



# Computer Security

## Lecture 5



# Simplified Advanced Encryption Standard

**Dr. Mohamed Loey**

Lecturer, Faculty of Computers and Information  
Benha University  
Egypt

# Table of Contents

**Simplified Advanced Encryption Standard**

**S-AES Encryption and Decryption**

**S-AES Key Generation**

**S-AES Encryption**

**S-AES Decryption**

# Table of Contents

**Simplified Advanced Encryption Standard**

**S-AES Encryption and Decryption**

**S-AES Key Generation**

**S-AES Encryption**

**S-AES Decryption**

# Simplified Advanced Encryption Standard

- ❑ Simplified AES (S-AES) was developed by Professor Edward Schaefer of Santa Clara University in 2003
- ❑ its purpose is educational, since its key and block size are very small 16bits
- ❑ it is possible for students to encrypt or decrypt a block doing all operations by hand
- ❑ it easier for students to understand the structure AES

# Table of Contents

**Simplified Advanced Encryption Standard**

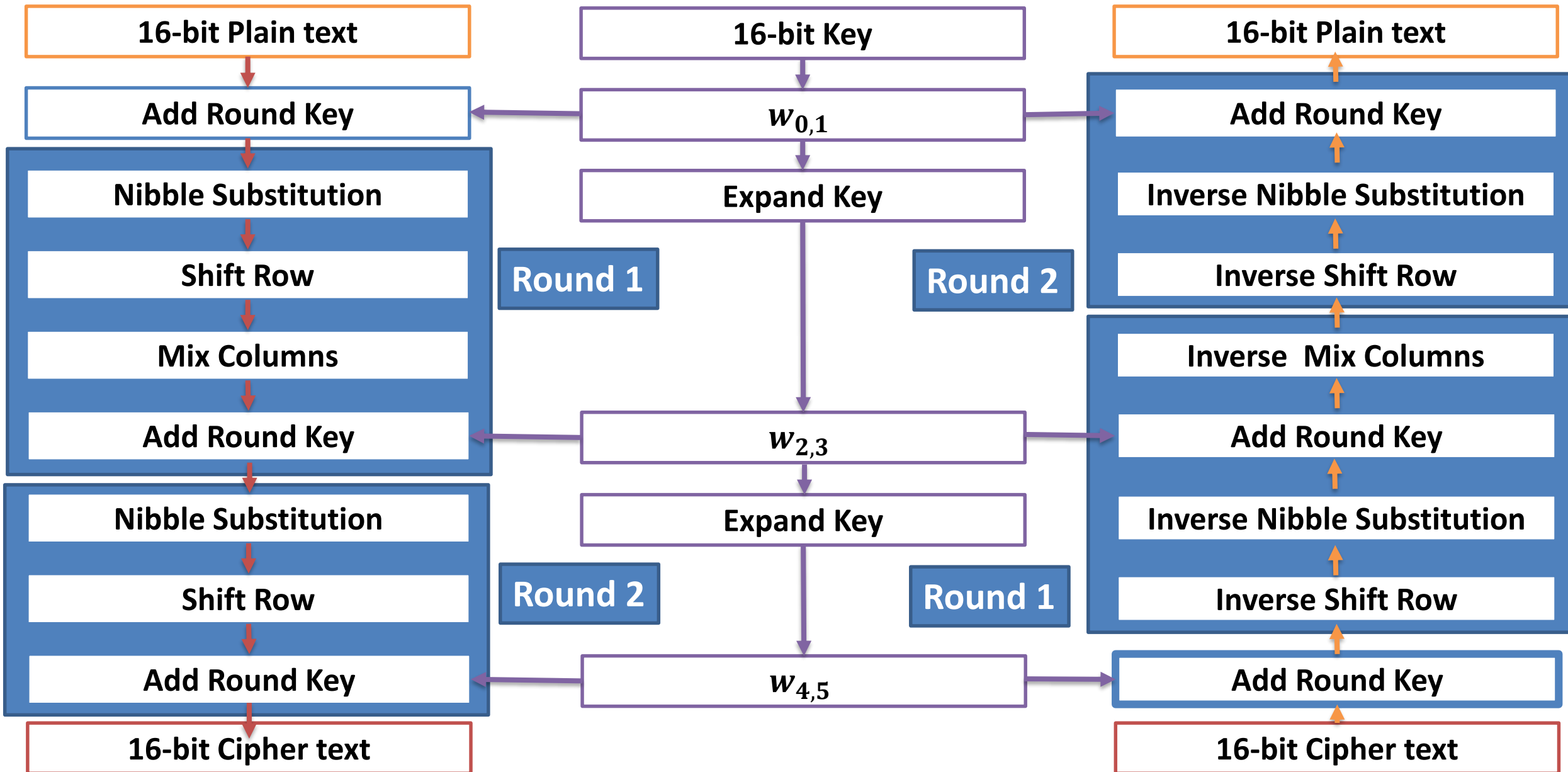
**S-AES Encryption and Decryption**

**S-AES Key Generation**

**S-AES Encryption**

**S-AES Decryption**

# S-AES Encryption and Decryption



# S-AES Encryption Example

□ 16-bit Plaintext,  $P = D7\ 28$

$= 1101\ 0111\ 0010\ 1000$

□ 16-bit Key,  $K = 4A\ F5$

$= 0100\ 1010\ 1111\ 0101$

# Table of Contents

**Simplified Advanced Encryption Standard**

**S-AES Encryption and Decryption**

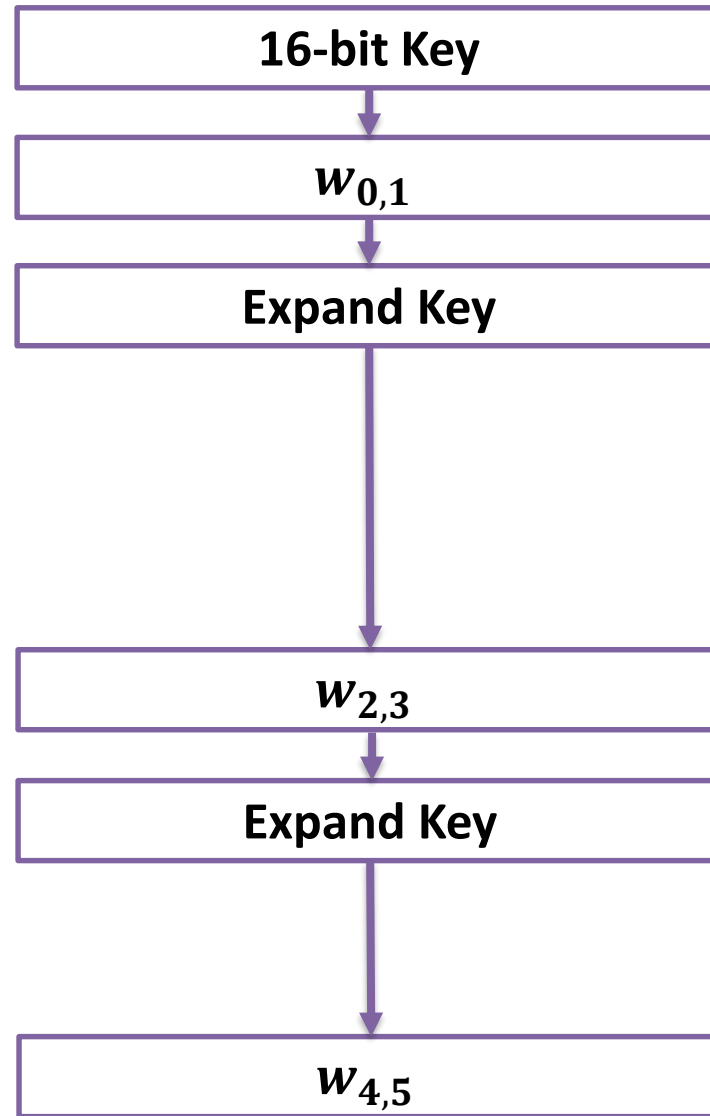
**S-AES Key Generation**

**S-AES Encryption**

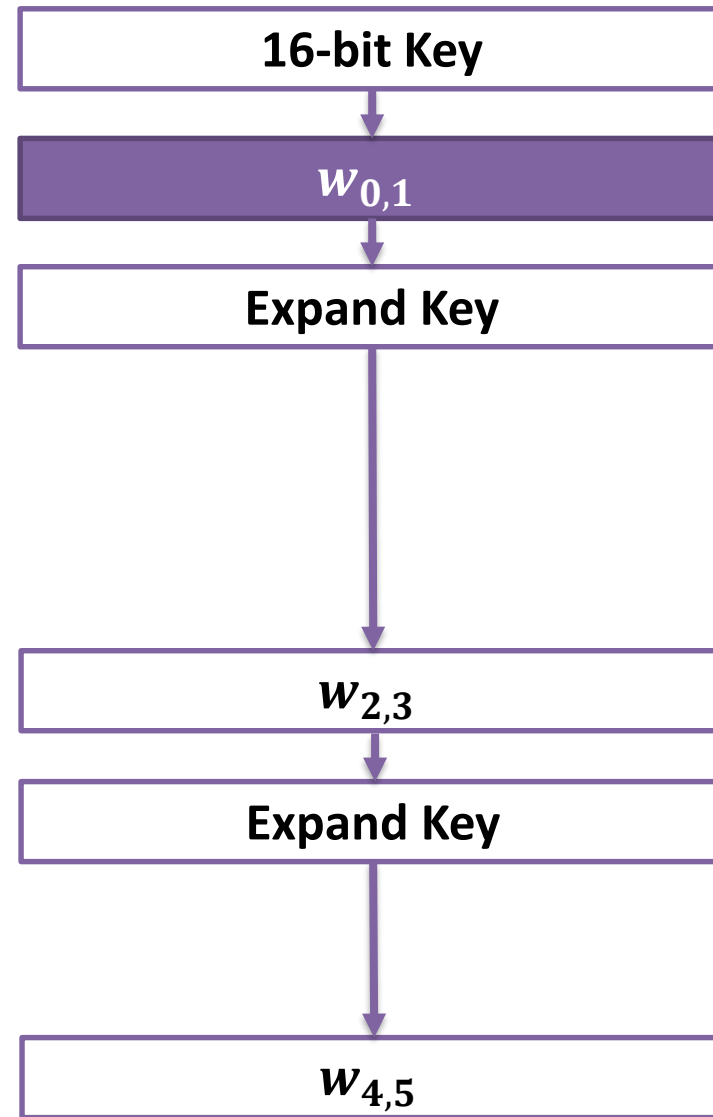
**S-AES Decryption**



# S-AES Key Generation



# S-AES Key Generation



# S-AES Key Generation

□  $K = 4A\ F5$

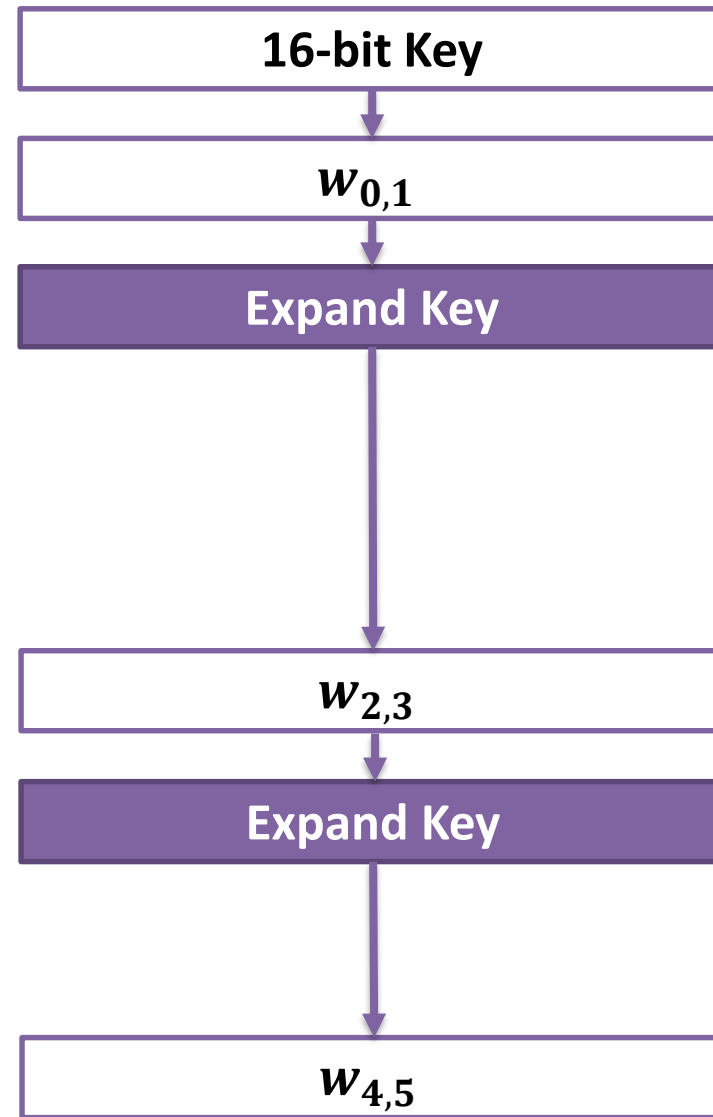
$= 0100\ 1010\ 1111\ 0101$

□ The input key,  $K$ , is split into 2 words,  $w_0$  and  $w_1$ :

