

Cybersecurity Concepts

Prepared by Dr. Diaa Salama

FNT625
Simplified Advanced Encryption Standard (S_AES) ,
RSA

Lecture 9





مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY

Cybersecurity Concepts

Lecture 9

FNT625

Simplified Advanced Encryption Standard (S_AES) ,
RSA

Prepared by
Dr. Diao Salama

www.midocean.ae

PLEASE
BE QUIET



10



Lecture

09

Lets Start the Eighth Lecture



Simplified Advanced
Encryption Standard (S_AES) ,
RSA



Simplified Advanced Encryption Standard (S_AES)

RSA

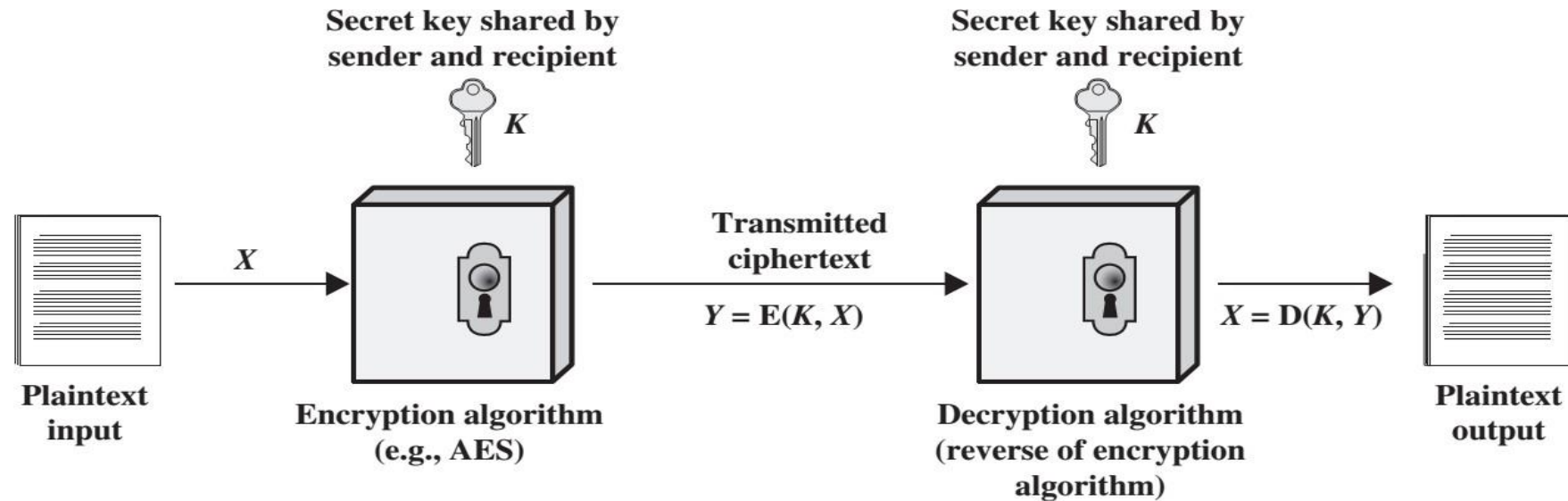
Simplified Advanced Encryption Standard S_AES

RSA

Cryptography and Network Security

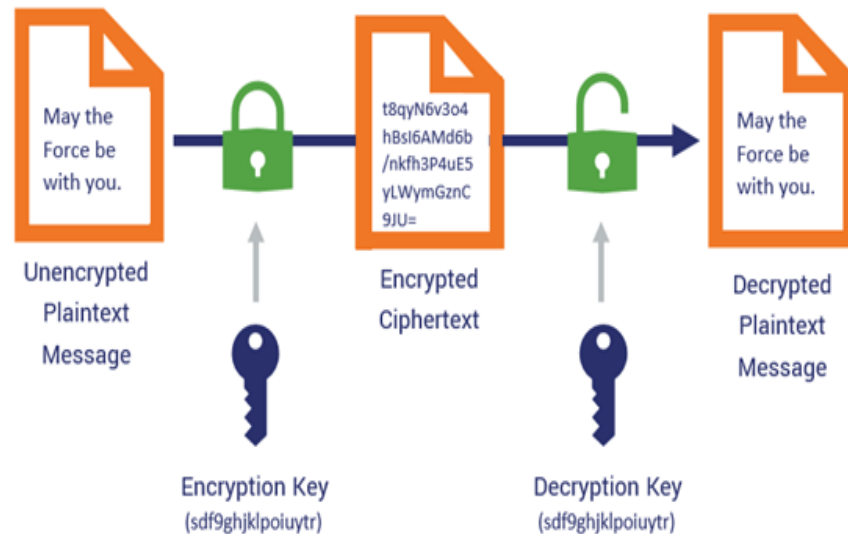
Lecture

09



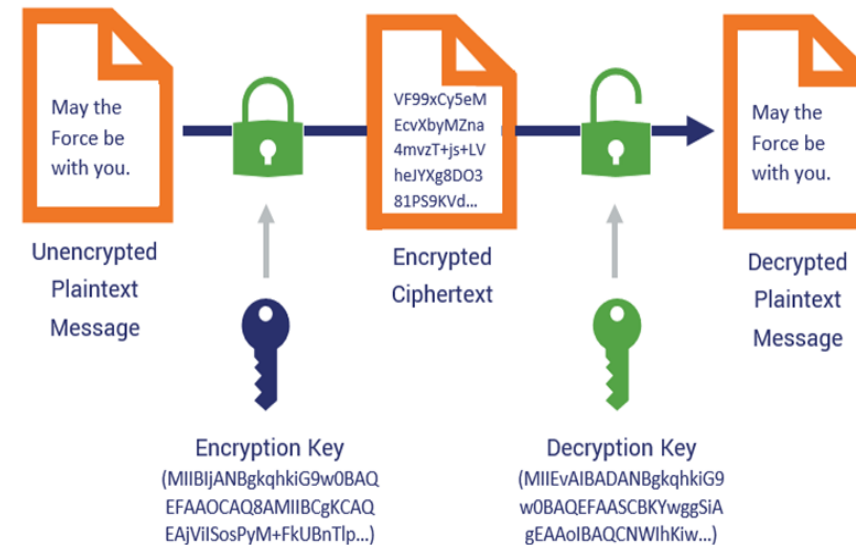
Symmetric Encryption Algorithm

How Encryption Works



Asymmetric Encryption Algorithm

How Asymmetric Encryption Works



Cryptographic Algorithms

Symmetric Encryption	Asymmetric Encryption
• Symmetric encryption consists of one key for encryption and decryption.	• Asymmetric Encryption consists of two cryptographic keys known as Public Key and Private Key.
• Symmetric Encryption is a lot quicker compared to the Asymmetric method.	• As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably.
• RC4 • AES • DES • 3DES • QUAD	• RSA • Diffie-Hellman • ECC • El Gamal • DSA

