the 2^3 polynomials of $GF(2^3)$ can therefore be represented by the bit strings:

0	\Rightarrow	000
1	\Rightarrow	001
x	\Rightarrow	010
x^2	\Rightarrow	100
$x + 1$	\Rightarrow	011
$x^2 + 1$	\Rightarrow	101
$x^2 + x$	\Rightarrow	110
$x^2 + x + 1$	\Rightarrow	111

- Given any n at all, exactly the same approach can be used to come up with 2^n bit patterns, each pattern consisting of n bits,

<i>Number</i>	<i>Binary</i>	<i>GF(2⁸) Polynomial</i>	<i>Simplified</i>
0	0	0	0
1	1	1	1
2	10	1x+0	x
3	11	1x+1	x+1
4	100	1x ² +0x+0	x ²
5	101	1x ² +0x+1	x ² +1
8	1000	1x ³ +0x ² +0x+0	x ³
16	10000	1x ⁴ +0x ³ +0x ² +0x+0	x ⁴
21	10101	1x ⁴ +0x ³ +1x ² +0x+1	x ⁴ +x ² +1