□  $w_0 = 0100\ 1010$

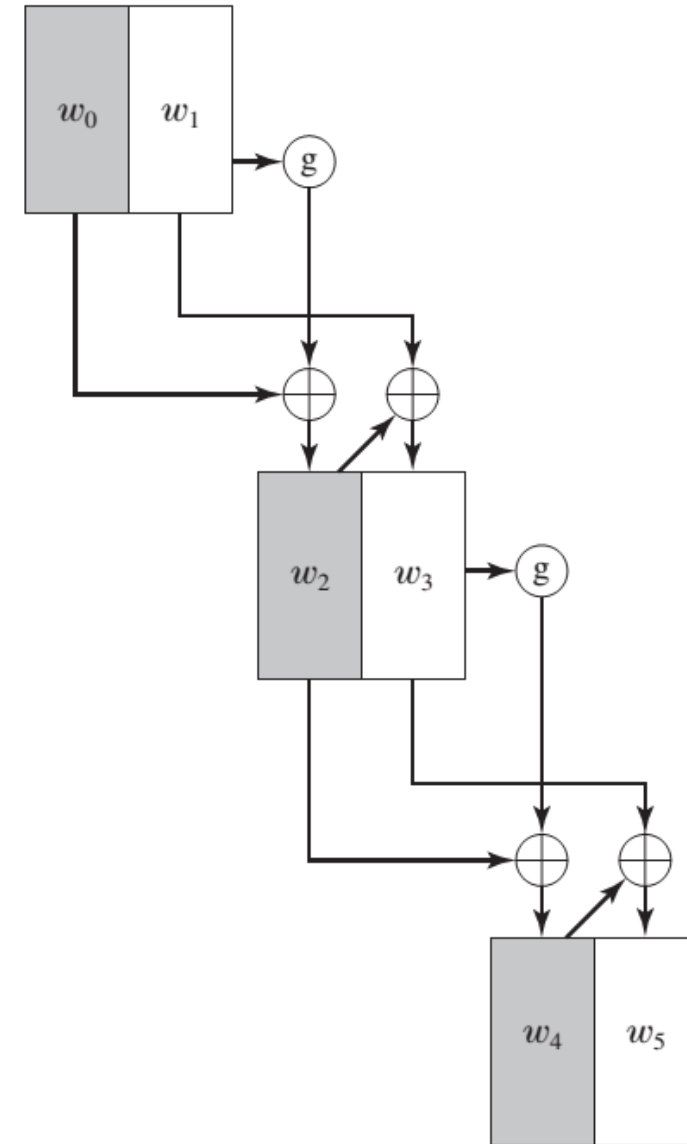
□  $w_1 = 1111\ 0101$

# S-AES Key Generation



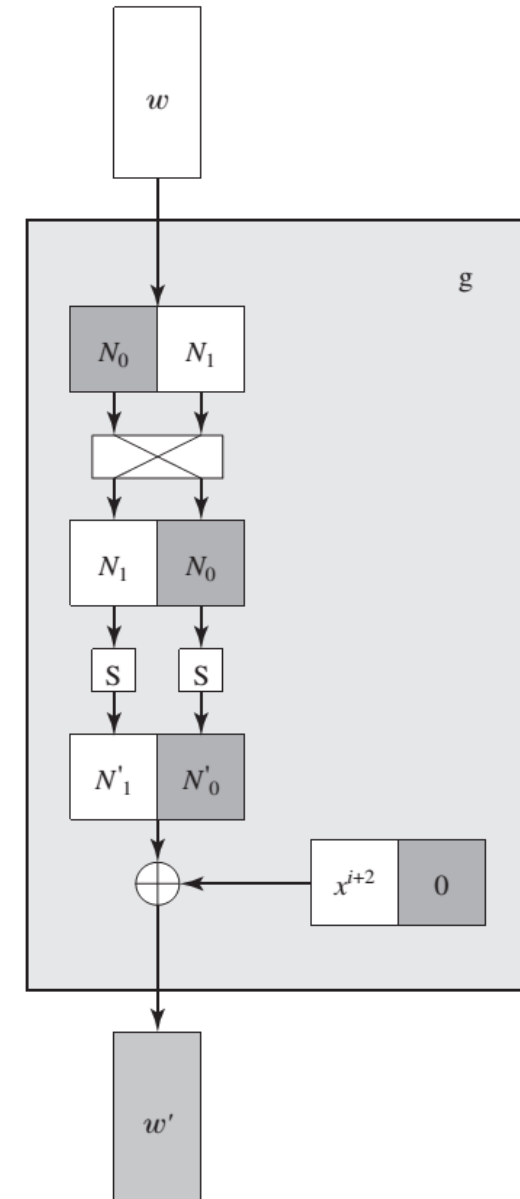
# S-AES Key Generation

## □ S-AES Key Expansion

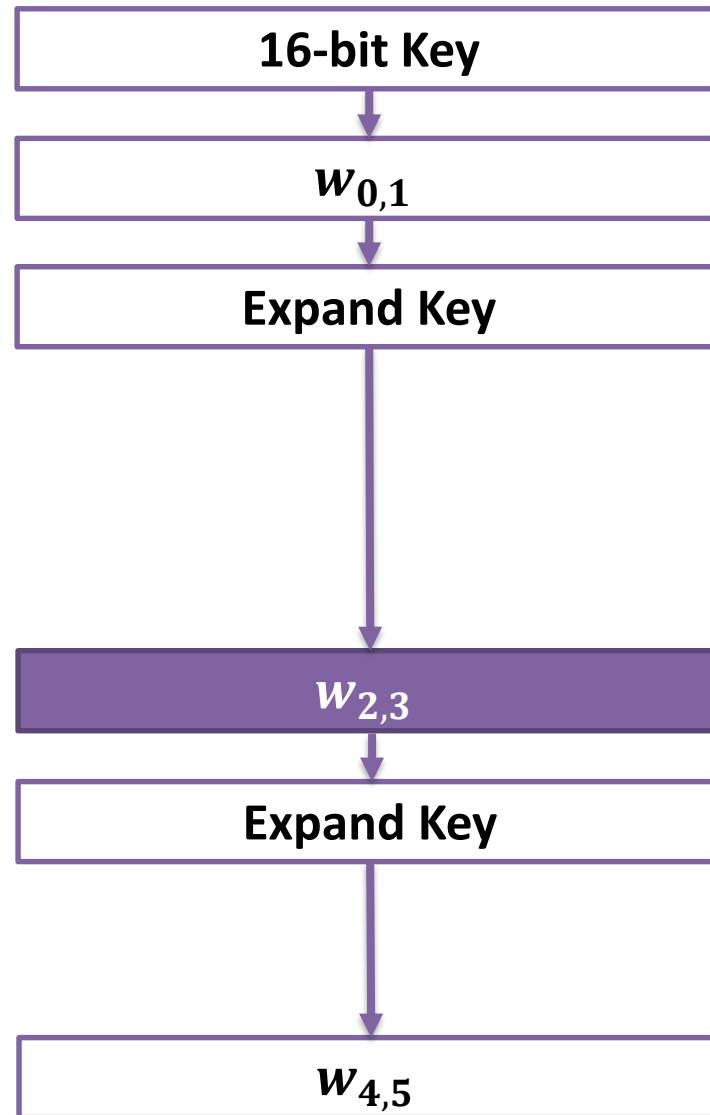


# S-AES Key Generation

## □ Function $g$



# S-AES Key Generation



# S-AES Key Generation

- ❑  $w_0 = 0100\ 1010$ ,  $w_1 = 1111\ 0101$
- ❑  $w_2 = w_0 \oplus \text{Rcon}(1) \oplus \text{SubNib}(\text{RotNib}(w_1))$
- ❑ **RotNib()** is “rotate the nibbles”, which is equivalent to swapping the nibbles, **Rcon** is a round constant
- ❑ **SubNib()** is “apply S-Box substitution on nibbles using encryption S-Box”
- ❑  $\text{RotNib}(w_1) = 0101\ 1111$
- ❑  $\text{SubNib}(0101\ 1111) = 0001\ 0111$
- ❑  $\text{Rcon}(1) = 10000000$

S-Box		<i>j</i>			
		00	01	10	11
<i>i</i>	00	9	4	A	B
	01	D	1	8	5
	10	6	2	0	3
	11	C	E	F	7



# S-AES Key Generation

$$\square w_0 = 0100\ 1010, w_1 = 1111\ 0101$$

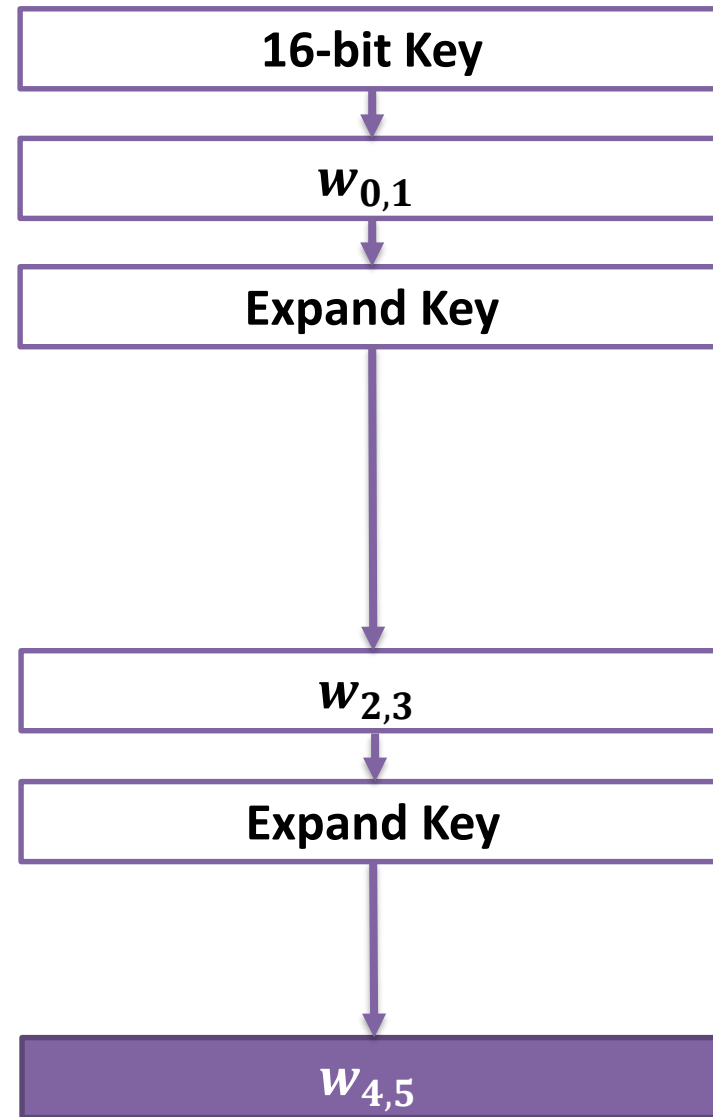
$$\begin{aligned}\square w_2 &= w_0 \oplus \text{Rcon}(1) \oplus \text{SubNib}(\text{RotNib}(w_1)) \\ &= 0100\ 1010 \oplus 1000\ 0000 \oplus 0001\ 0111 \\ &= 0100\ 1010 \oplus 1001\ 0111 = 1101\ 1101\end{aligned}$$

$$\square w_2 = 1101\ 1101$$

$$\square w_3 = w_2 \oplus w_1 = 1101\ 1101 \oplus 1111\ 0101 = 0010\ 1000$$

$$\square w_3 = 0010\ 1000$$

# S-AES Key Generation



# S-AES Key Generation

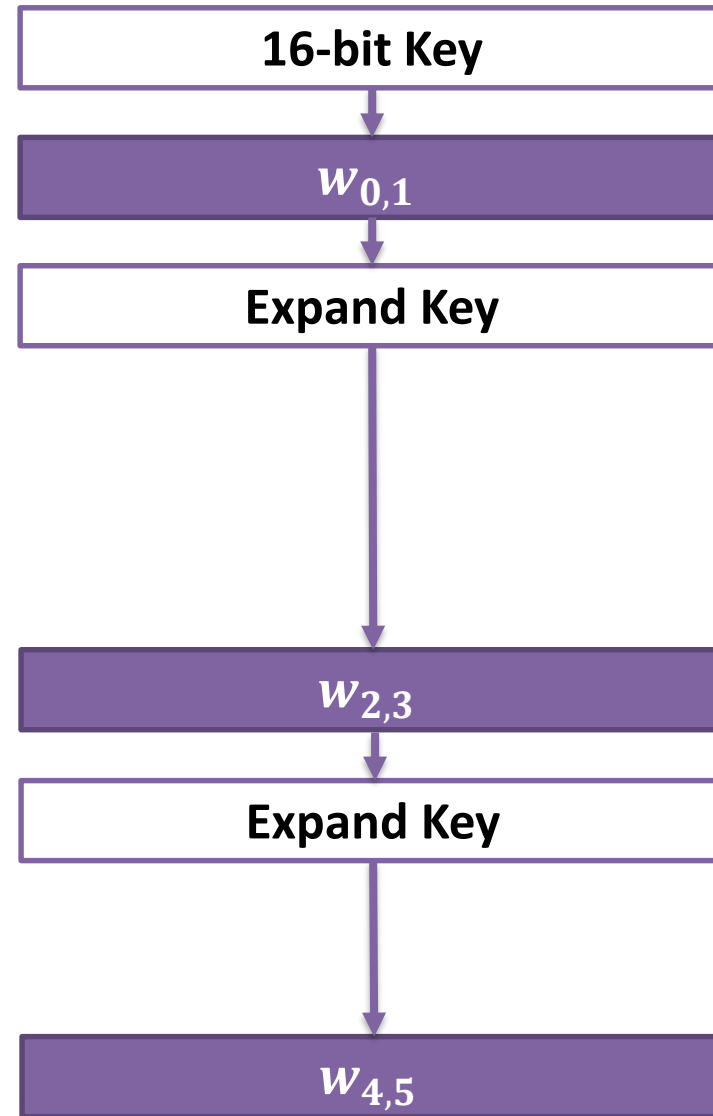
$$\square w_2 = 1101\ 1101, w_3 = 0010\ 1000$$

$$\begin{aligned}\square w_4 &= w_2 \oplus \text{Rcon}(2) \oplus \text{SubNib}(\text{RotNib}(w_3)) \\ &= 1101\ 1101 \oplus 0011\ 0000 \oplus \text{SubNib}(1000\ 0010) \\ &= 1101\ 1101 \oplus 0011\ 0000 \oplus 0110\ 1010 \\ &= 1101\ 1101 \oplus 0101\ 1010 \\ &= 1000\ 0111\end{aligned}$$

$$\begin{aligned}\square w_5 &= w_4 \oplus w_3 \\ &= 1000\ 0111 \oplus 0010\ 1000 \\ &= 1010\ 1111\end{aligned}$$

S-Box		<i>j</i>			
		00	01	10	11
<i>i</i>	00	9	4	A	B
	01	D	1	8	5
	10	6	2	0	3
	11	C	E	F	7