Stream Cipher and Block Cipher

Lecture

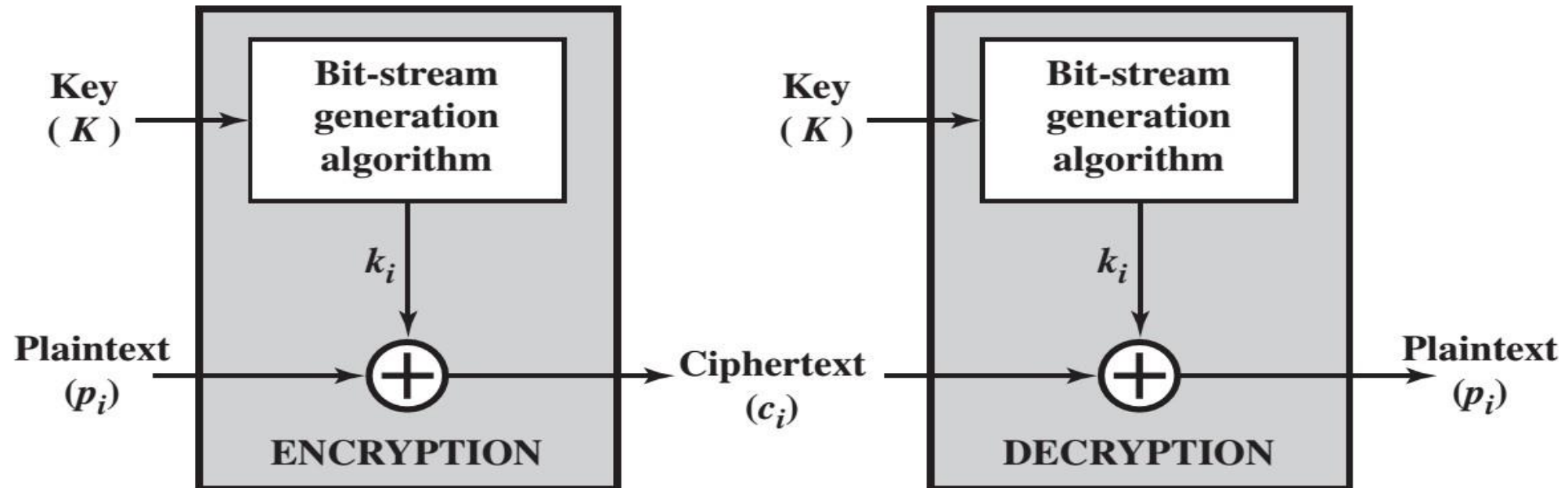
09

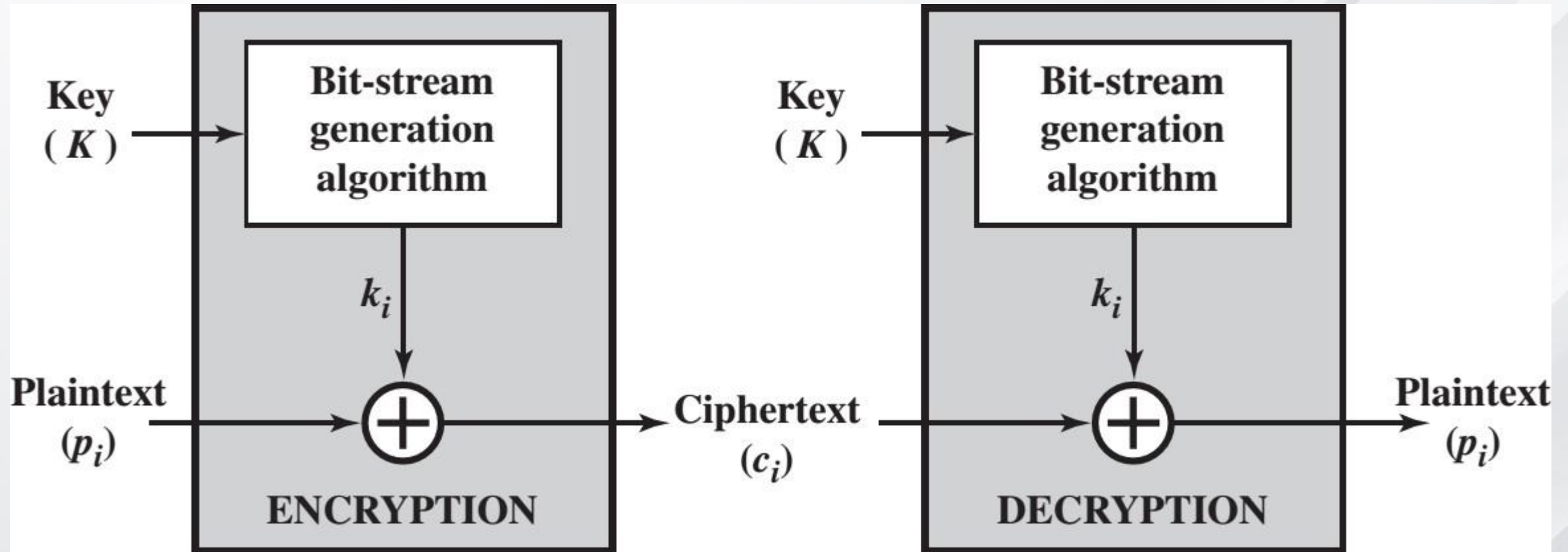
- Stream cipher is one that encrypts a digital data stream one bit or one byte at a time.
- Block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

Stream Cipher

Lecture

09

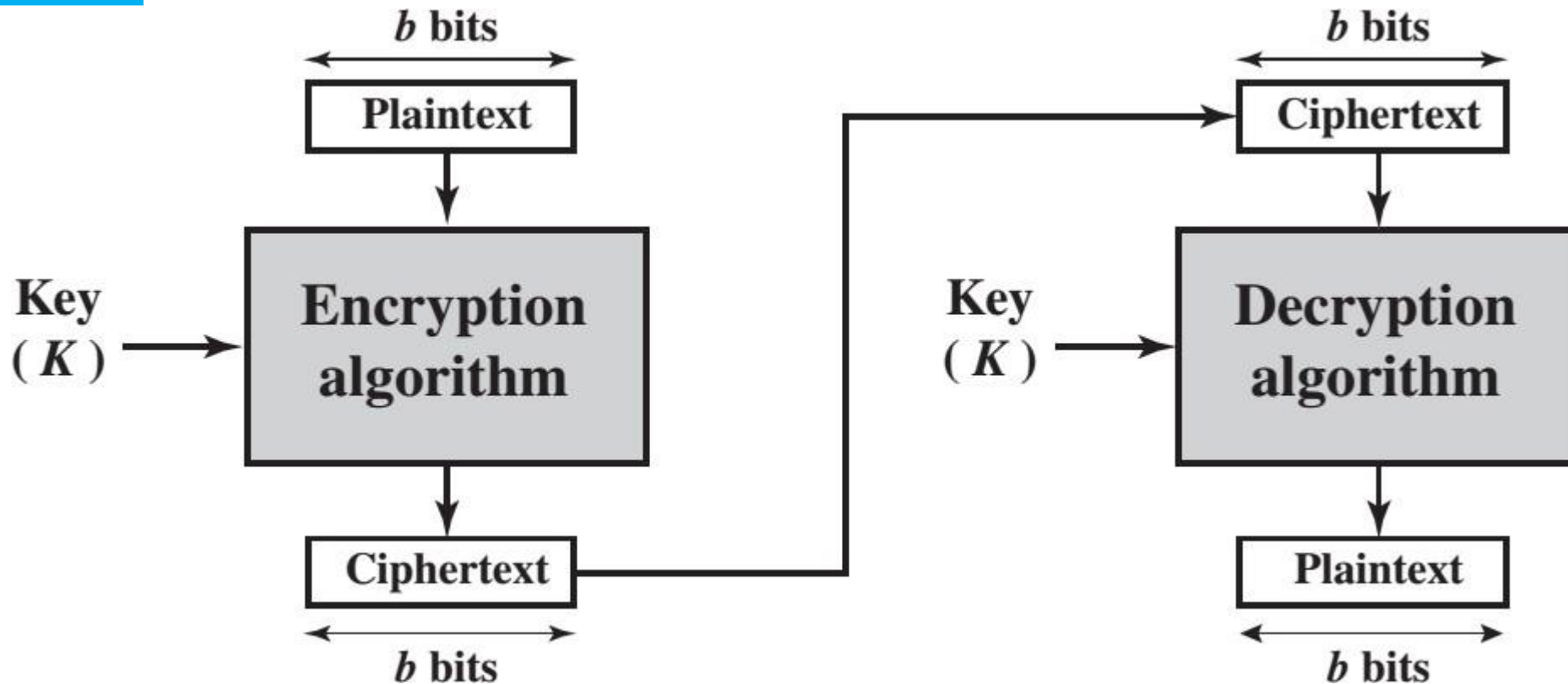




Block Cipher

Lecture

09



- 1999: NIST indicates that DES should be replaced as a standard
 - have theoretical attacks that can break it
 - have demonstrated exhaustive key search attacks
- Triple-DES should be used before a new standard is approved
 - 3DES has 168-bit key: brute-force attack is infeasible
 - Same engine as for DES is running – software/hardware can be reused
 - Confident that no effective attack exists: DES has been around for a long time
 - As far as security is concerned, 3DES is ideal to replace DES
- Drawbacks of 3DES
 - Relatively slow software implementations – DES was designed for 1970's hardware
 - DES and 3DES use 64-bit blocks: for efficiency and security, larger blocks should be used

Requirements for the new standard

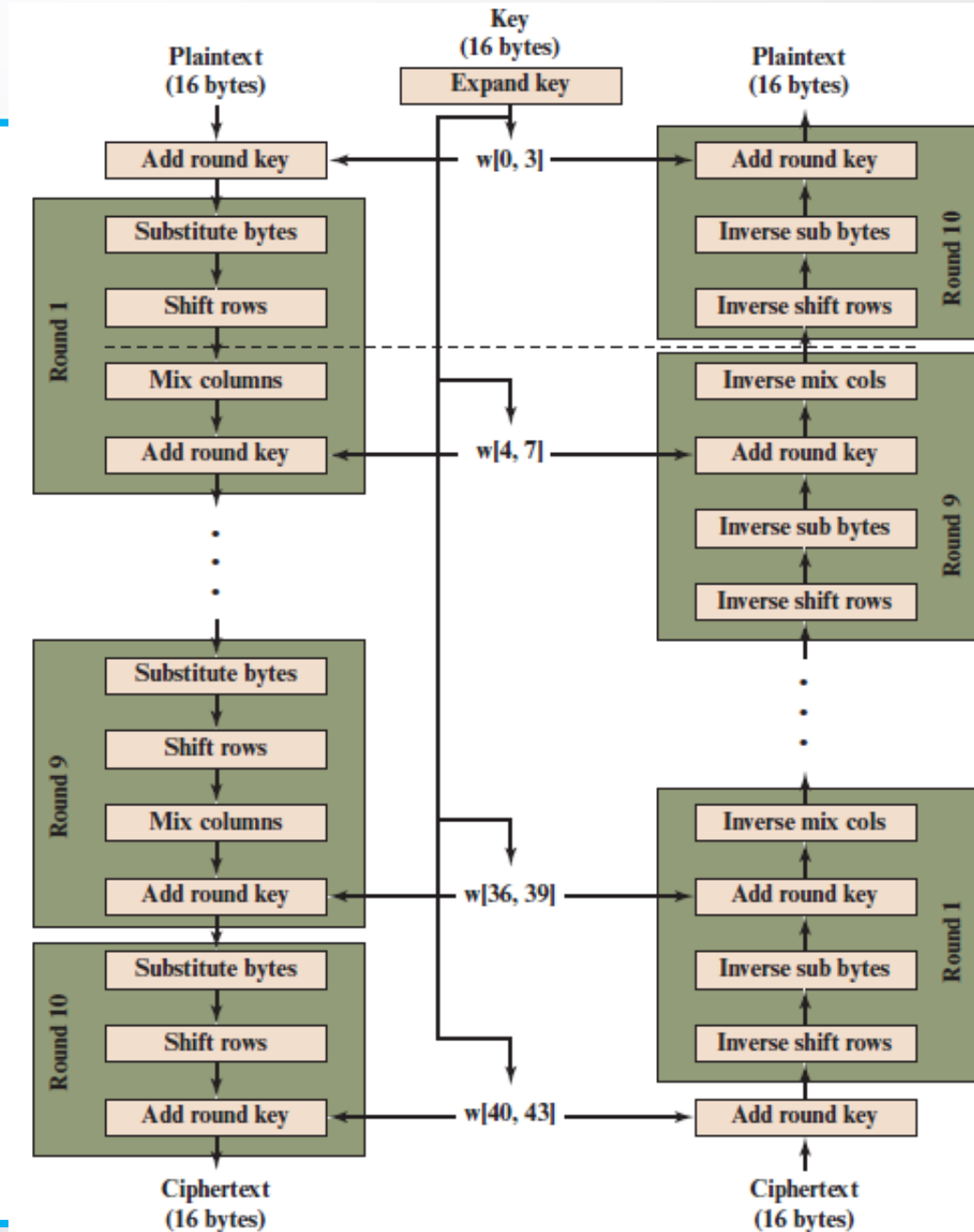
- Private key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than 3DES
- Active life of 20-30 years (+ archival use)
- Provide full specification and design details
- Both C and Java implementations
- NIST have released all submissions & unclassified analyses

- Processes data as 4 groups of 4 bytes – 128-bit block
- Input block copied into **State** array, modified at each stage of encryption or decryption and copied to the output matrix after the final round
- has 9/11/13 rounds (depending on which variant is used) in which **State** undergoes:
 - byte substitution (one S-box used on every byte)
 - shift rows: a simple permutation
 - mix columns: substitution using arithmetic in $GF(2^8)$
 - add round key (XOR **State** with the round key)
- initial XOR of the plaintext with a round key
- There is an incomplete last round (the 10th/12th/14th)
- Note: all operations can be combined into XOR and table lookups - hence very fast and efficient