# S-AES Key Generation



# S-AES Key Generation

□ Key

□ Key0 =  $w_0w_1$

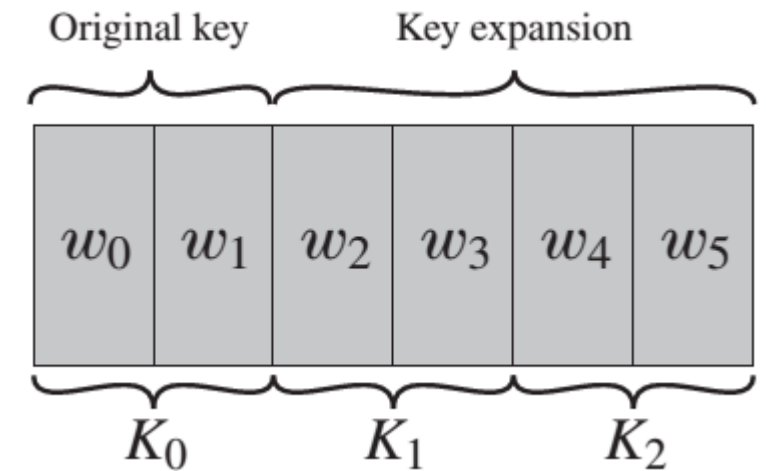
= 0100 1010 1111 0101

□ Key1 =  $w_2w_3$

= 1101 1101 0010 1000

□ Key2 =  $w_4w_5$

= 1000 0111 1010 1111



# Table of Contents

**Simplified Advanced Encryption Standard**

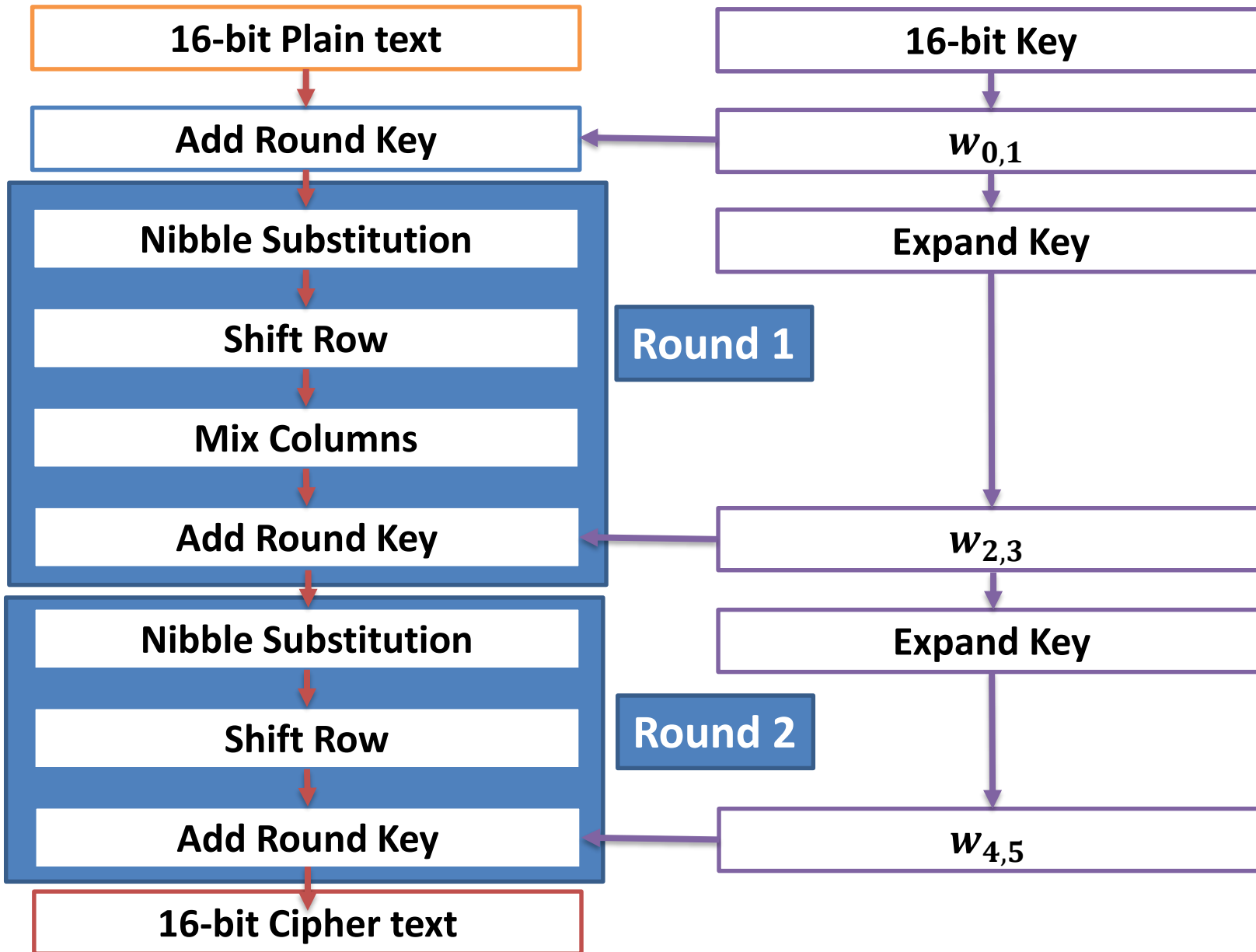
**S-AES Encryption and Decryption**

**S-AES Key Generation**

**S-AES Encryption**

**S-AES Decryption**

# S-AES Encryption



# S-AES Encryption

❑ Assume:  $P = 1101\ 0111\ 0010\ 1000$

❑  $\text{Key0} = w_0w_1$

$= 0100\ 1010\ 1111\ 0101$

❑  $\text{Key1} = w_2w_3$

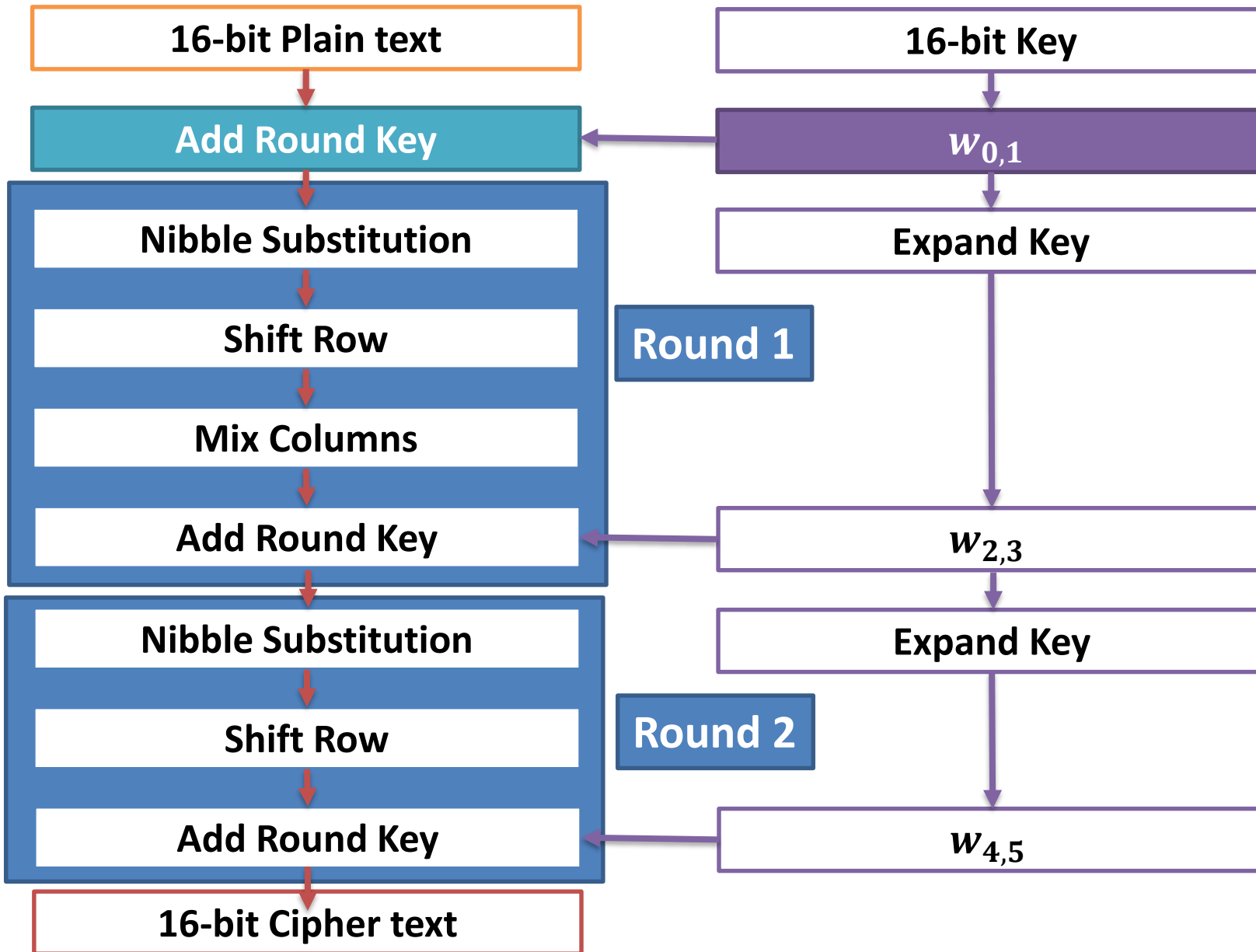
$= 1101\ 1101\ 0010\ 1000$

❑  $\text{Key2} = w_4w_5$

$= 1000\ 0111\ 1010\ 1111$



# S-AES Encryption



# S-AES Encryption

❑ Round 0

❑  $P = 1101\ 0111\ 0010\ 1000$

❑  $Key0 = 0100\ 1010\ 1111\ 0101$

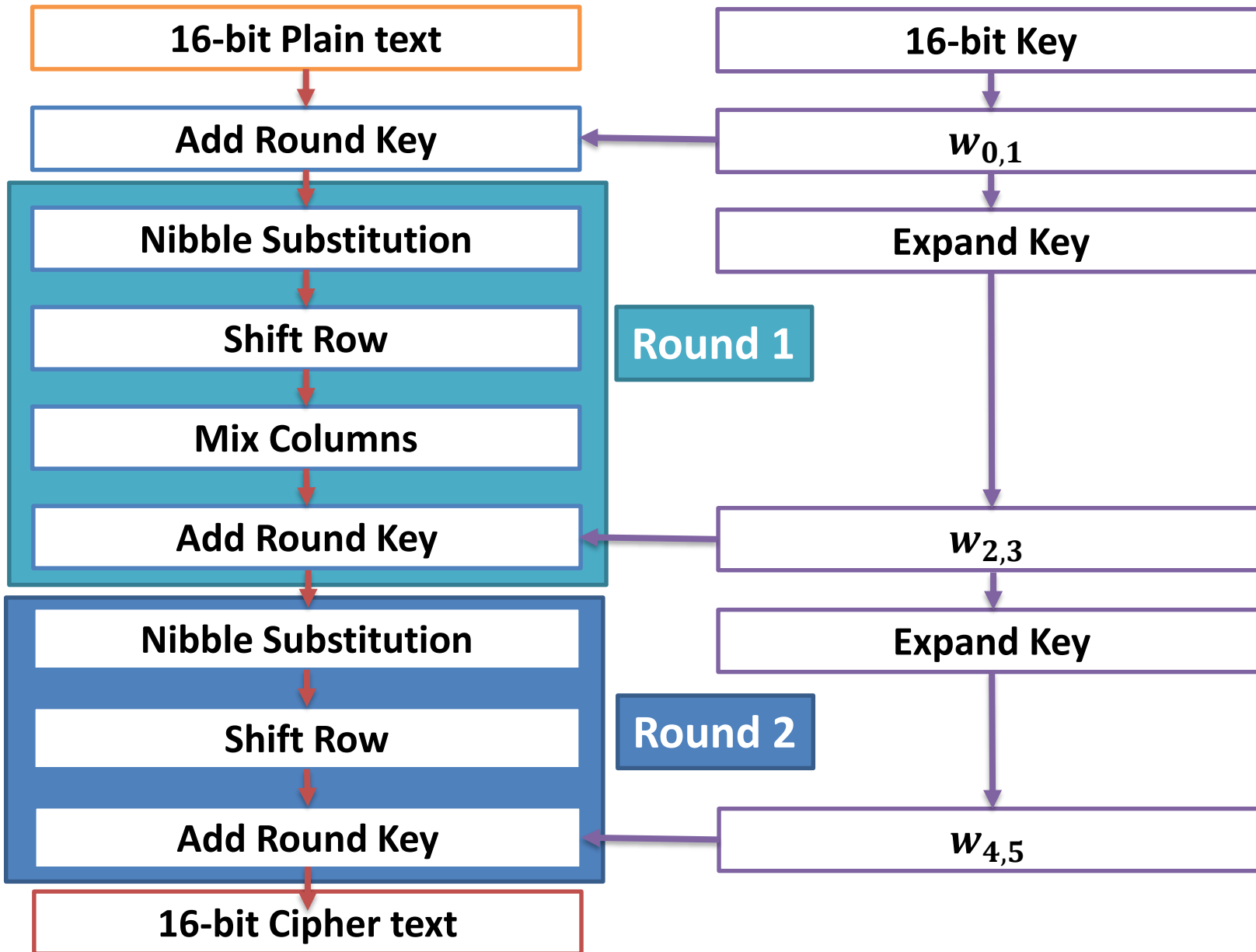
❑  $R0 = P \oplus Key0$

$= 1101\ 0111\ 0010\ 1000 \oplus$

$0100\ 1010\ 1111\ 0101$

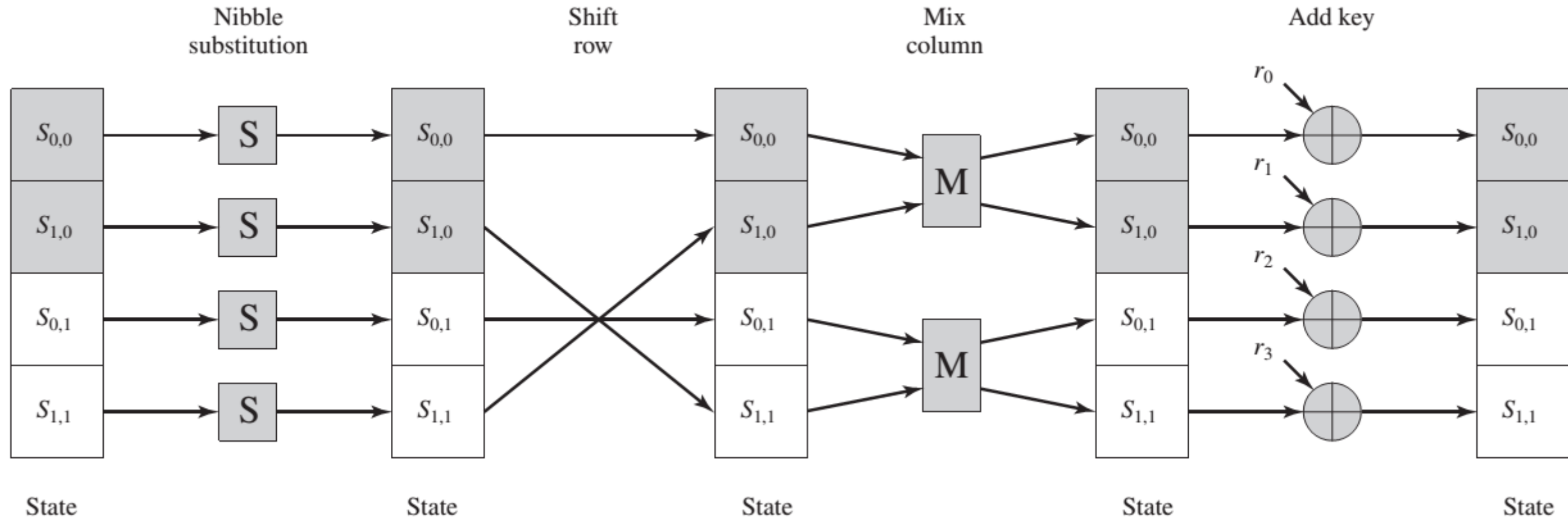
$= 1001\ 1101\ 1101\ 1101$

# S-AES Encryption



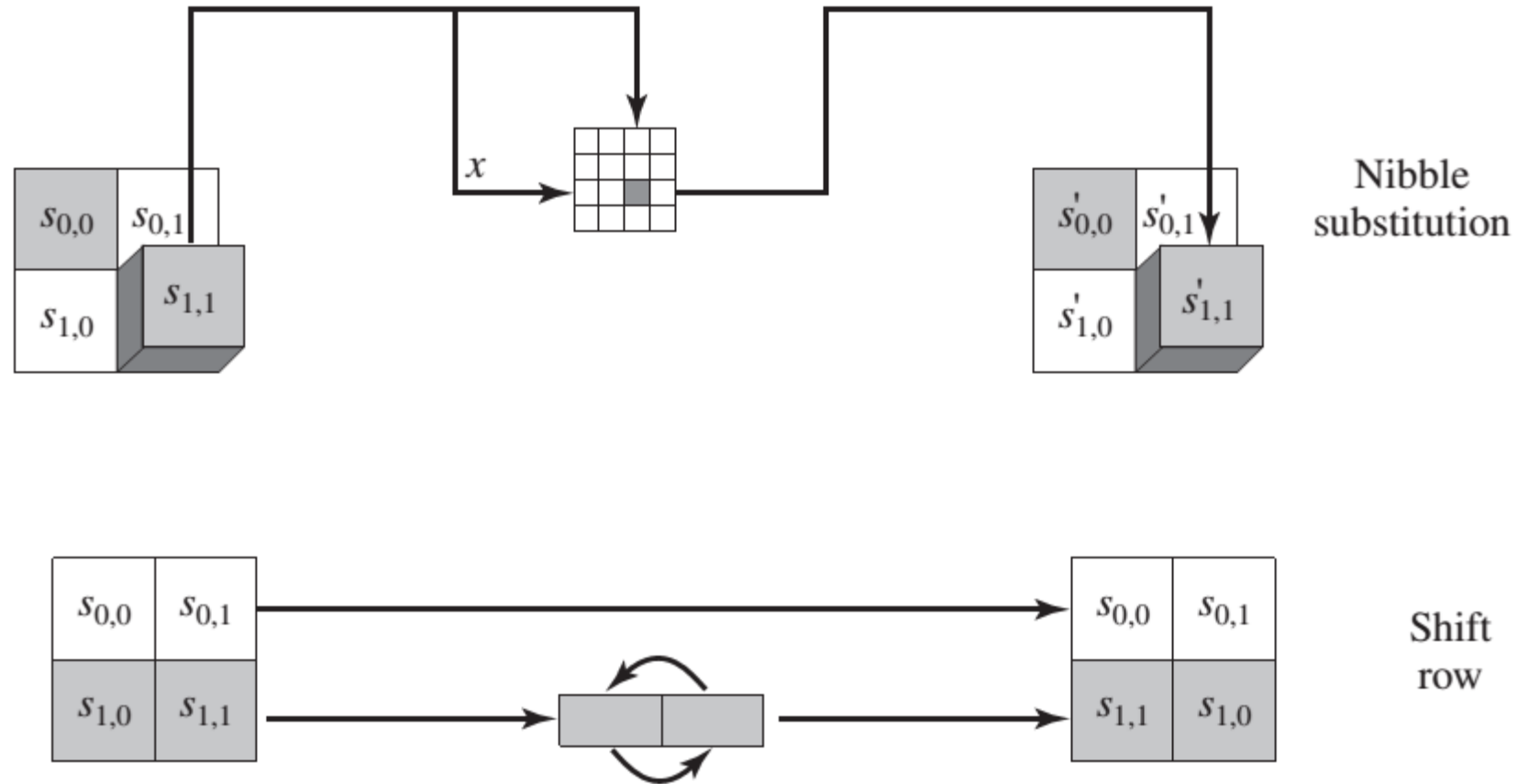
# S-AES Encryption

## □ S-AES Encryption Round

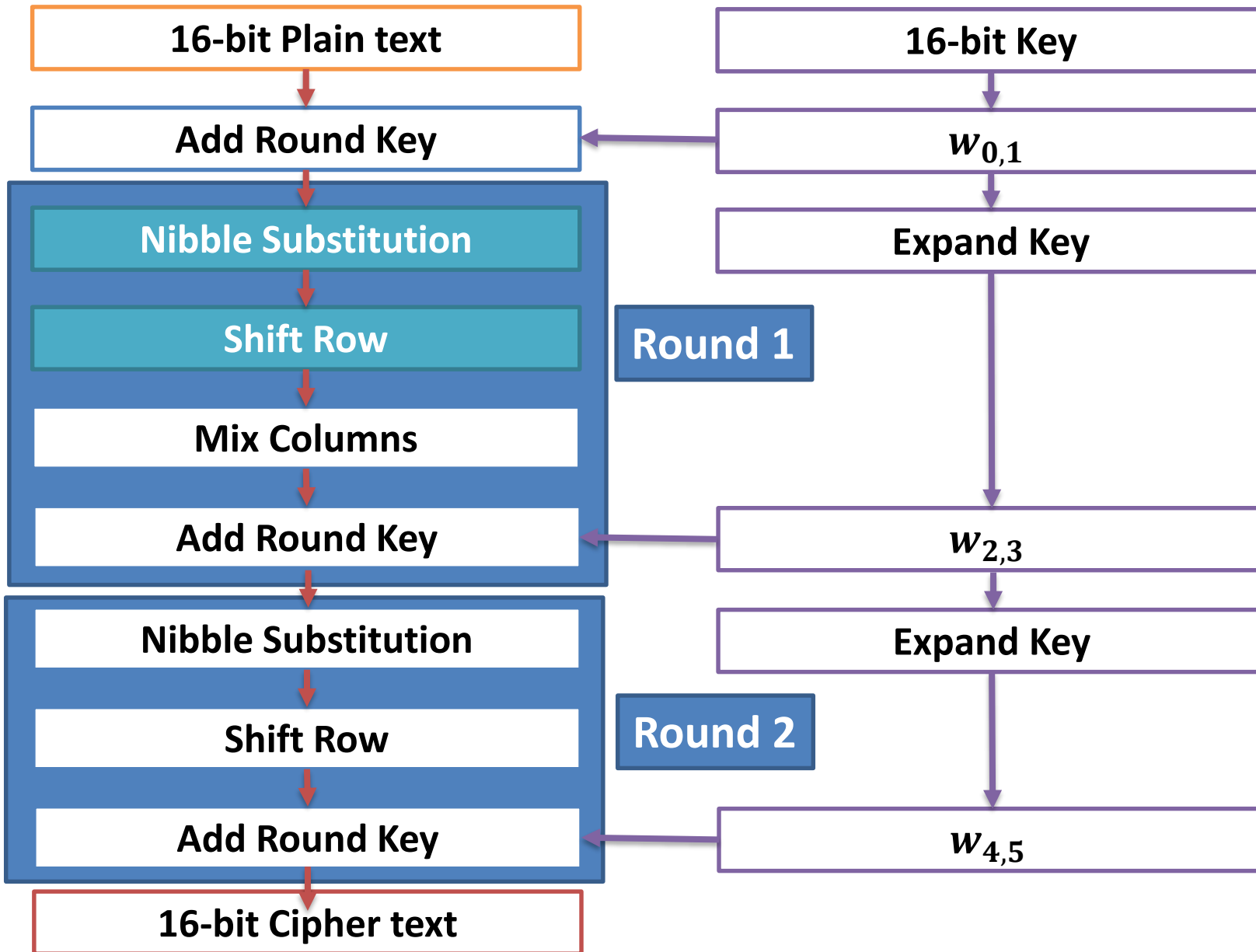


# S-AES Encryption

## □ S-AES Transformation (Substitution and Shift row)



# S-AES Encryption



# S-AES Encryption

## ❑ Round 1

### 1) Nibble Substitution :

❑  $\text{SubNib}(1001\ 1101\ 1101\ 1101) = 0010\ 1110\ 1110\ 1110$

### 2) Shift Row:

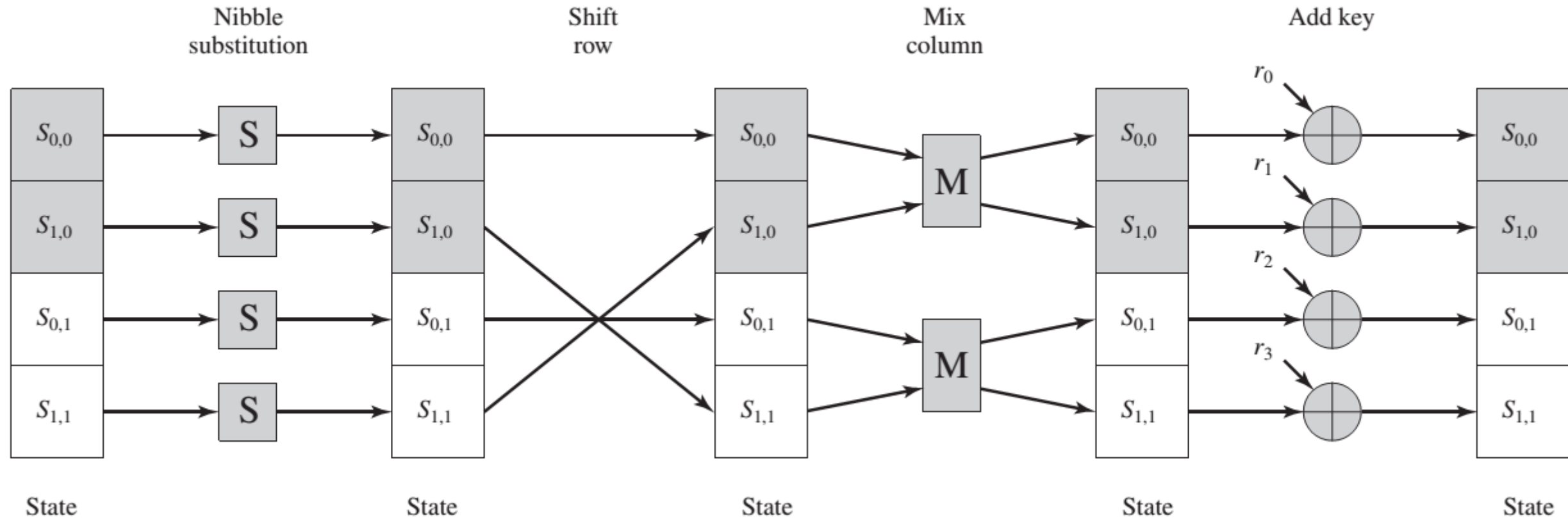
❑ Swap 2nd nibble and 4th nibble

❑  $\text{ShRow}(0010\ 1110\ 1110\ 1110)$   
 $= 0010\ 1110\ 1110\ 1110$

S-Box		<i>j</i>			
		00	01	10	11
<i>i</i>	00	9	4	A	B
	01	D	1	8	5
	10	6	2	0	3
	11	C	E	F	7

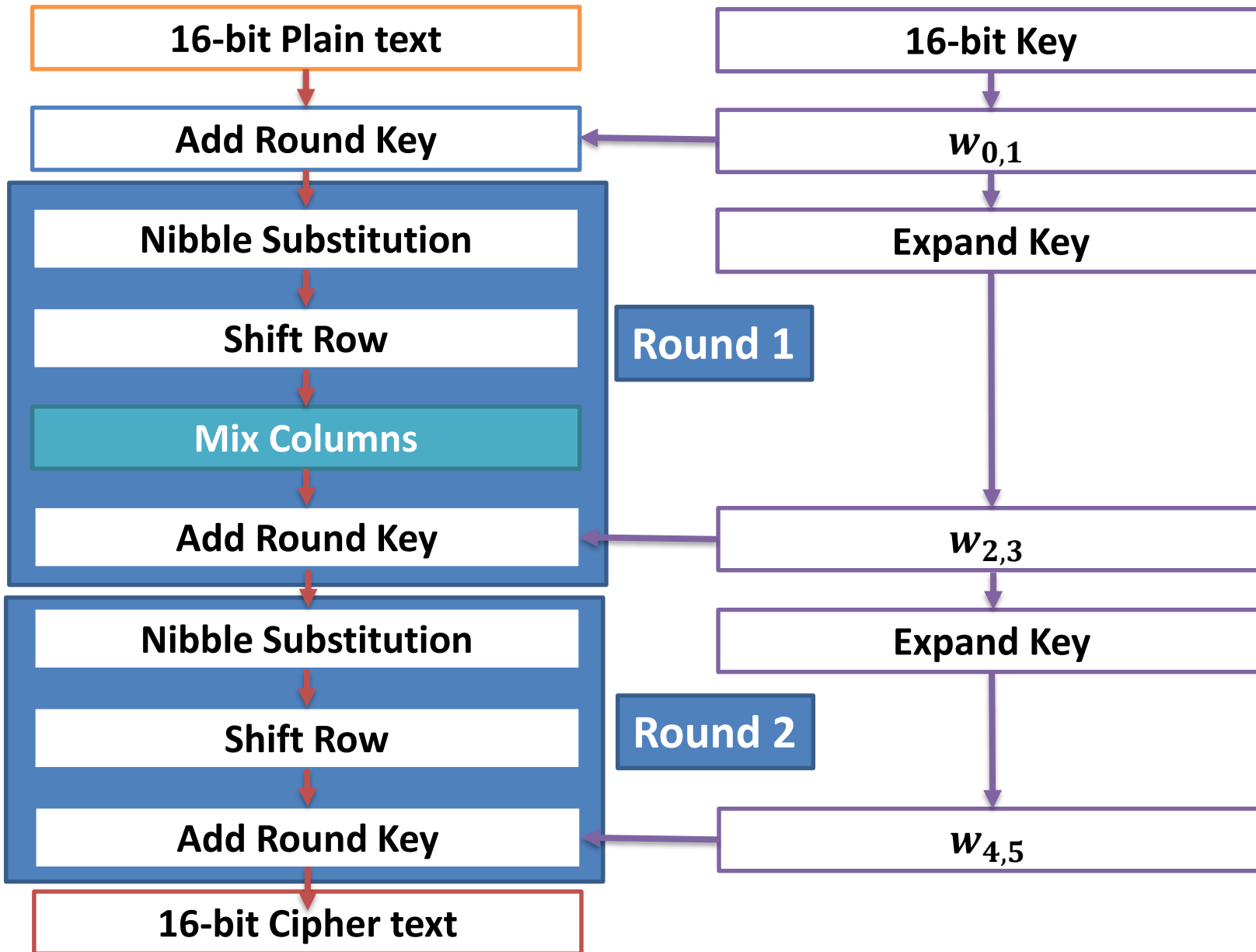
# Key Generation

## ❑ S-AES Encryption Round



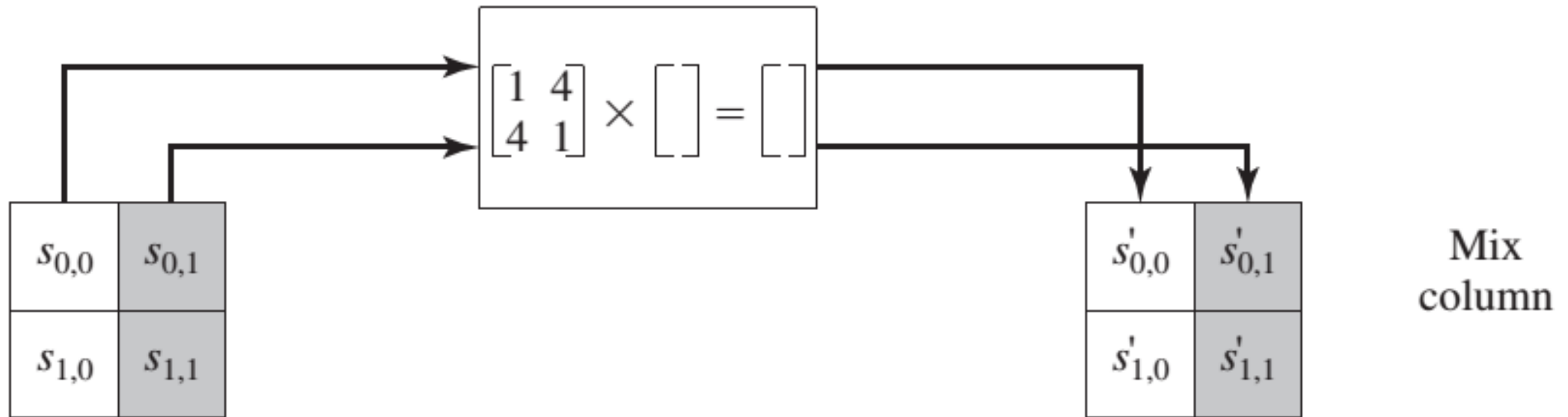


# S-AES Encryption



# S-AES Encryption

## ❑ S-AES Transformation (Mix Column)



# S-AES Encryption

## ❑ Mix Column Table

*	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
4	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
9	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E

# S-AES Encryption

❑ Round 1

3) Mix Columns:

*	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
4	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
9	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E

$$\square \text{ MixCol } (0010 \ 1110 \ 1110 \ 1110) = \begin{pmatrix} 0010 & 1110 \\ 1110 & 1110 \end{pmatrix} * \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix} =$$