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

Figure 6.3 AES Encryption and Decryption



Advanced Encryption Standard

Simplified Advanced Encryption Standard (AES)

Simplified Advanced Encryption Standard

S-AES Encryption and Decryption

S-AES Key Generation

S-AES Encryption

S-AES Decryption

Simplified Advanced Encryption Standard

S-AES Encryption and Decryption

S-AES Key Generation

S-AES Encryption

S-AES Decryption

Simplified Advanced Encryption Standard

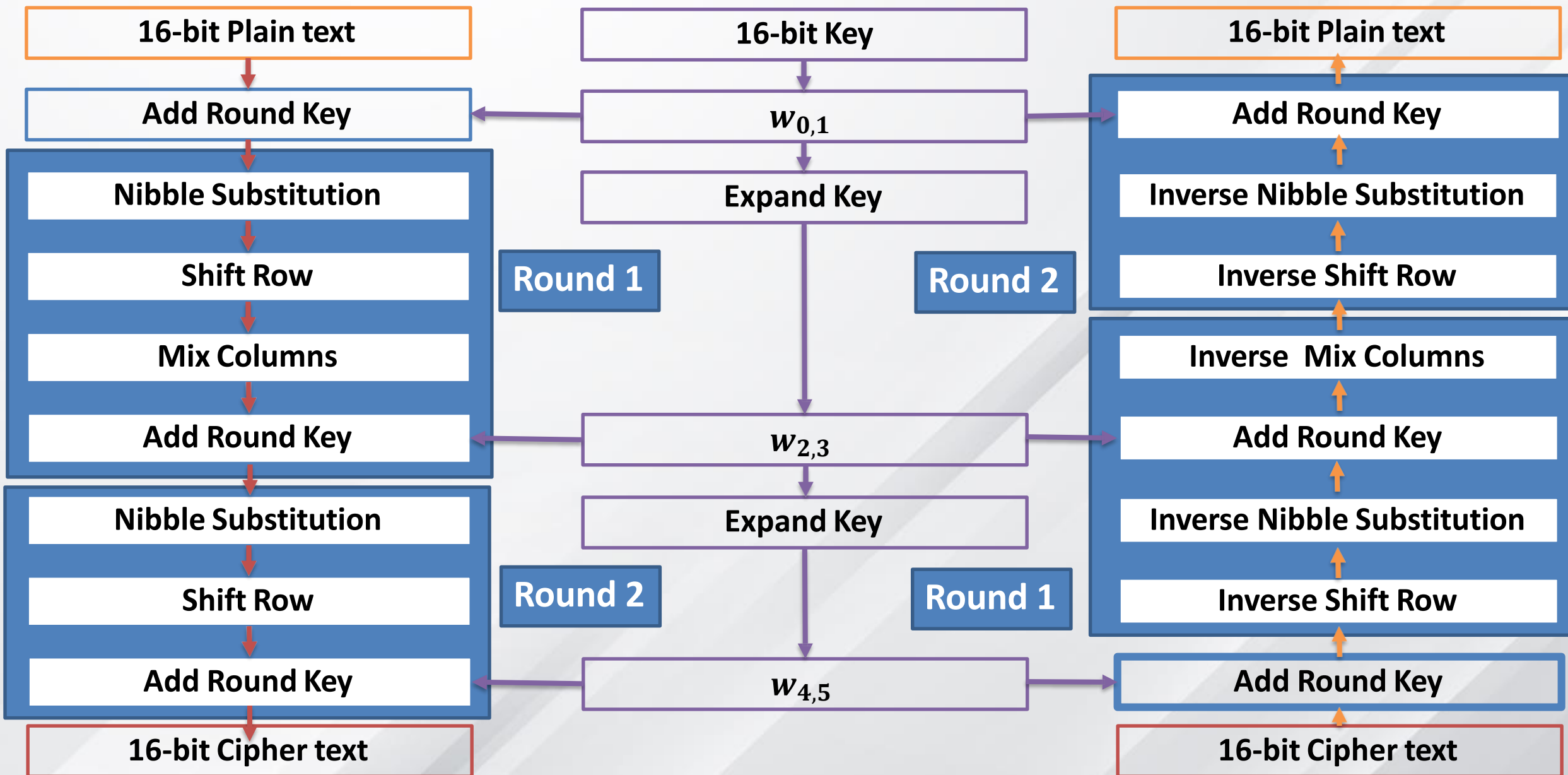
S-AES Encryption and Decryption

S-AES Key Generation

S-AES Encryption

S-AES Decryption

S-AES Encryption and Decryption



□ 16-bit Plaintext, P= D7 28

=1101 0111 0010 1000

□ 16-bit Key, K= 4A F5

=0100 1010 1111 0101

Simplified Advanced Encryption Standard

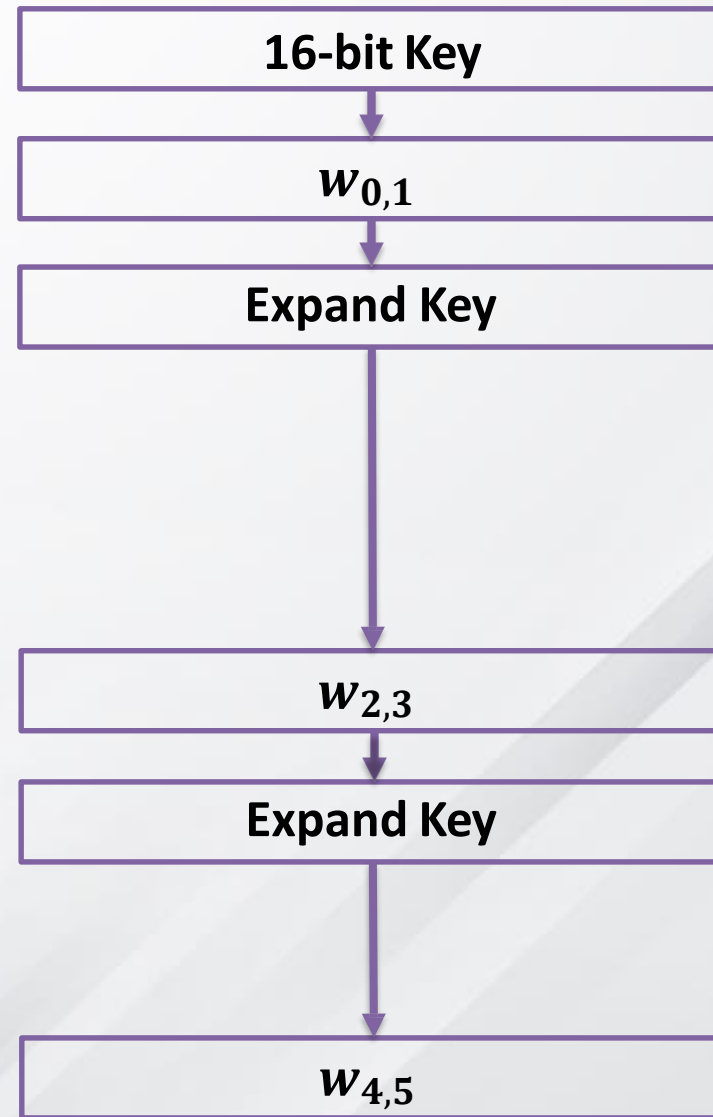
S-AES Encryption and Decryption

S-AES Key Generation

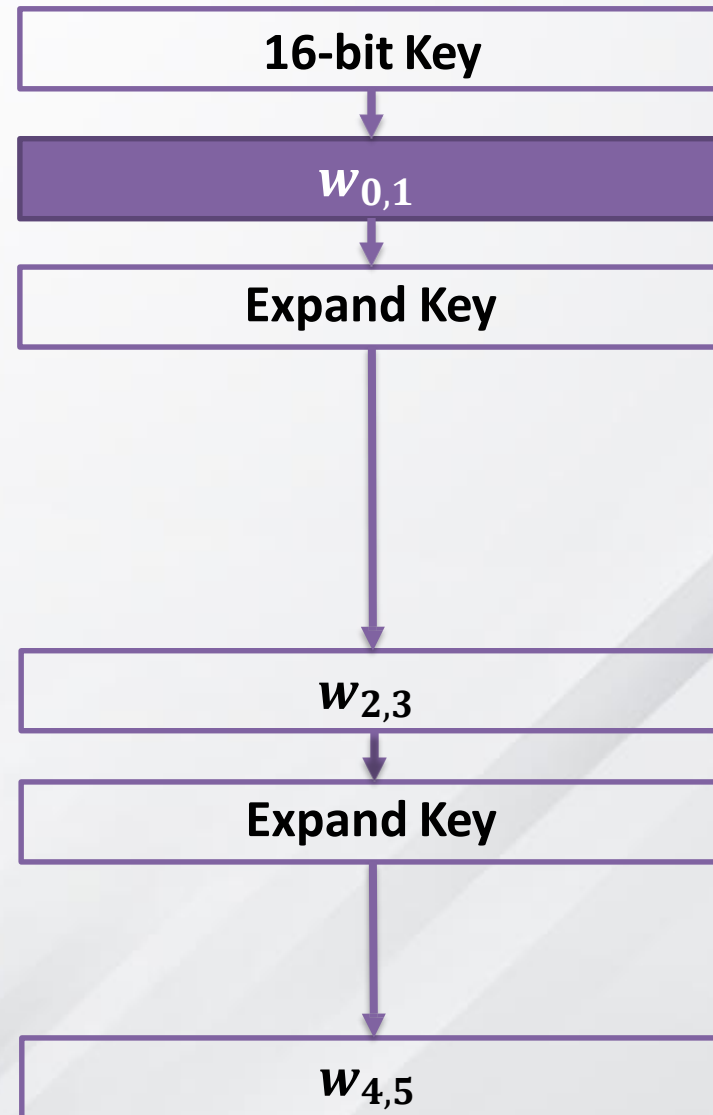
S-AES Encryption

S-AES Decryption

S-AES Key Generation



S-AES Key Generation



□ $K = 4A\ F5$