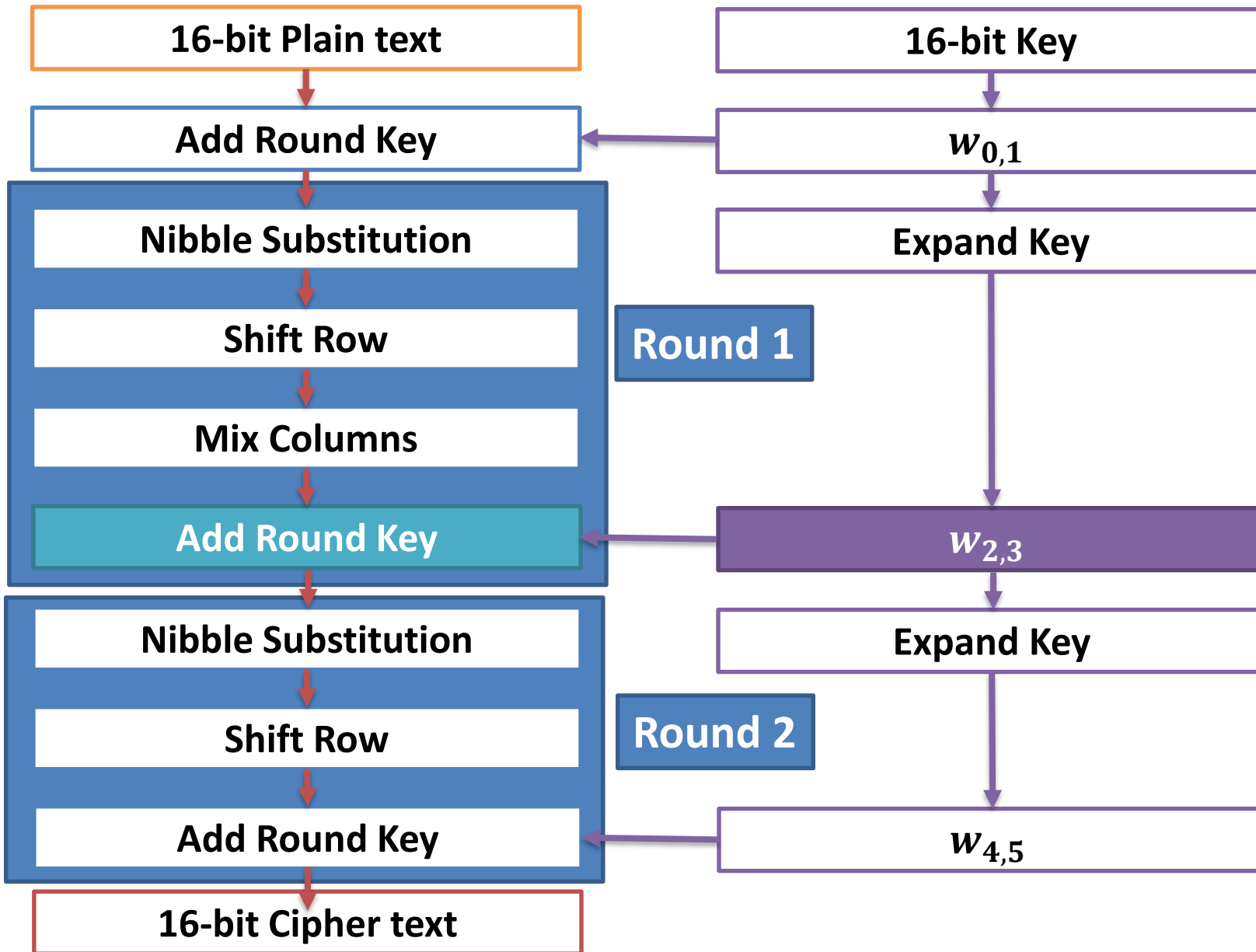
$$\square = \begin{pmatrix} 2 & E \\ E & E \end{pmatrix} * \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} (2*1 \oplus E*4) & (E*1 \oplus E*4) \\ (2*4 \oplus E*1) & (E*4 \oplus E*1) \end{pmatrix}$$

# S-AES Encryption

$$\square = \begin{pmatrix} (2 \oplus D) & (E \oplus D) \\ (8 \oplus E) & (D \oplus E) \end{pmatrix} = \begin{pmatrix} (0010 \oplus 1101) & (1110 \oplus 1101) \\ (1000 \oplus 1110) & (1101 \oplus 1110) \end{pmatrix}$$

$$\square \begin{pmatrix} (0010 \oplus 1101) & (1110 \oplus 1101) \\ (1000 \oplus 1110) & (1101 \oplus 1110) \end{pmatrix} = \begin{pmatrix} 1111 & 0011 \\ 0110 & 0011 \end{pmatrix}$$
$$= 1111 \ 0110 \ 0011 \ 0011$$

# S-AES Encryption



# S-AES Encryption

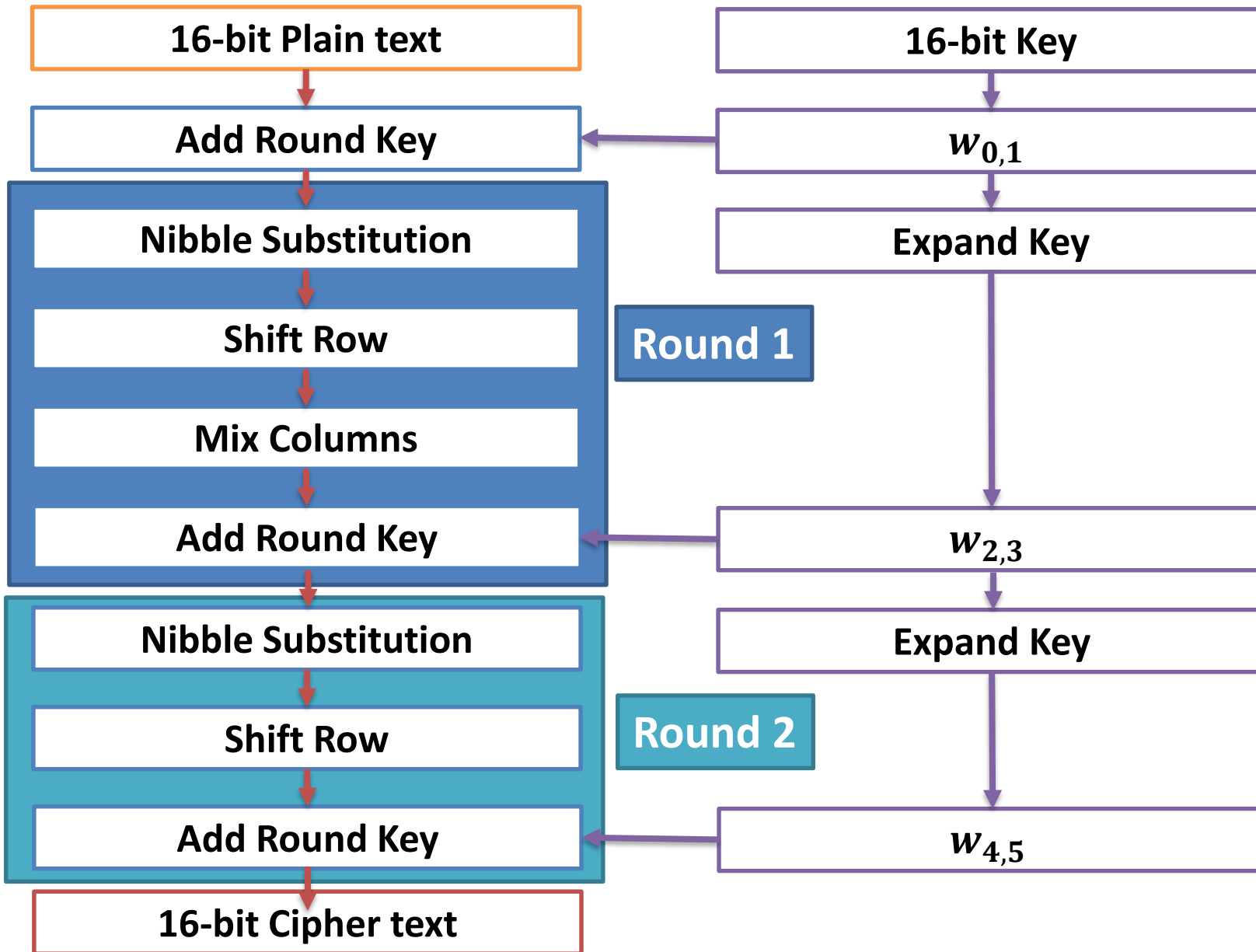
□ Round 1

4) Add round Key1

□ Key1 = 1101 1101 0010 1000

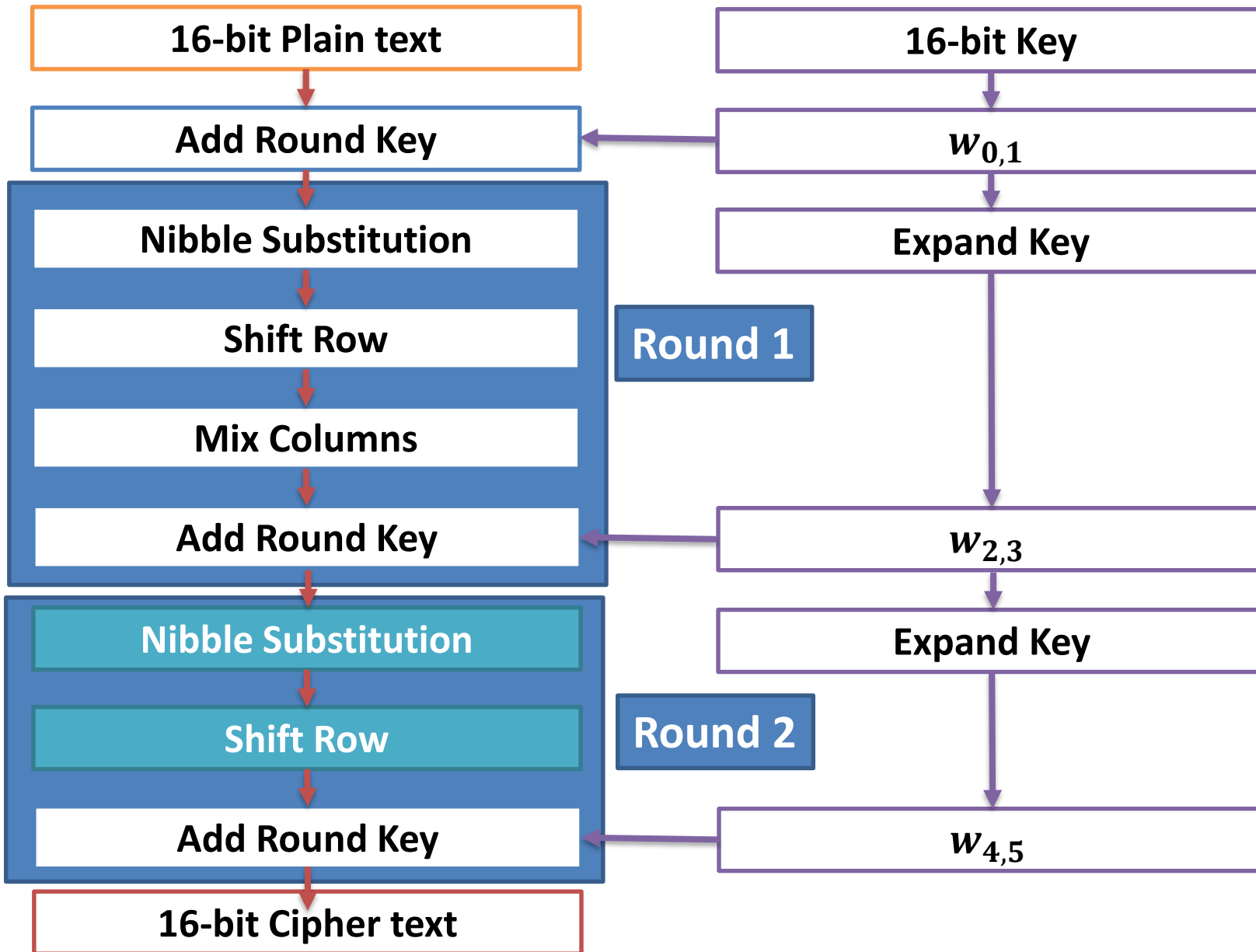
□  $R1 = \text{Key1} \oplus \text{MixCol}(\text{ShRow}(\text{SubNib}(R0)))$   
 $= 1101\ 1101\ 0010\ 1000 \oplus 1111\ 0110\ 0011\ 0011$   
 $= 0010\ 1011\ 0001\ 1011$

# S-AES Encryption



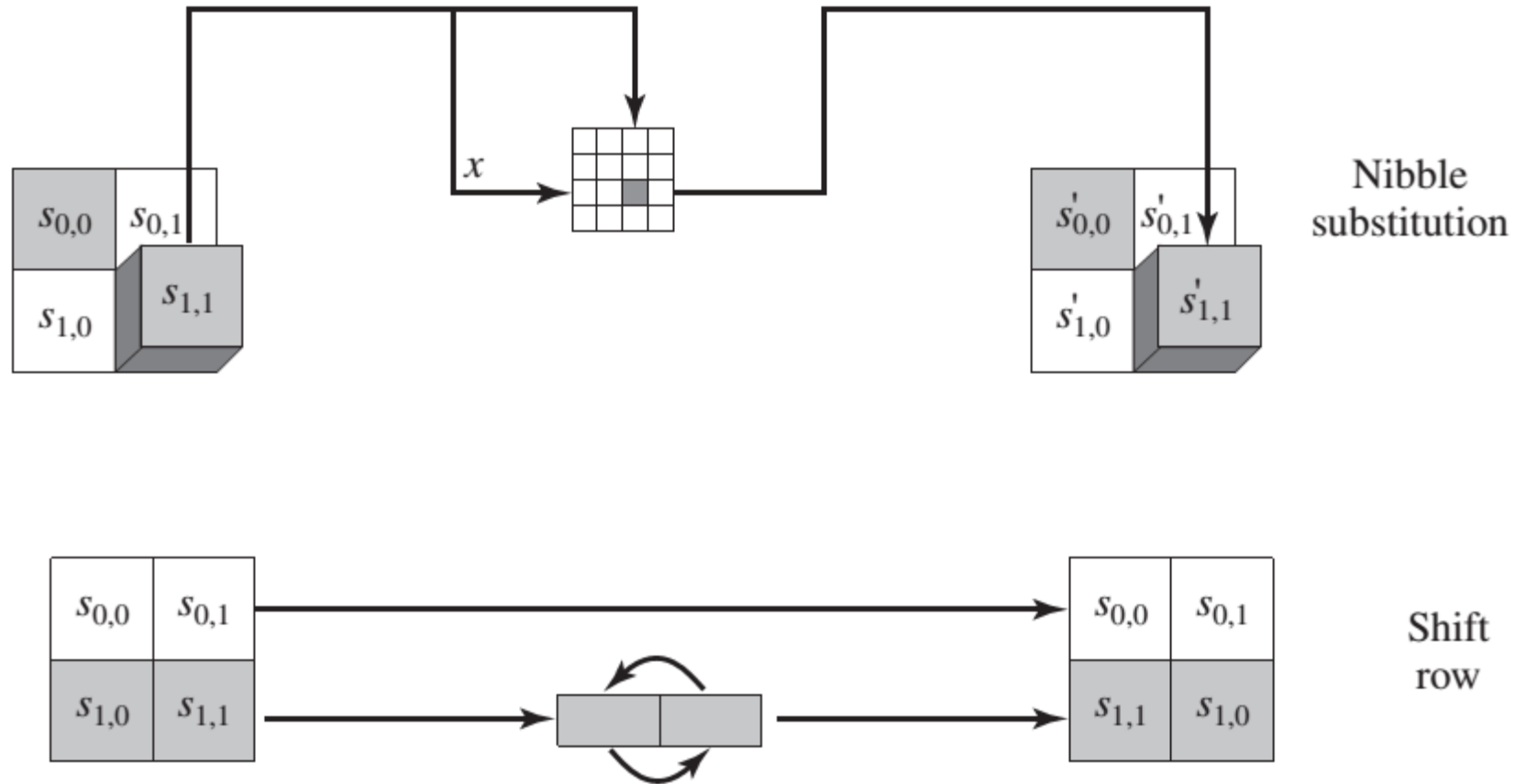


# S-AES Encryption



# S-AES Encryption

## □ S-AES Transformation (Substitution and Shift row)



# S-AES Encryption

## ❑ Round 2

### 1) Nibble Substitution :

$$\text{SubNib}(\text{0010 } \text{1011 } \text{0001 } \text{1011}) = \text{1010 } \text{0011 } \text{0100 } \text{0011}$$

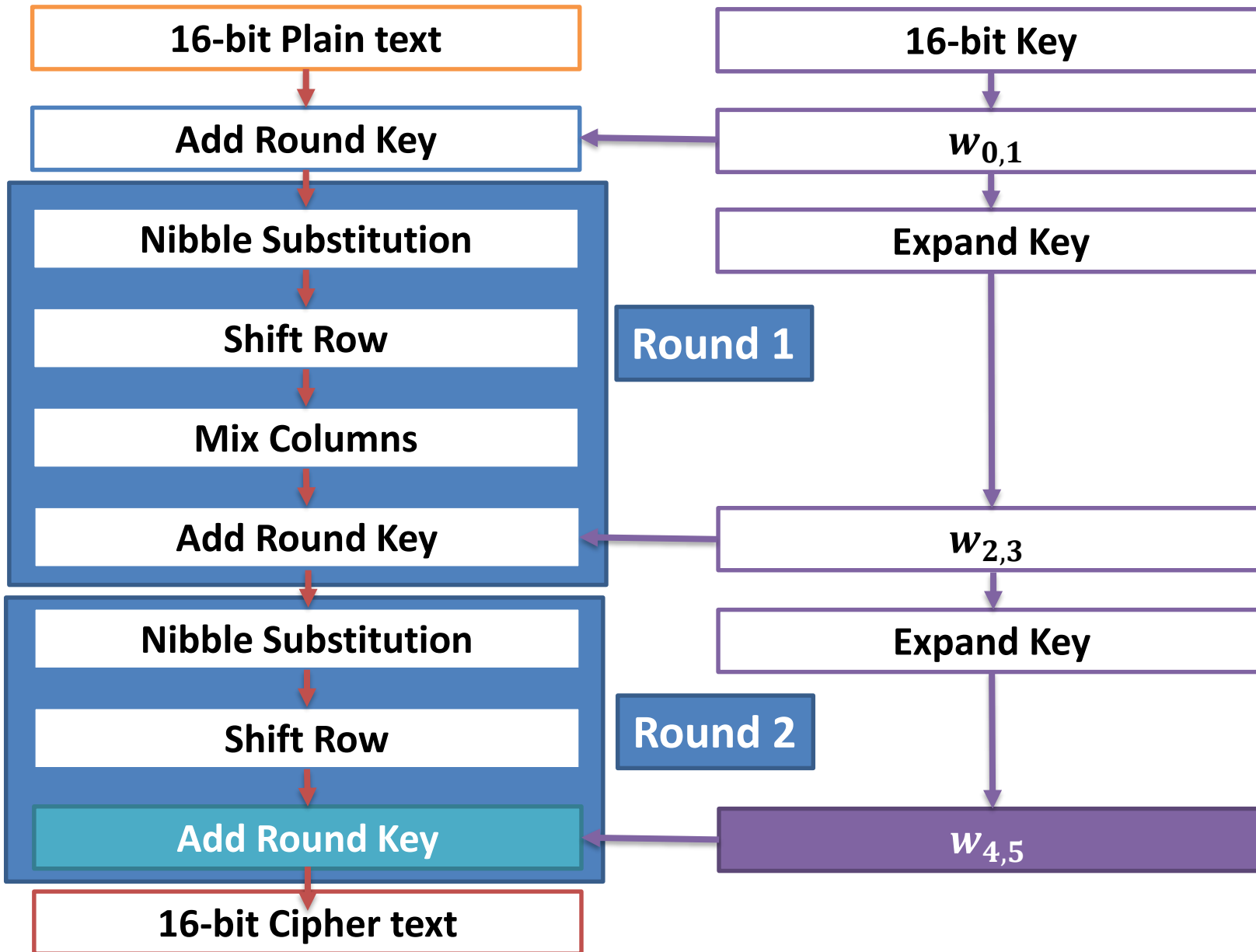
### 2) Shift Row:

❑ Swap 2nd nibble and 4th nibble

$$\begin{aligned} \text{ShRow}(\text{1010 } \text{0011 } \text{0100 } \text{0011}) \\ = \text{1010 } \text{0011 } \text{0100 } \text{0011} \end{aligned}$$

S-Box		<i>j</i>			
		00	01	10	11
<i>i</i>	00	9	4	A	B
	01	D	1	8	5
	10	6	2	0	3
	11	C	E	F	7