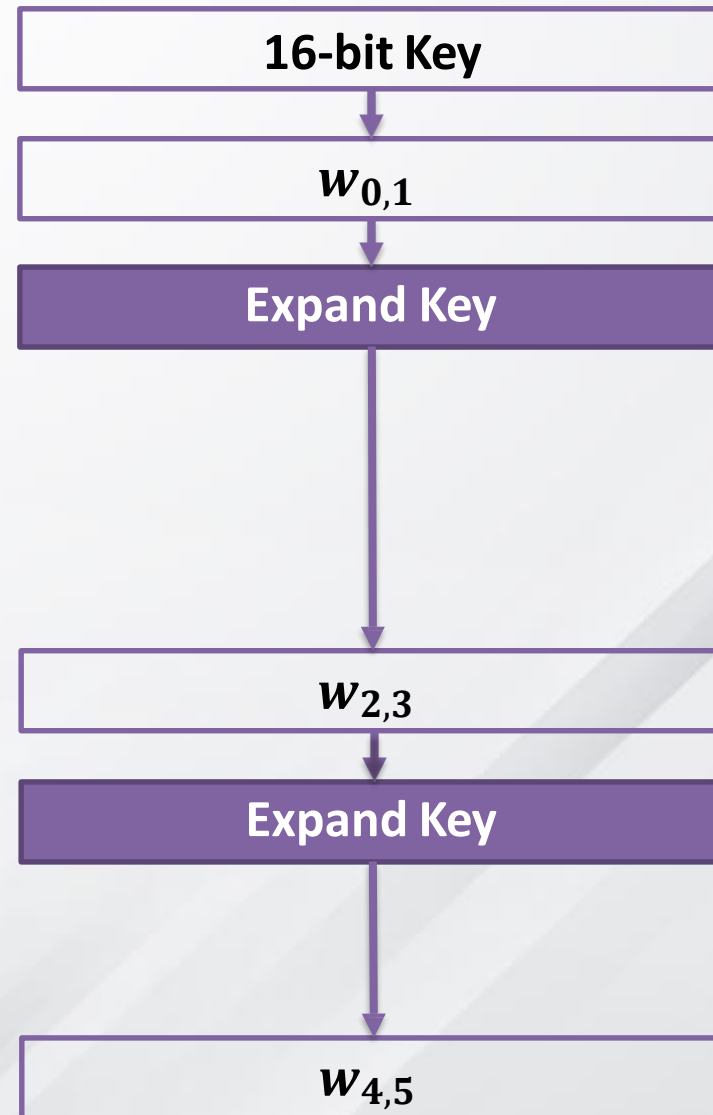
$= 0100\ 1010\ 1111\ 0101$

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

□ $w_0 = 0100\ 1010$

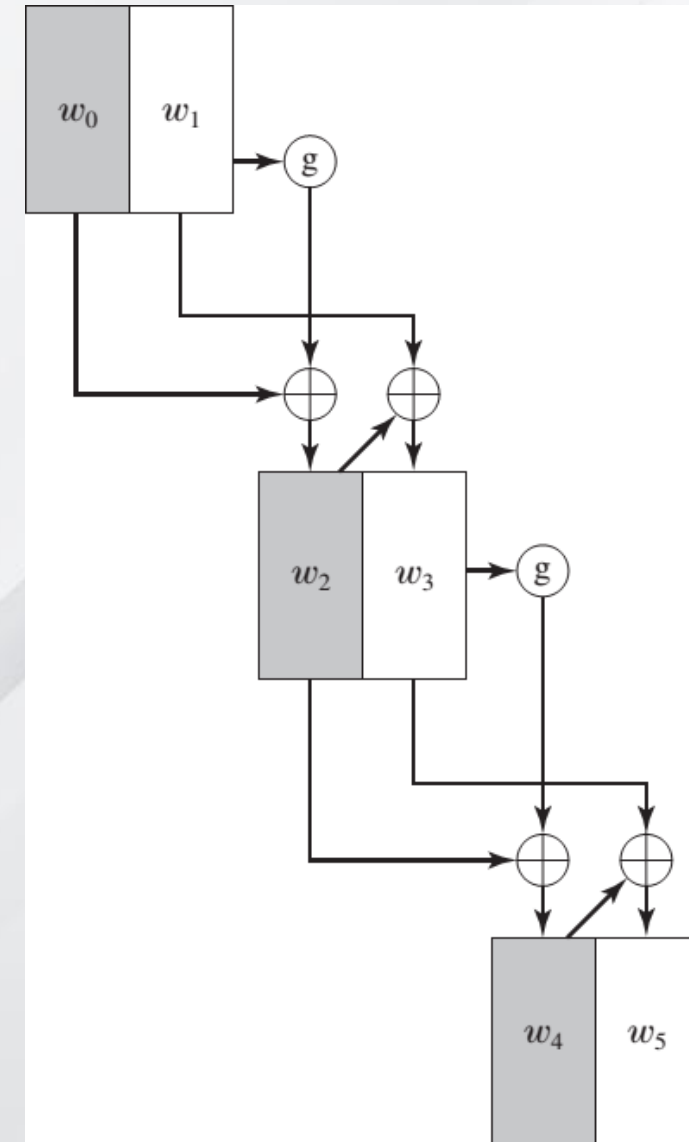
□ $w_1 = 1111\ 0101$

S-AES Key Generation



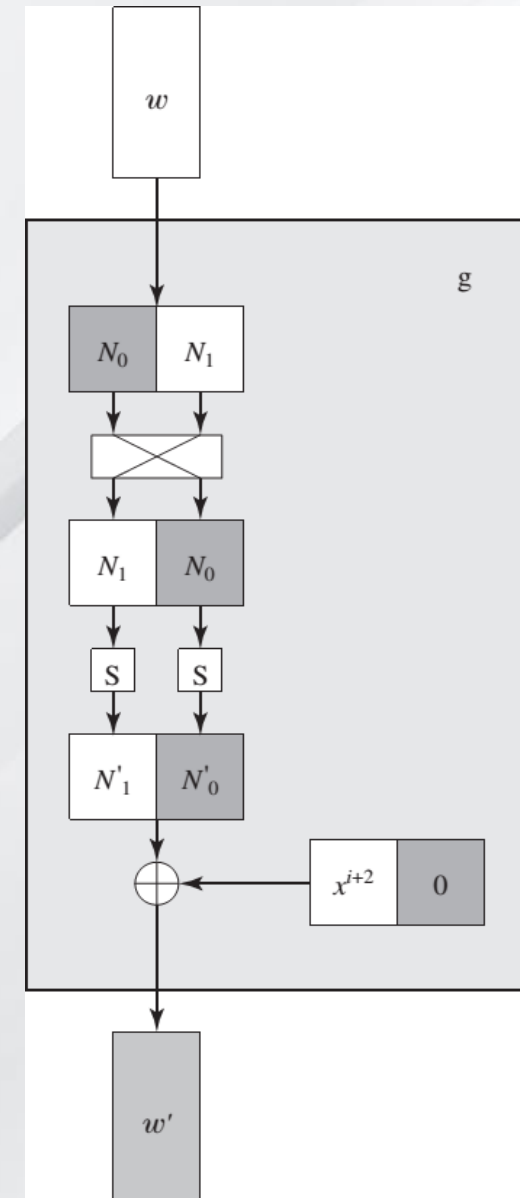
S-AES Key Generation

□ S-AES Key Expansion

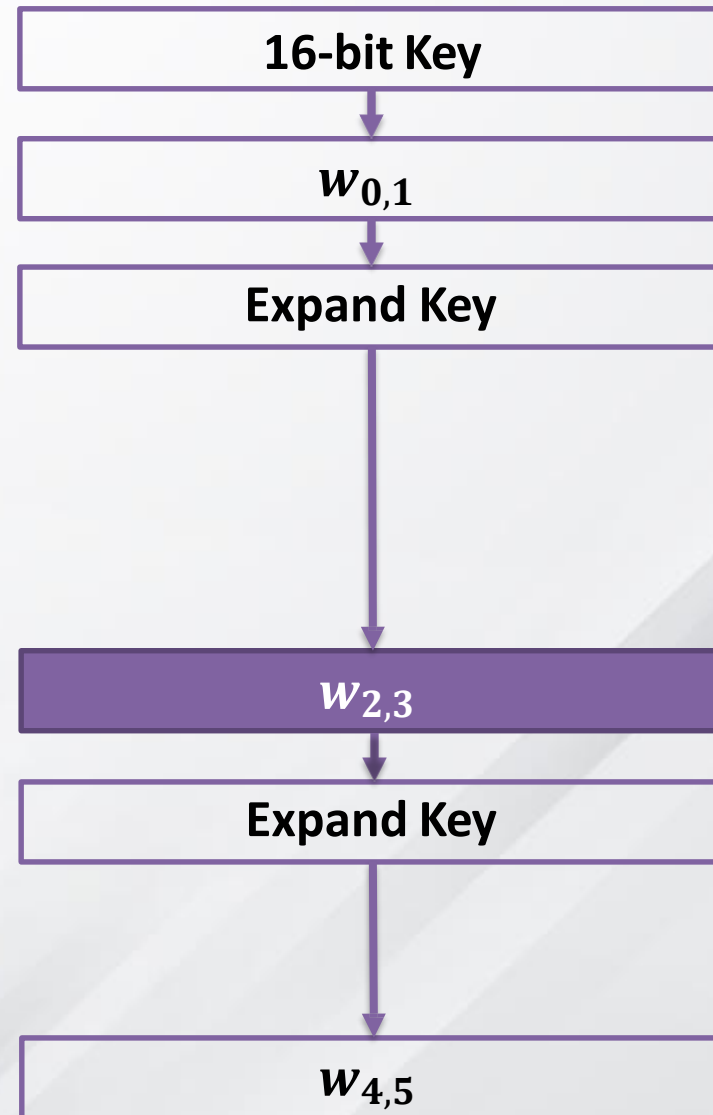


S-AES Key Generation

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

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

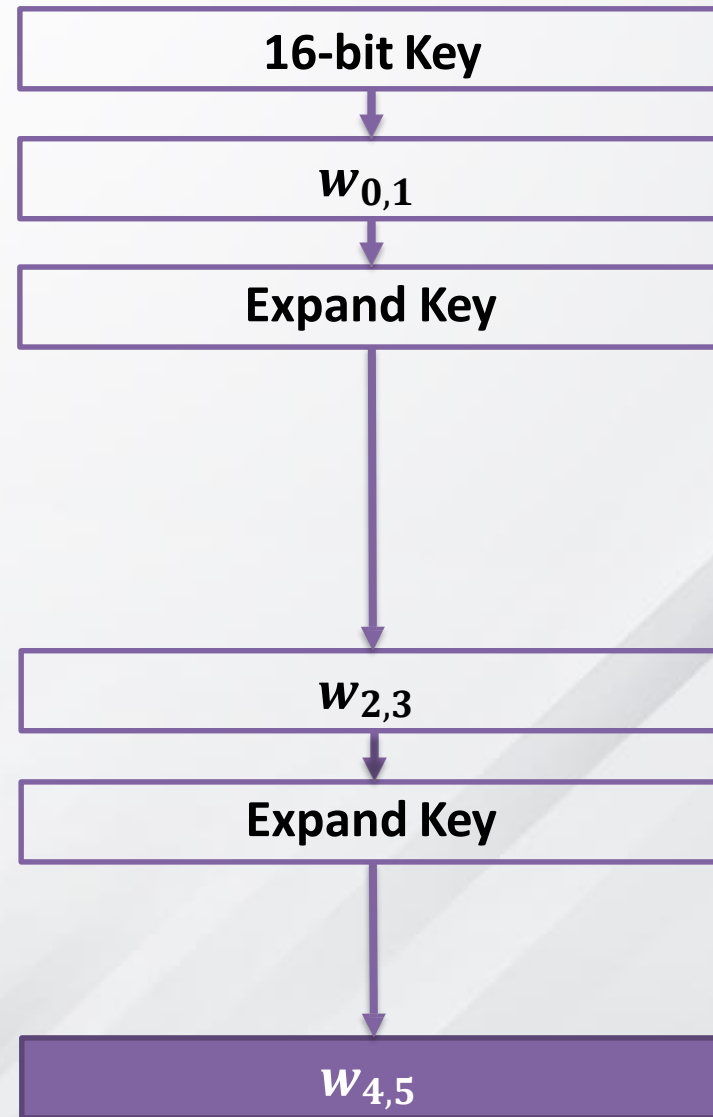
$$\begin{aligned}\square w_2 &= w_0 \oplus \text{Rcon}(1) \oplus \text{SubNib}(\text{RotNib}(w_1)) \\ &= 0100\ 1010 \oplus 1000\ 0000 \oplus 0001\ 0111 \\ &= 0100\ 1010 \oplus 1001\ 0111 = 1101\ 1101\end{aligned}$$

$$\square w_2 = 1101\ 1101$$

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

$$\square w_3 = 0010\ 1000$$

S-AES Key Generation



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

$$\square w_4 = w_2 \oplus \text{Rcon}(2) \oplus \text{SubNib}(\text{RotNib}(w_3))$$

$$\bullet = 1101\ 1101 \oplus 0011\ 0000 \oplus \text{SubNib}(1000\ 0010)$$

$$\bullet = 1101\ 1101 \oplus 0011\ 0000 \oplus 0110\ 1010$$

$$\bullet = 1101\ 1101 \oplus 0101\ 1010$$

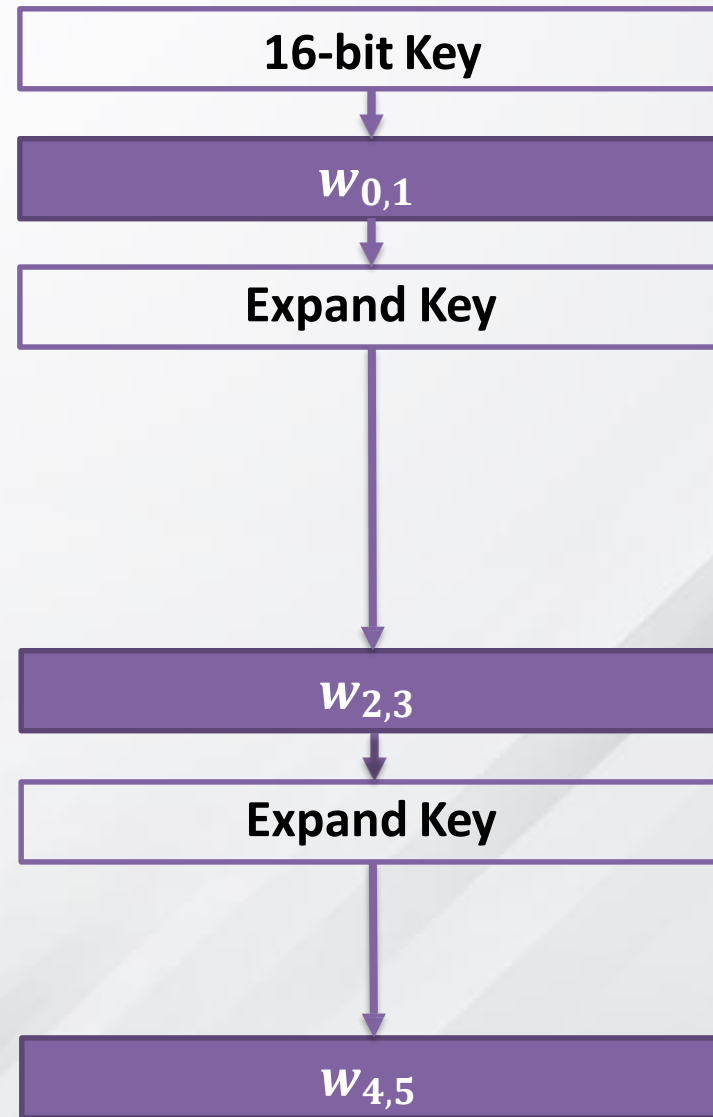
$$\square w_5 = w_4 \oplus w_3$$

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

$$= 1010\ 1111$$

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

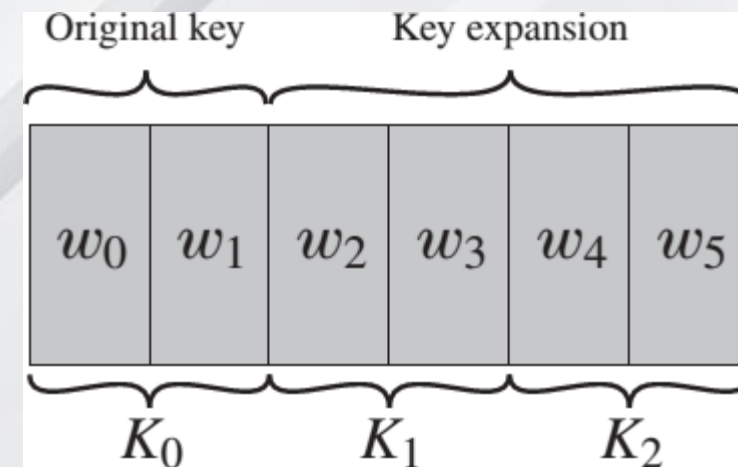
= 0100 1010 1111 0101

□ Key1 = w_2w_3

= 1101 1101 0010 1000

□ Key2 = w_4w_5

= 1000 0111 1010 1111



Simplified Advanced Encryption Standard