# S-AES Encryption



# S-AES Encryption

## ❑ Round 2

### 4) Add round Key2

❑  $\text{Key2} = 1000\ 0111\ 1010\ 1111$

❑  $R2 = \text{Key2} \oplus \text{ShRow}(\text{SubNib}(R1))$

$$= 1000\ 0111\ 1010\ 1111 \oplus 1010\ 0011\ 0100\ 0011$$

$$= 0010\ 0100\ 1110\ 1100$$

$$\text{Ciphertext} = 0010\ 0100\ 1110\ 1100$$

# Table of Contents

**Simplified Advanced Encryption Standard**

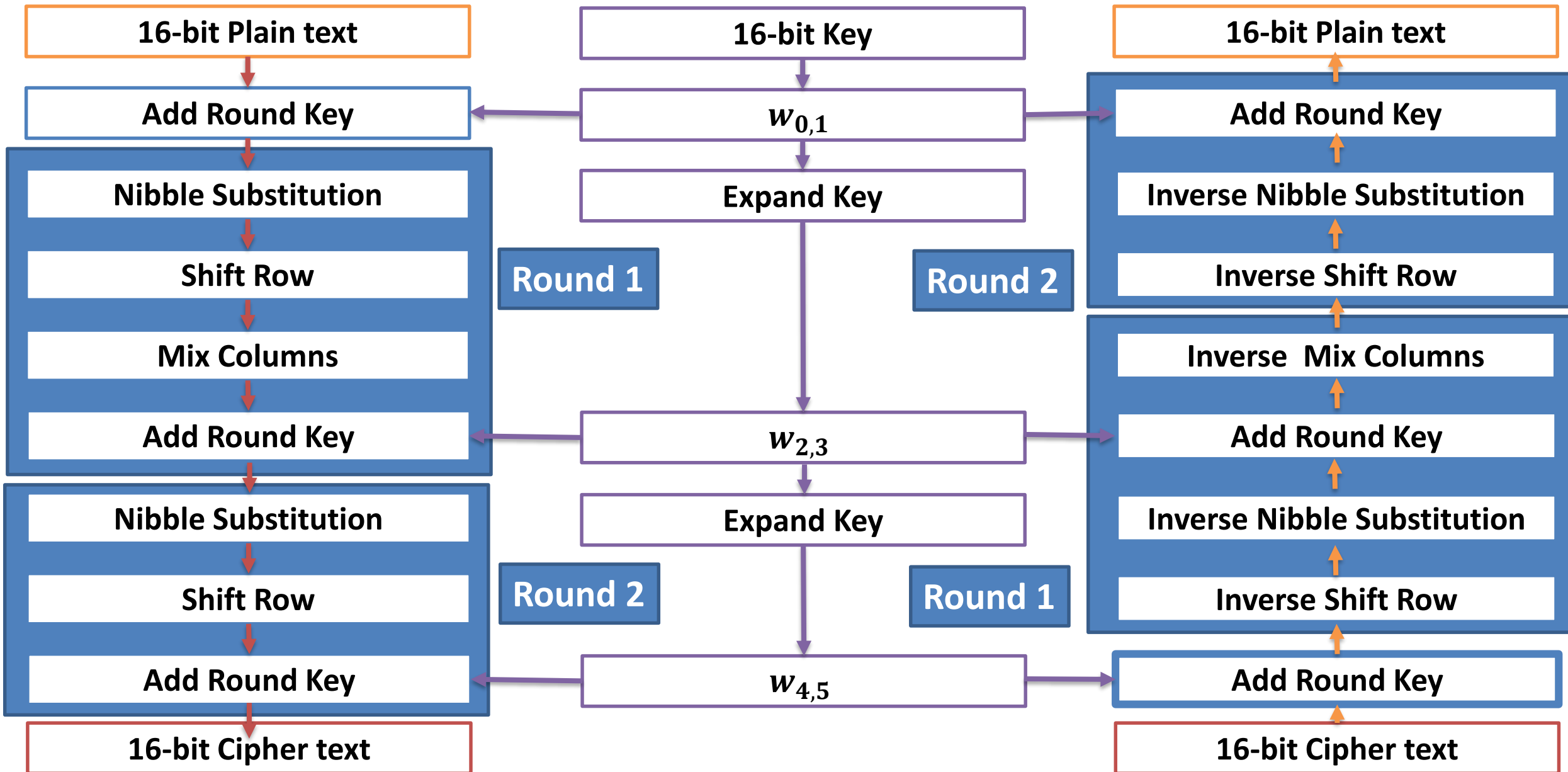
**S-AES Encryption and Decryption**

**S-AES Key Generation**

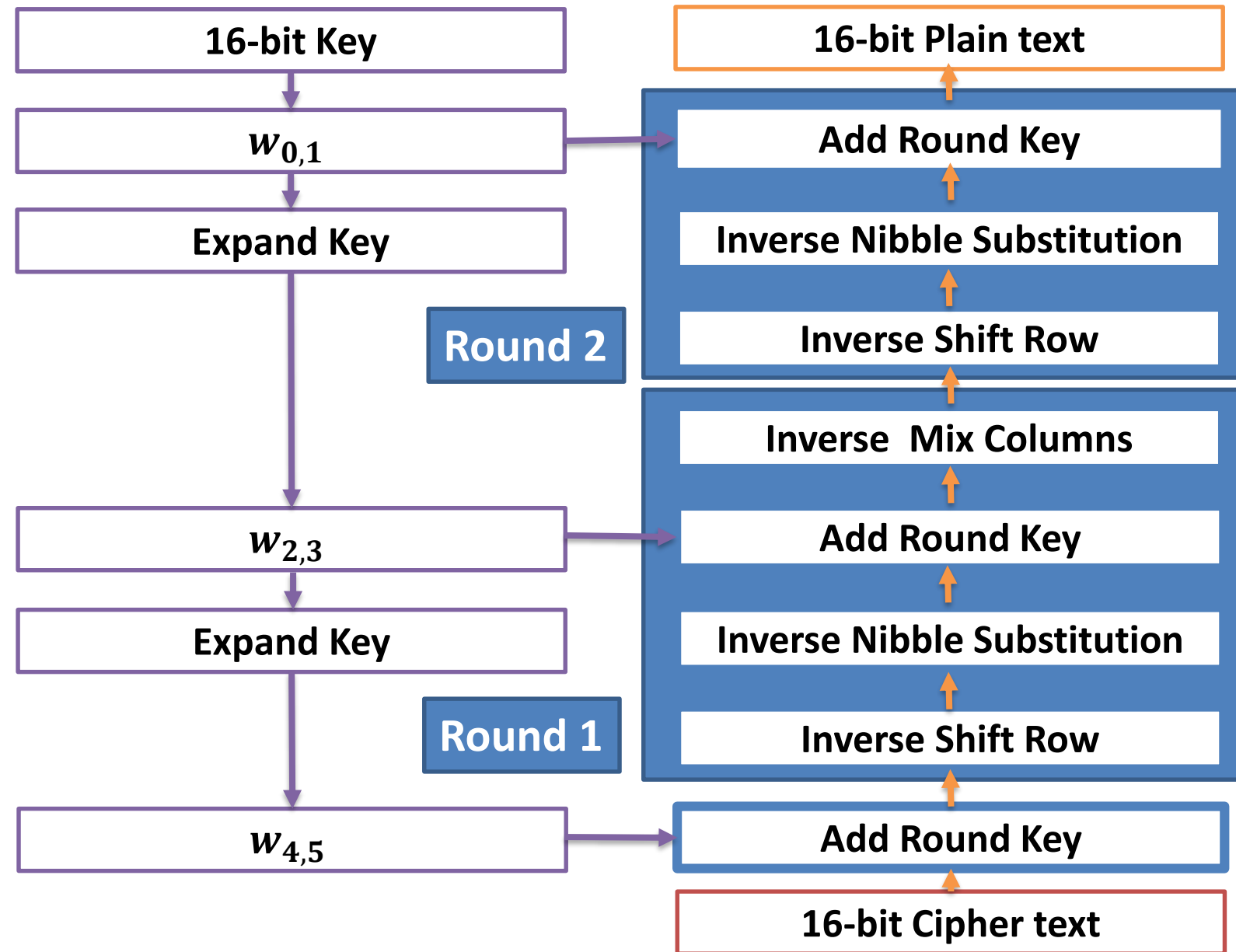
**S-AES Encryption**

**S-AES Decryption**

# S-AES Encryption and Decryption



# S-AES Decryption





# S-AES Decryption

❑ Assume:  $C = 0010\ 0100\ 1110\ 1100$

❑  $Key0 = w0w1$

$= 0100\ 1010\ 1111\ 0101$

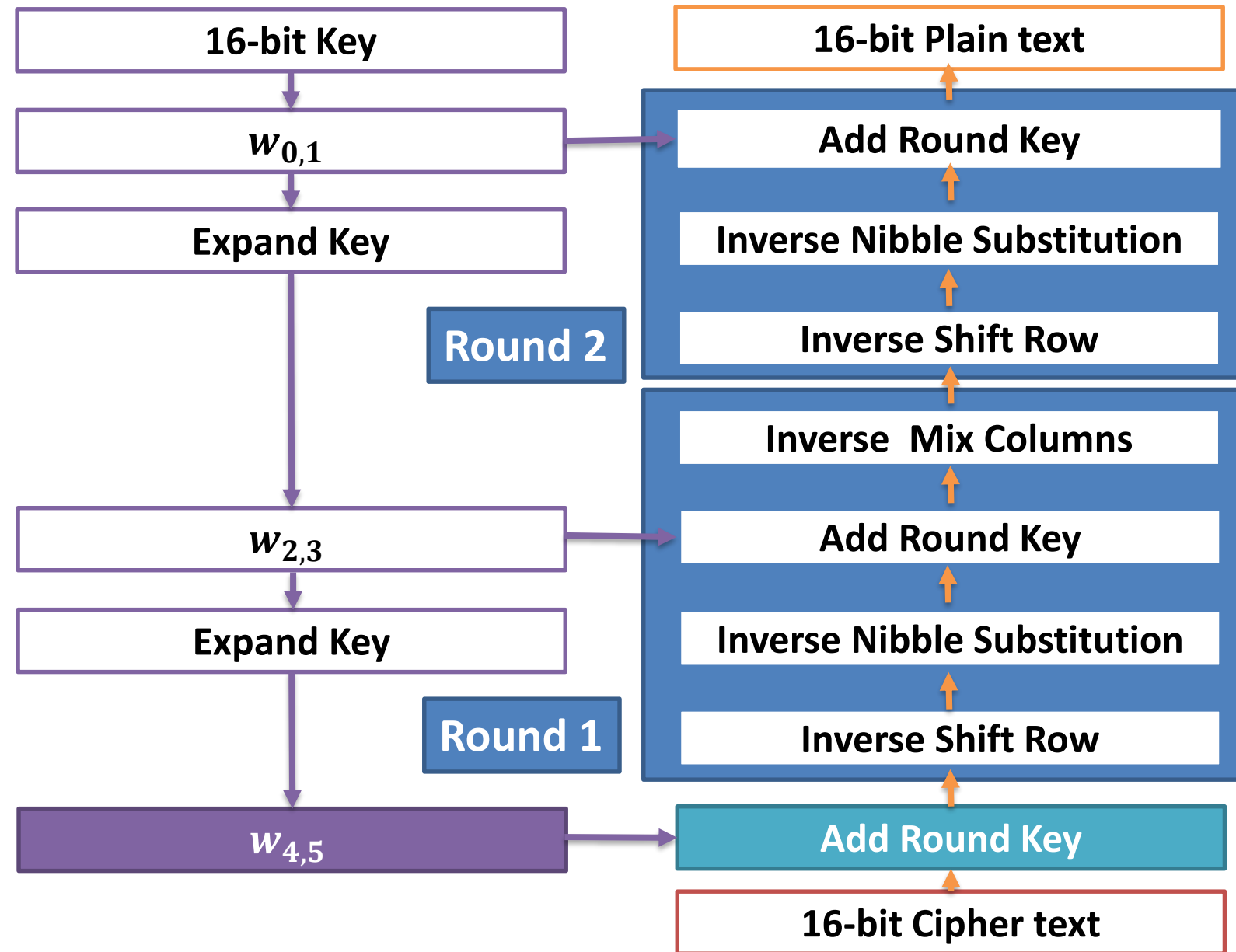
❑  $Key1 = w2w3$

$= 1101\ 1101\ 0010\ 1000$

❑  $Key2 = w4w5$

$= 1000\ 0111\ 1010\ 1111$

# S-AES Decryption



# S-AES Decryption

$$\square \text{Key2} = w_4 w_5$$

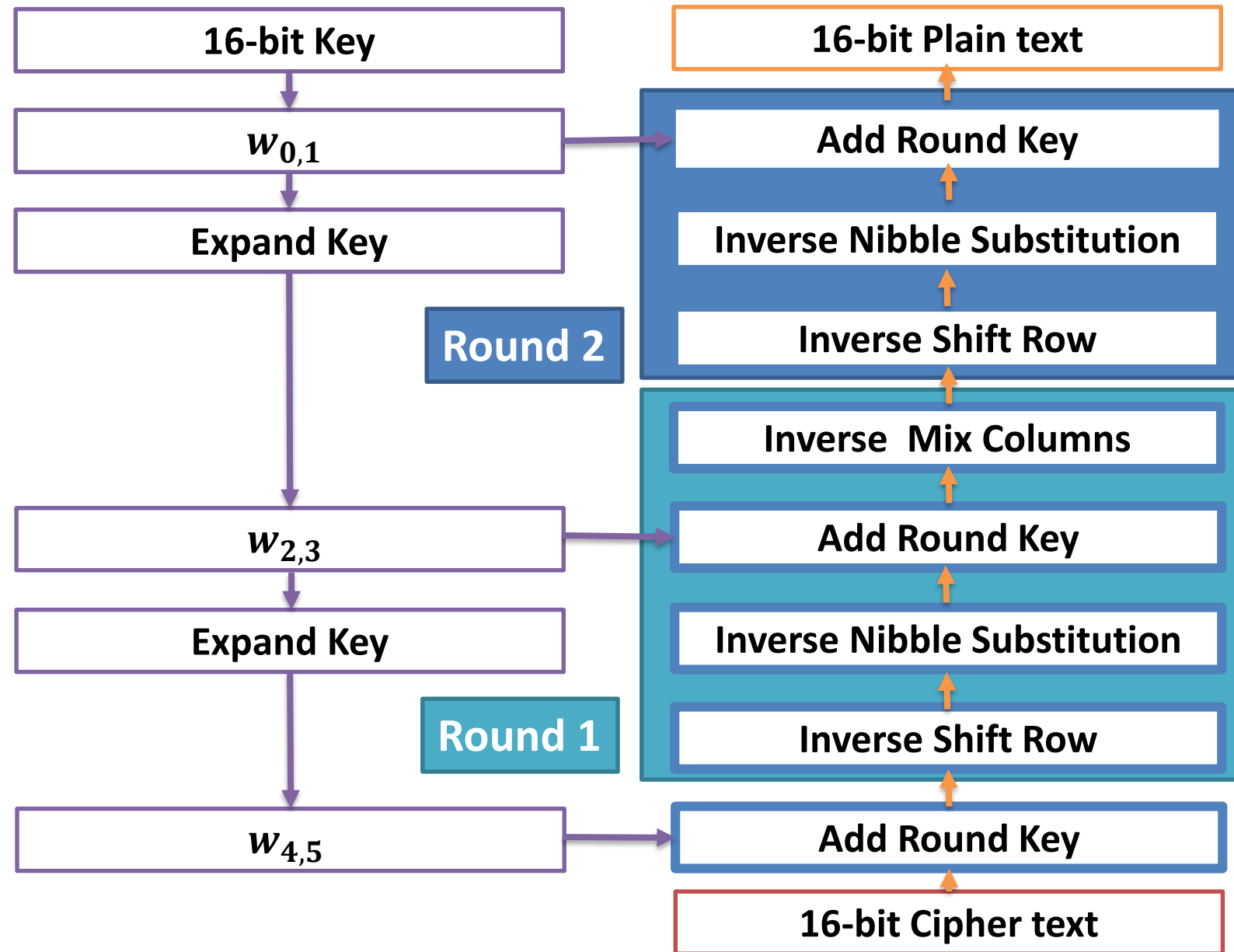
$$= 1000\ 0111\ 1010\ 1111$$

$$\square C = 0010\ 0100\ 1110\ 1100$$

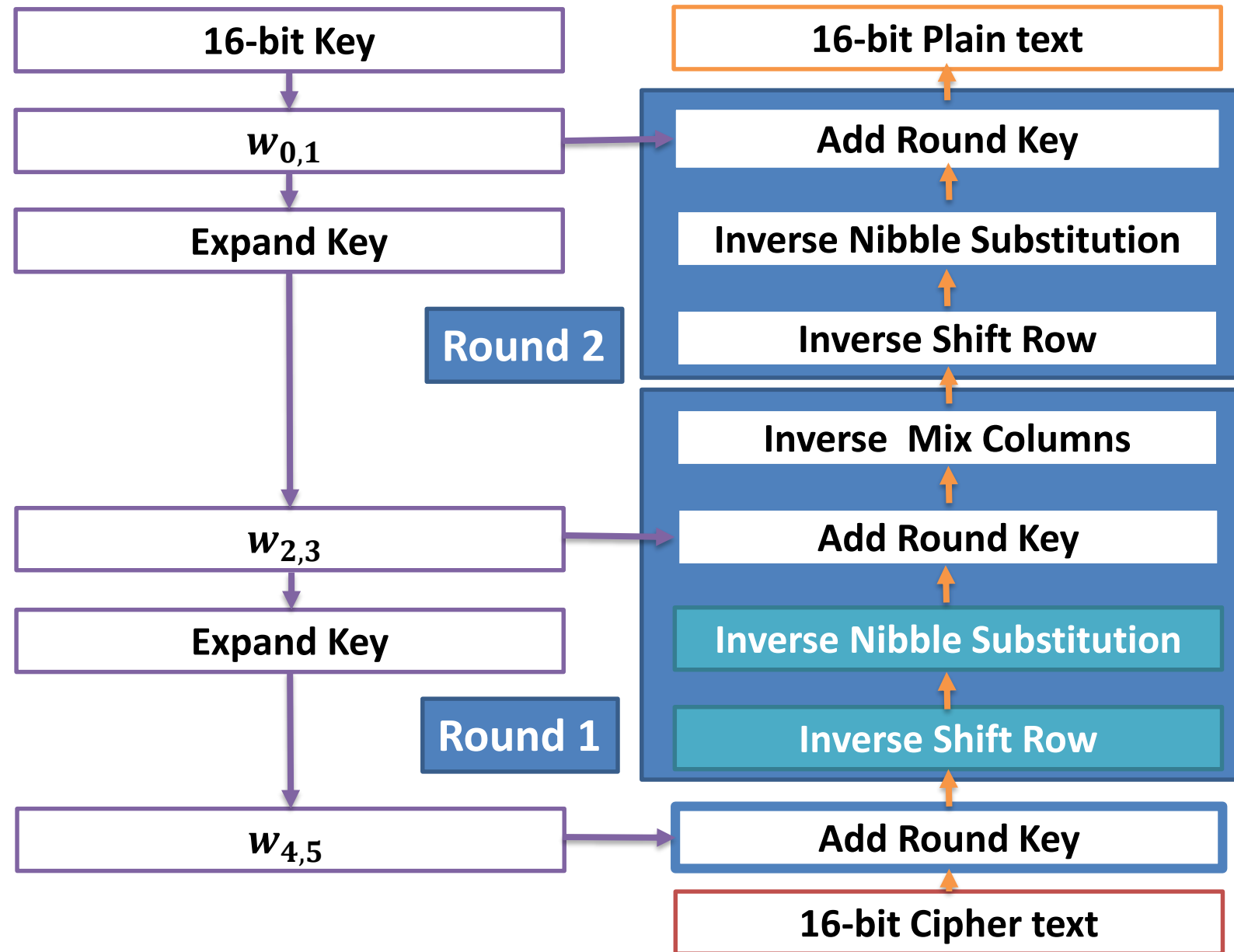
$$\square R_0 = C \oplus \text{Key2} = 0010\ 0100\ 1110\ 1100 \oplus 1000\ 0111\ 1010\ 1111$$

$$\square = 1010\ 0011\ 0100\ 0011$$

# S-AES Decryption



# S-AES Decryption



## □ Round 1

### 1) Inverse Shift Row

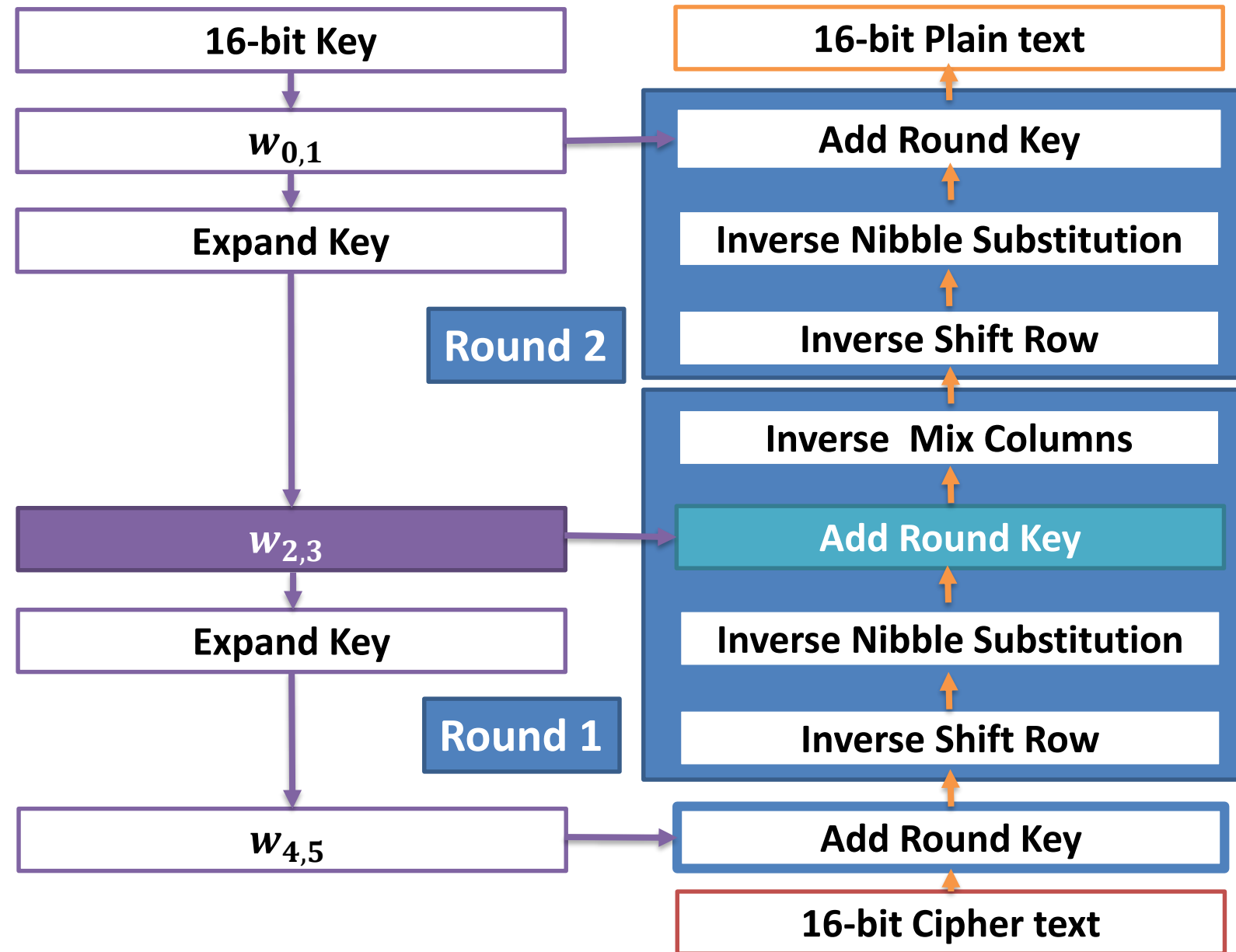
$$\begin{aligned}\square \text{IShRow}(R_0) &= \text{IShRow}(1010 \text{ } 0011 \text{ } 0100 \text{ } 0011) = \\ &= 1010 \text{ } 0011 \text{ } 0100 \text{ } 0011\end{aligned}$$

### 2) Inverse Nibble Sub

$$\begin{aligned}\square \text{ISubNib}( \text{ } 1010 \text{ } 0011 \text{ } 0100 \text{ } 0011 ) &= \\ &= 0010 \text{ } 1011 \text{ } 0001 \text{ } 1011\end{aligned}$$

Inv S-Box		<i>j</i>			
		00	01	10	11
<i>i</i>	00	A	5	9	B
	01	1	7	8	F
	10	6	0	2	3
	11	C	4	D	E

# S-AES Decryption



# S-AES Decryption

## 3) Add Round 1 Key

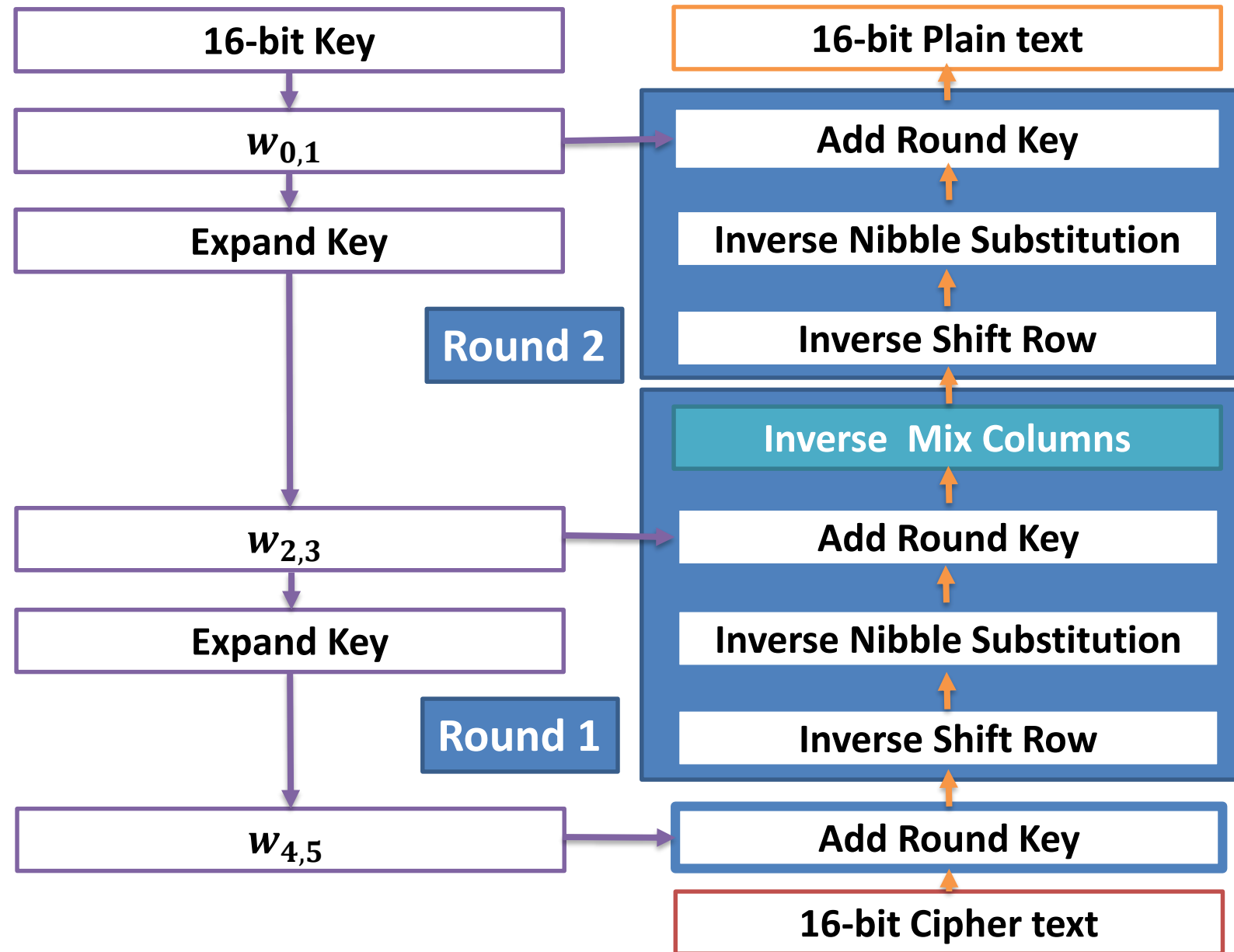
$$\square 0010\ 1011\ 0001\ 1011 \oplus \text{Key1}$$