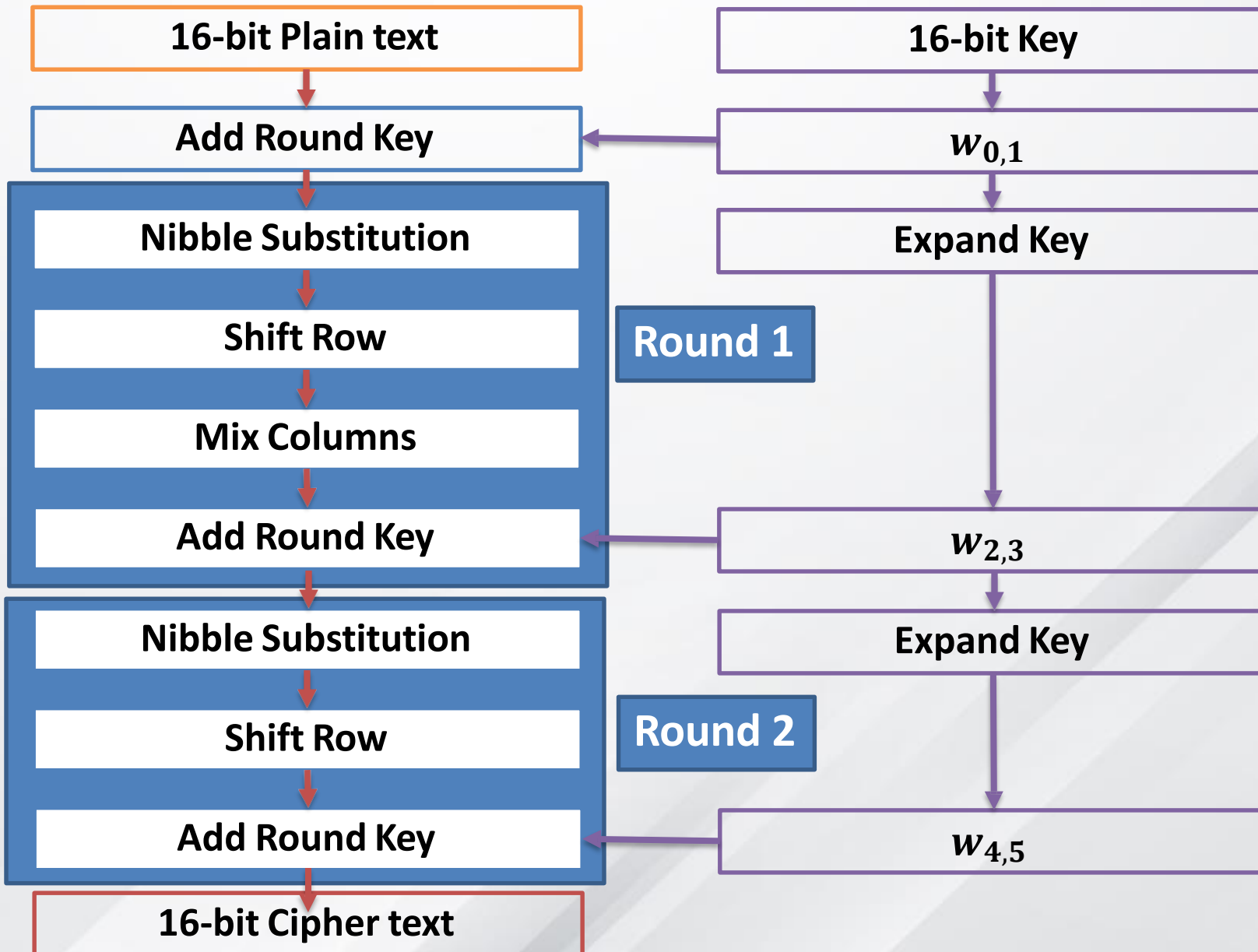
S-AES Encryption and Decryption

S-AES Key Generation

S-AES Encryption

S-AES Decryption

S-AES Encryption



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

❑ $\text{Key}_0 = w_0w_1$

$= 0100\ 1010\ 1111\ 0101$

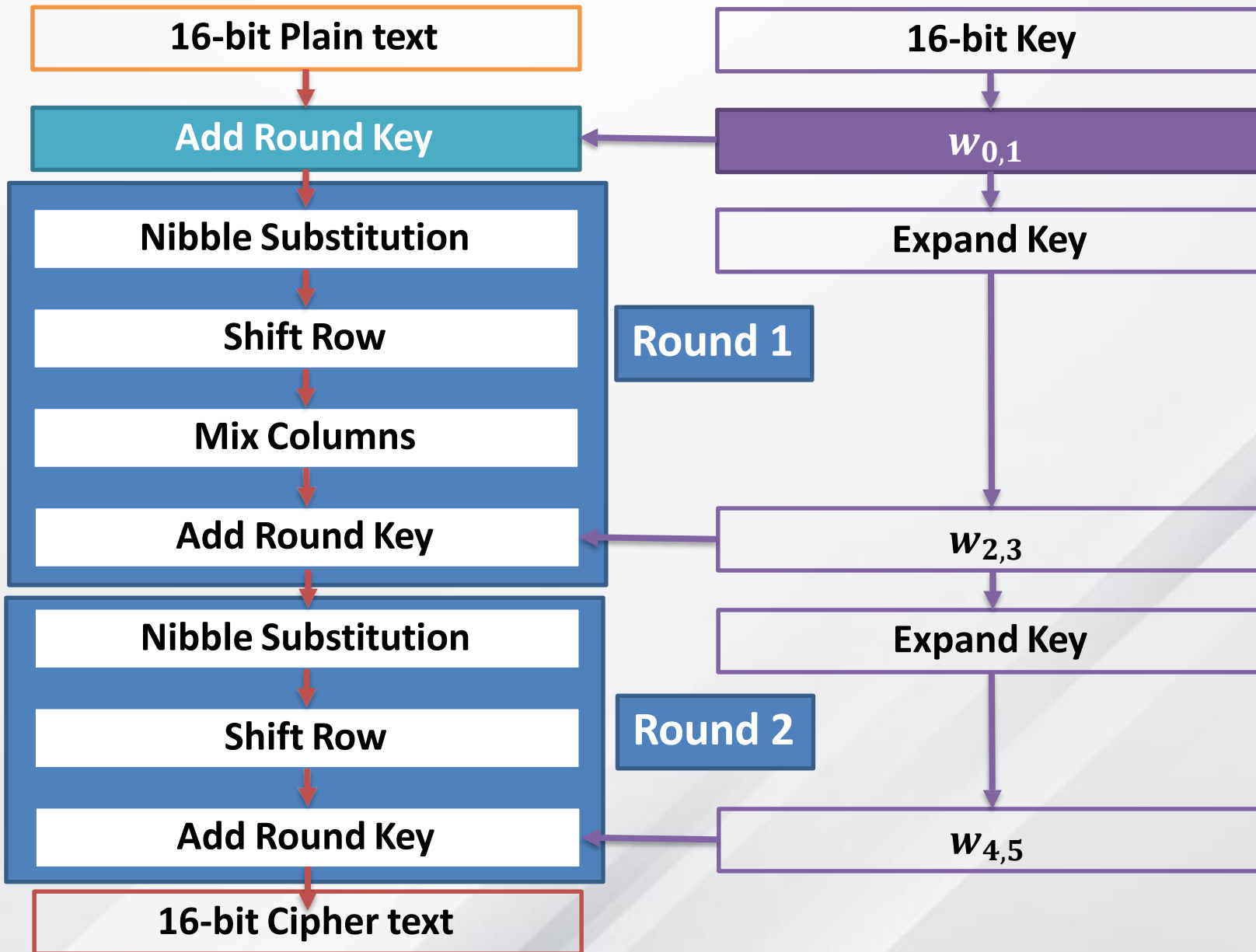
❑ $\text{Key}_1 = w_2w_3$

$= 1101\ 1101\ 0010\ 1000$

❑ $\text{Key}_2 = w_4w_5$

$= 1000\ 0111\ 1010\ 1111$

S-AES Encryption



❑ Round 0

❑ $P = 1101\ 0111\ 0010\ 1000$

❑ $Key0 = 0100\ 1010\ 1111\ 0101$

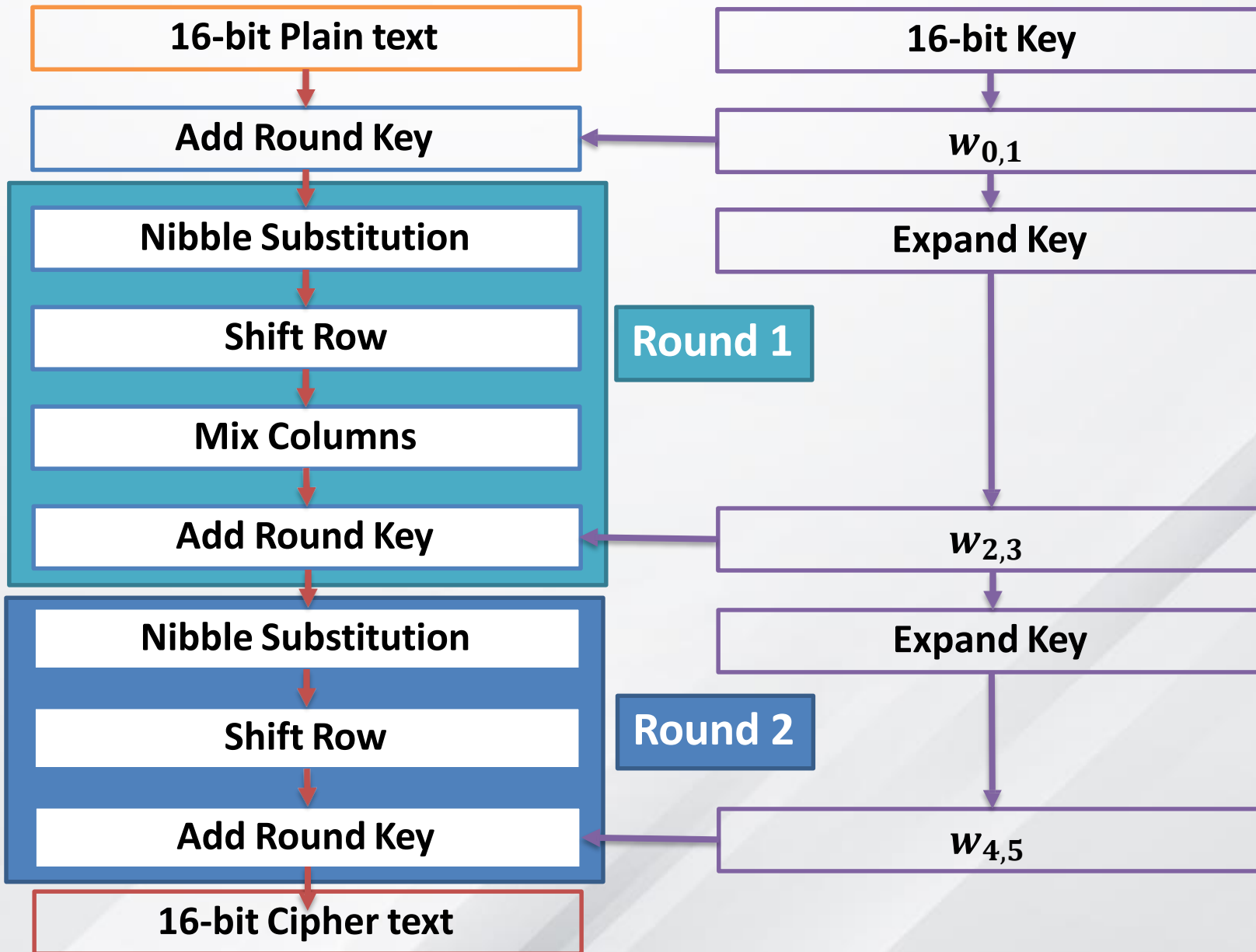