$$= 0010\ 1011\ 0001\ 1011 \oplus 1101\ 1101\ 0010\ 1000$$

$$= 1111\ 0110\ 0011\ 0011$$



# S-AES Decryption



# S-AES Encryption

## ❑ Round 1

### 4) Inverse Mix Columns :

$$\text{❑ MixCol (1111 0110 0011 0011)} = \begin{pmatrix} 1111 & 0011 \\ 0110 & 0011 \end{pmatrix} * \begin{pmatrix} 9 & 2 \\ 2 & 9 \end{pmatrix} =$$

$$\text{❑} = \begin{pmatrix} F & 3 \\ 6 & 3 \end{pmatrix} * \begin{pmatrix} 9 & 2 \\ 2 & 9 \end{pmatrix} = \begin{pmatrix} (F*9 \oplus 6*2) & (3*9 \oplus 3*2) \\ (F*2 \oplus 6*9) & (3*2 \oplus 3*9) \end{pmatrix}$$

$$\text{❑} = \begin{pmatrix} (E \oplus C) & (8 \oplus 6) \\ (D \oplus 3) & (6 \oplus 8) \end{pmatrix}$$

$$\text{❑} = \begin{pmatrix} (1110 \oplus 1100) & (1000 \oplus 0110) \\ (1101 \oplus 0011) & (0110 \oplus 1000) \end{pmatrix}$$

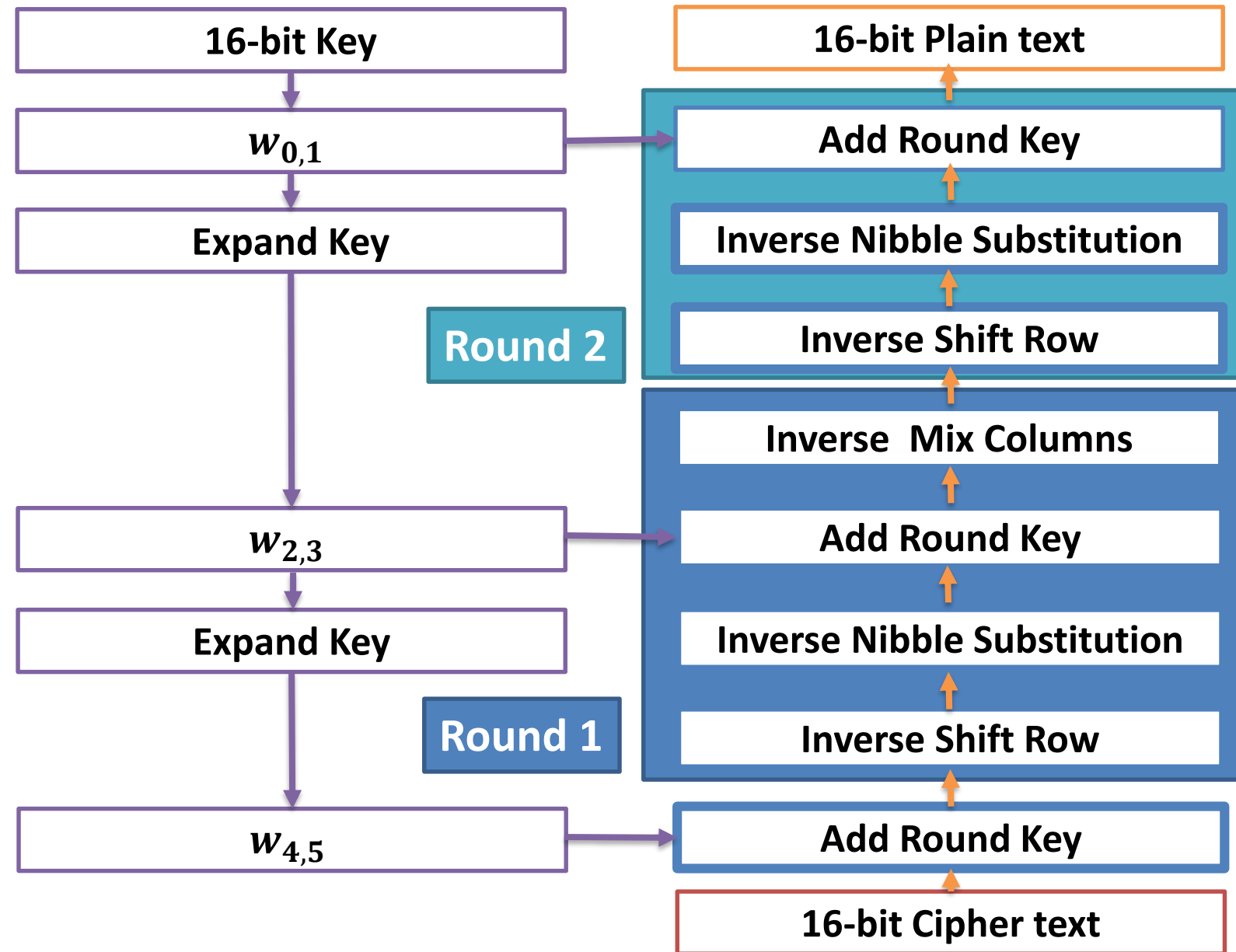
*	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
4	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
9	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E

# S-AES Encryption

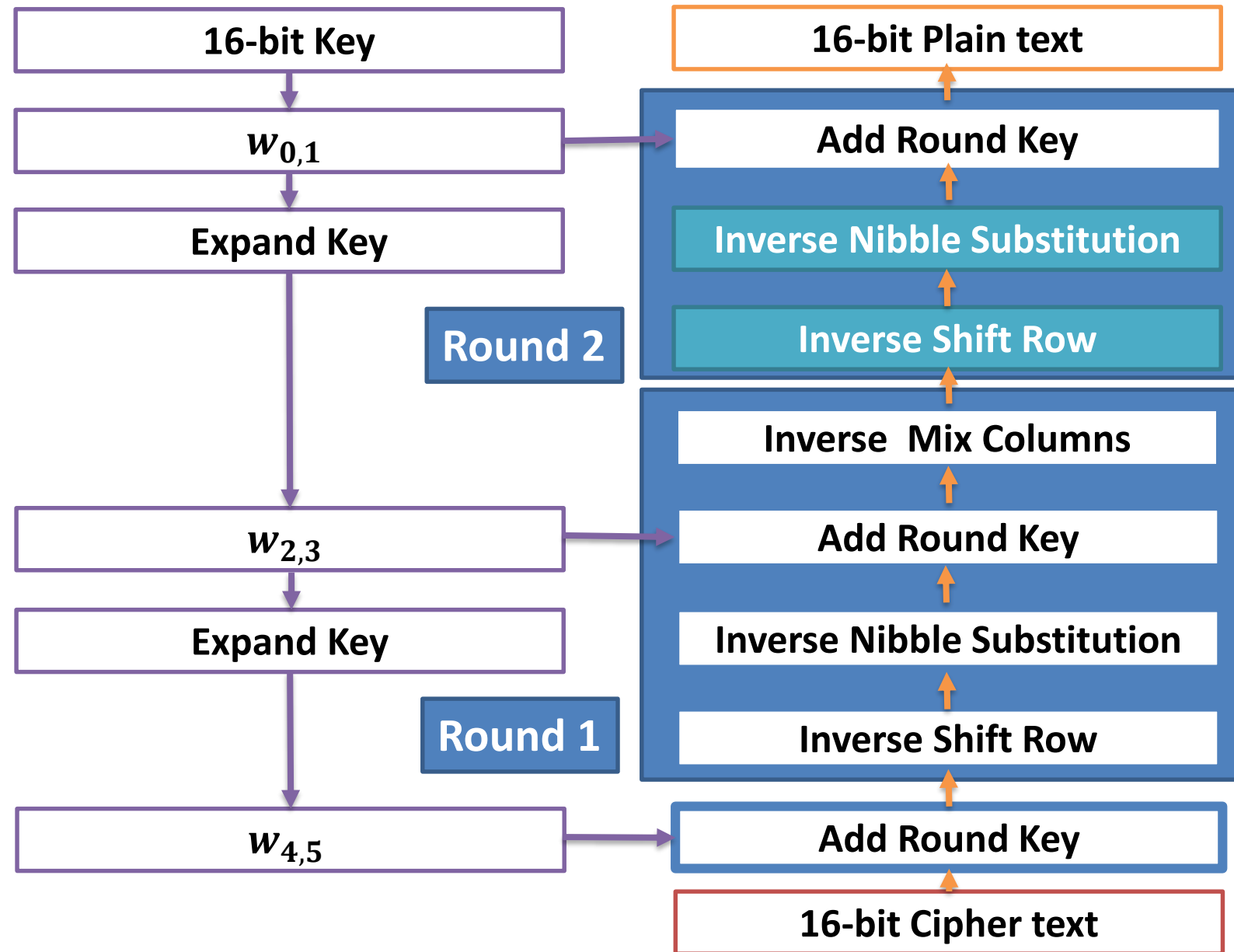
$$\square \begin{pmatrix} (1110 \oplus 1100) & (1000 \oplus 0110) \\ (1101 \oplus 0011) & (0110 \oplus 1000) \end{pmatrix} = \begin{pmatrix} 0010 & 1110 \\ 1110 & 1110 \end{pmatrix}$$

$$R1 = 0010 \ 1110 \ 1110 \ 1110$$

# S-AES Decryption



# S-AES Decryption



## □ Round 2

### 1) Inverse Shift Row

$$\begin{aligned}\square \text{IShRow}(R1) &= \text{IShRow}(0010 \text{ } 1110 \text{ } 1110 \text{ } 1110) = \\ &= 0010 \text{ } 1110 \text{ } 1110 \text{ } 1110\end{aligned}$$

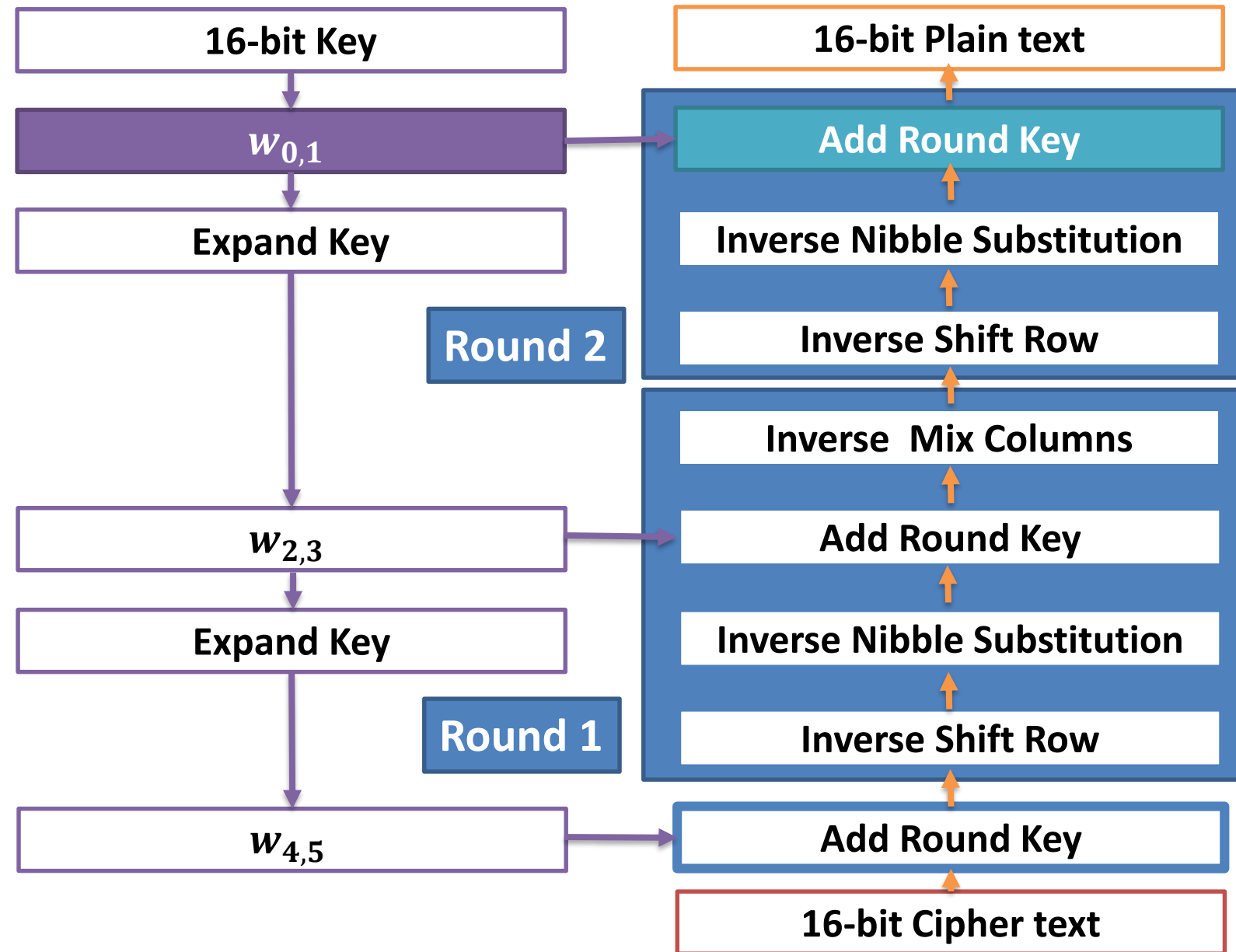
### 2) Inverse Nibble Sub

$$\begin{aligned}\square \text{ISubNib}( \text{ } 0010 \text{ } 1110 \text{ } 1110 \text{ } 1110 ) &= \\ &= 1001 \text{ } 1101 \text{ } 1101 \text{ } 1101\end{aligned}$$

		<i>j</i>			
		00	01	10	11
<i>i</i>	00	A	5	9	B
	01	1	7	8	F
	10	6	0	2	3
	11	C	4	D	E

Inv S-Box

# S-AES Decryption



# S-AES Decryption

## 3) Add Round 2 Key

$$\begin{aligned}\square R2 &= 1001\ 1101\ 1101\ 1101 \oplus \text{Key0} \\ &= 1001\ 1101\ 1101\ 1101 \oplus 0100\ 1010\ 1111\ 0101 \\ &= 1101\ 0111\ 0010\ 1000\end{aligned}$$

Plaintext = 1101 0111 0010 1000 = D7 28



# Contact Me



[facebook.com/mloey](https://facebook.com/mloey)



[mohamedloey@gmail.com](mailto:mohamedloey@gmail.com)



[twitter.com/mloey](https://twitter.com/mloey)



[linkedin.com/in/mloey](https://linkedin.com/in/mloey)



[mloey@fci.bu.edu.eg](mailto:mloey@fci.bu.edu.eg)



[mloey.github.io](https://mloey.github.io)

THANKS FOR  
YOUR TIME