❑ $R0 = P \oplus Key0$

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

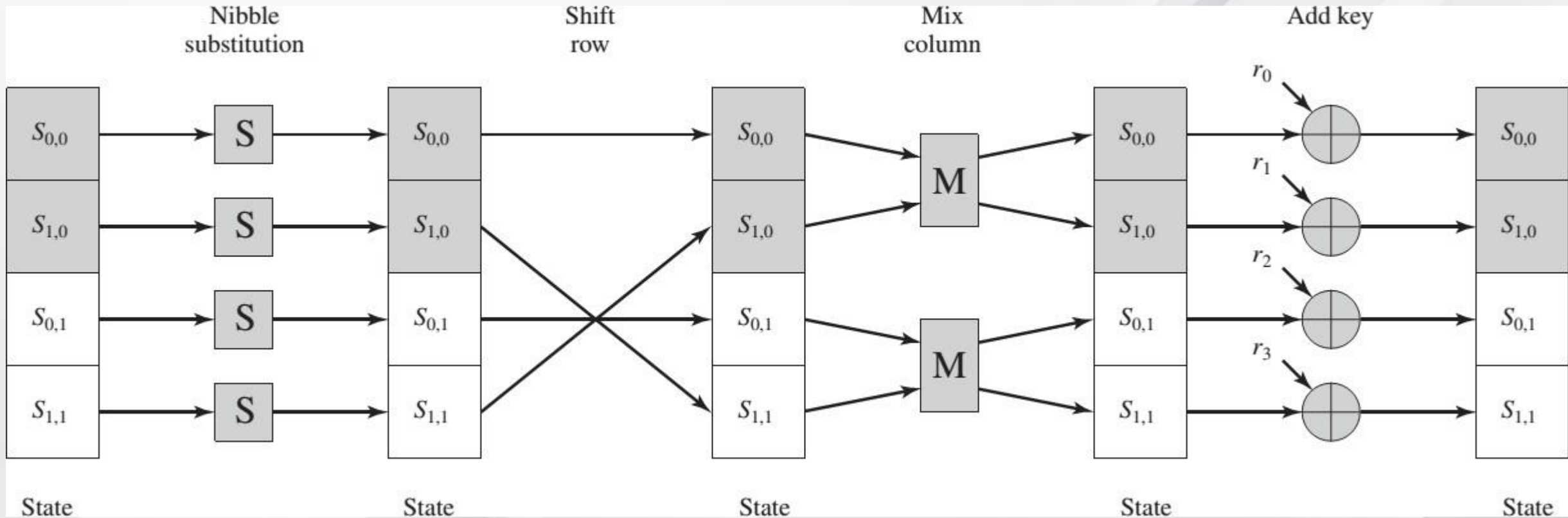
$0100\ 1010\ 1111\ 0101$

$= 1001\ 1101\ 1101\ 1101$

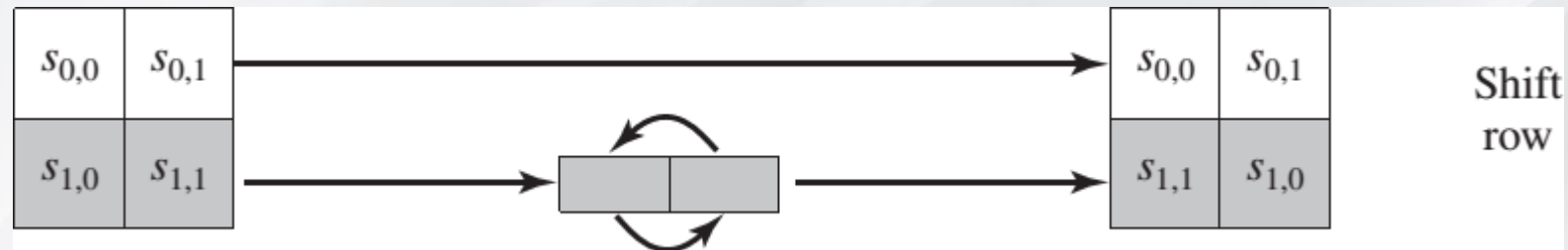
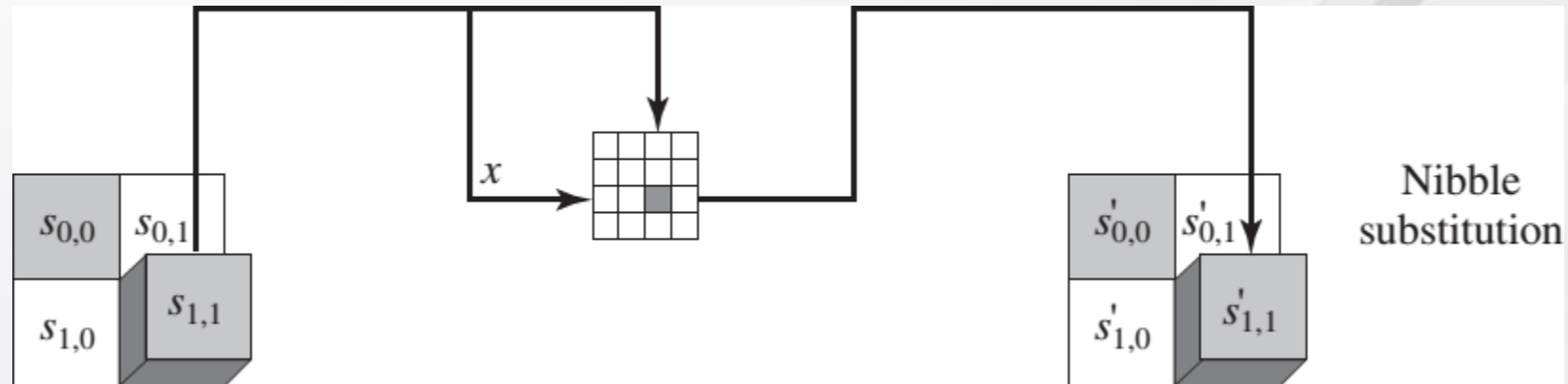
S-AES Encryption



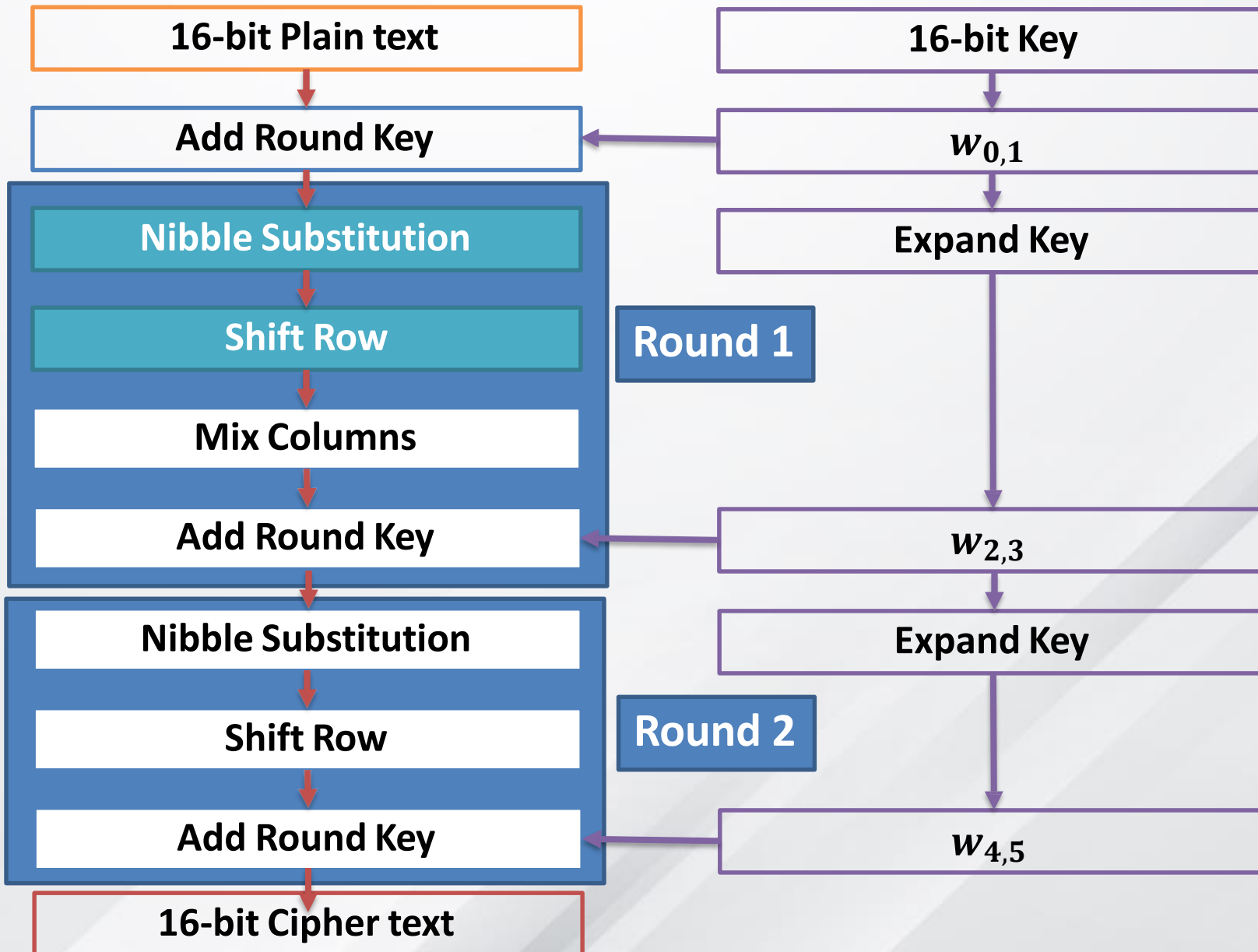
□ S-AES Encryption Round



□ S-AES Transformation (Substitution and Shift row)



S-AES Encryption



□ Round 1

1) Nibble Substitution :

□ SubNib(1001 1101 1101 1101) = 0010 1110 1110 1110

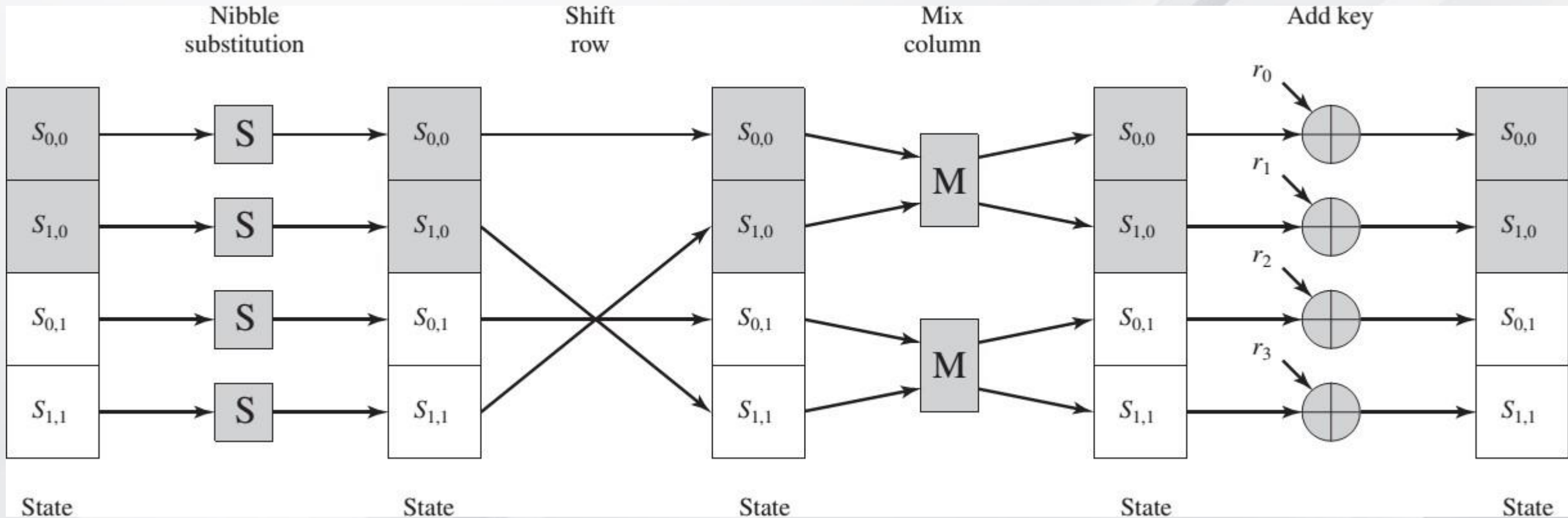
2) Shift Row:

□ Swap 2nd nibble and 4th nibble

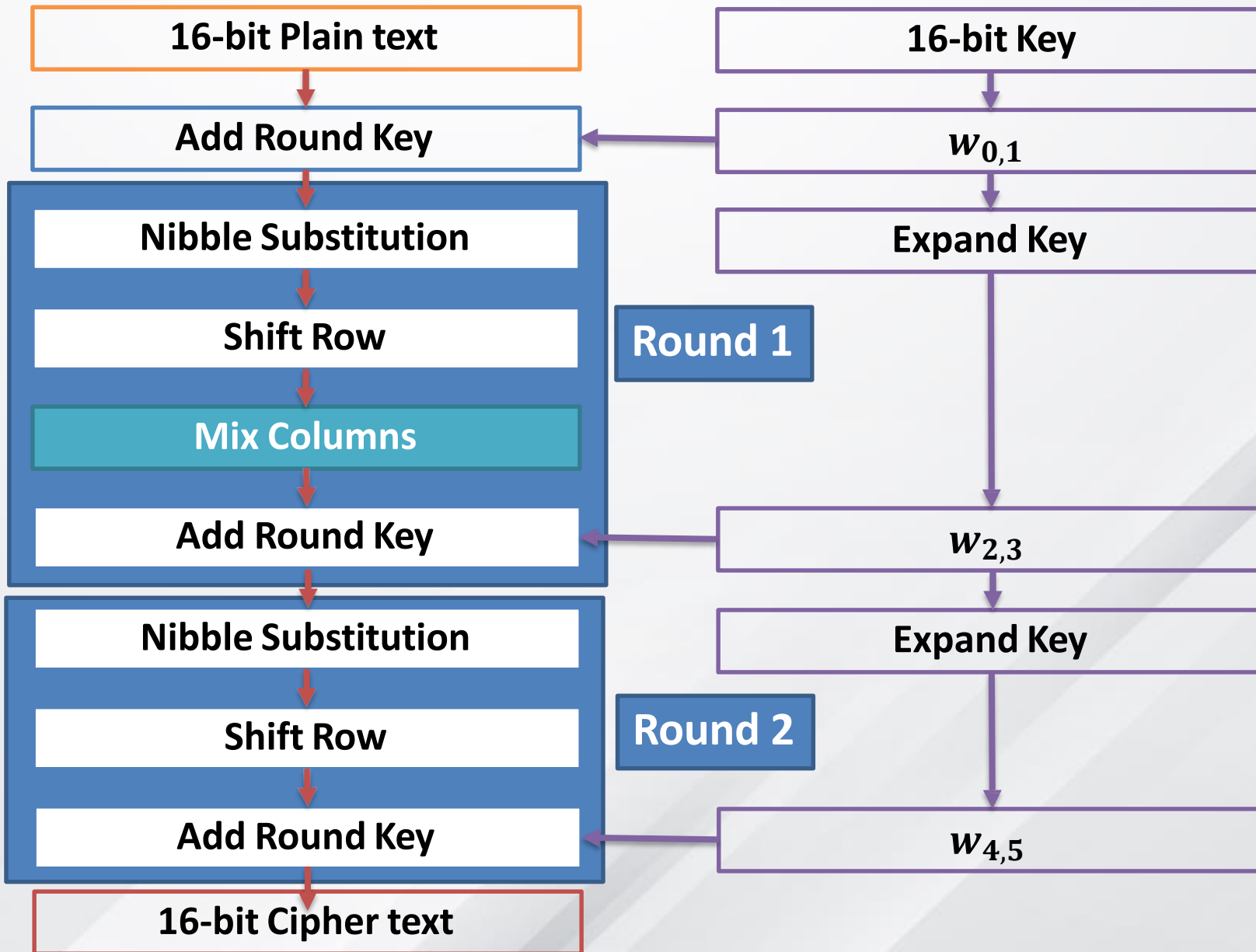
□ ShRow(0010 1110 1110 1110)
= 0010 1110 1110 1110

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

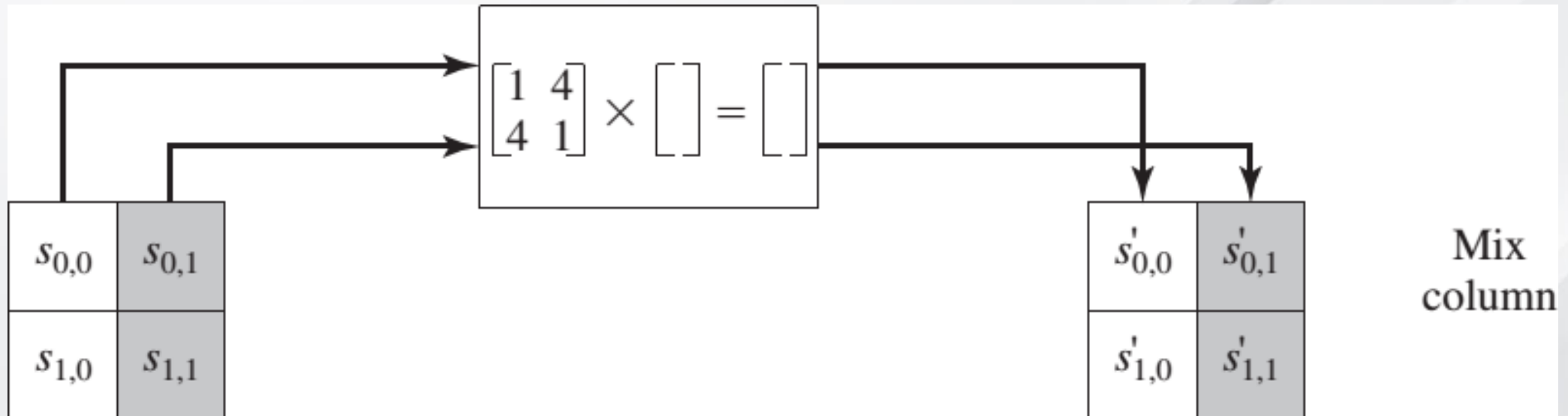
□ S-AES Encryption Round



S-AES Encryption



□ S-AES Transformation (Mix Column)



❑ 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

□ 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

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

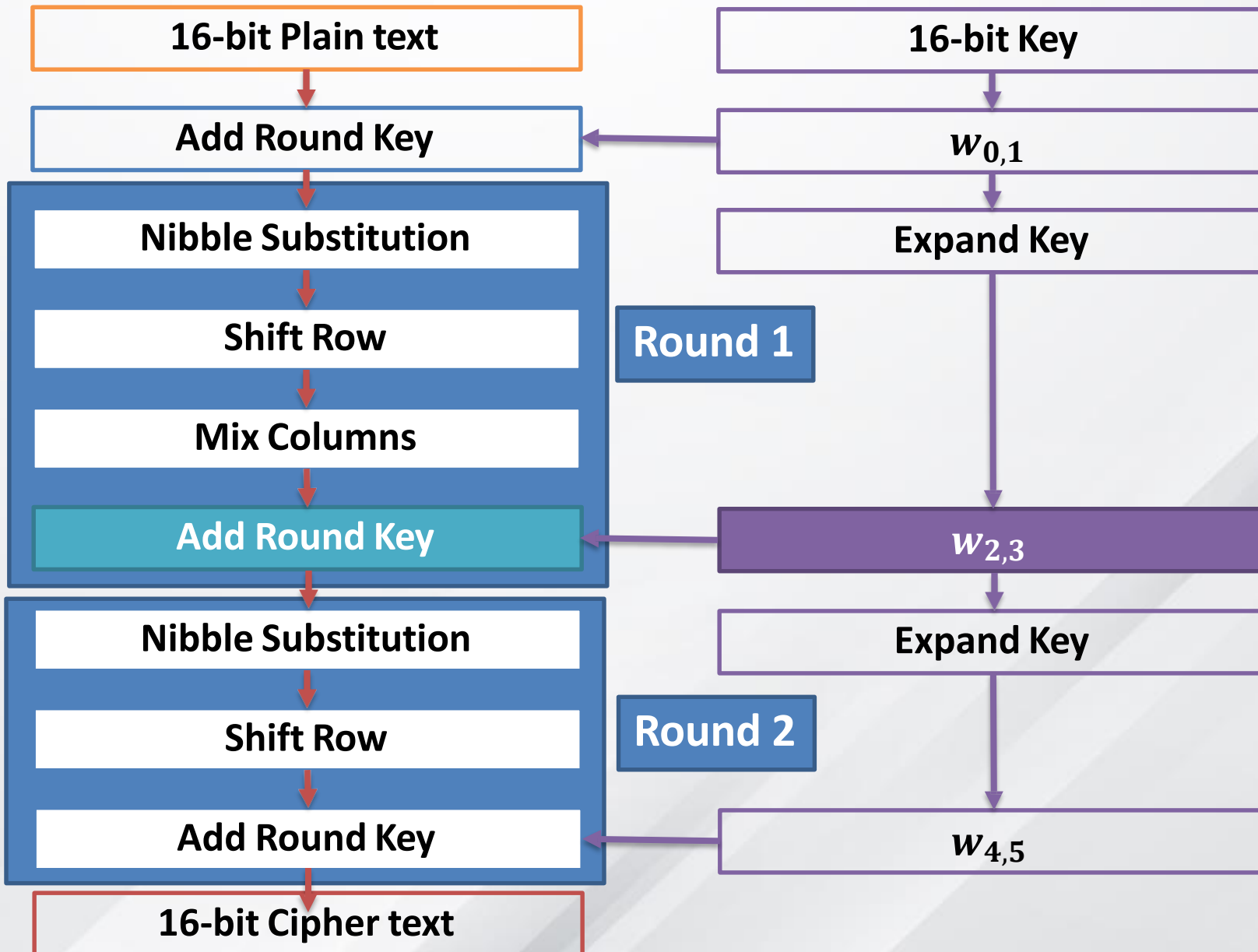
$$\square = \begin{pmatrix} 2 & E \\ E & E \end{pmatrix} * \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} (2*1 \oplus E*4) & (E*1 \oplus E*4) \\ (2*4 \oplus E*1) & (E*4 \oplus E*1) \end{pmatrix}$$

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

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

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

S-AES Encryption



□ Round 1

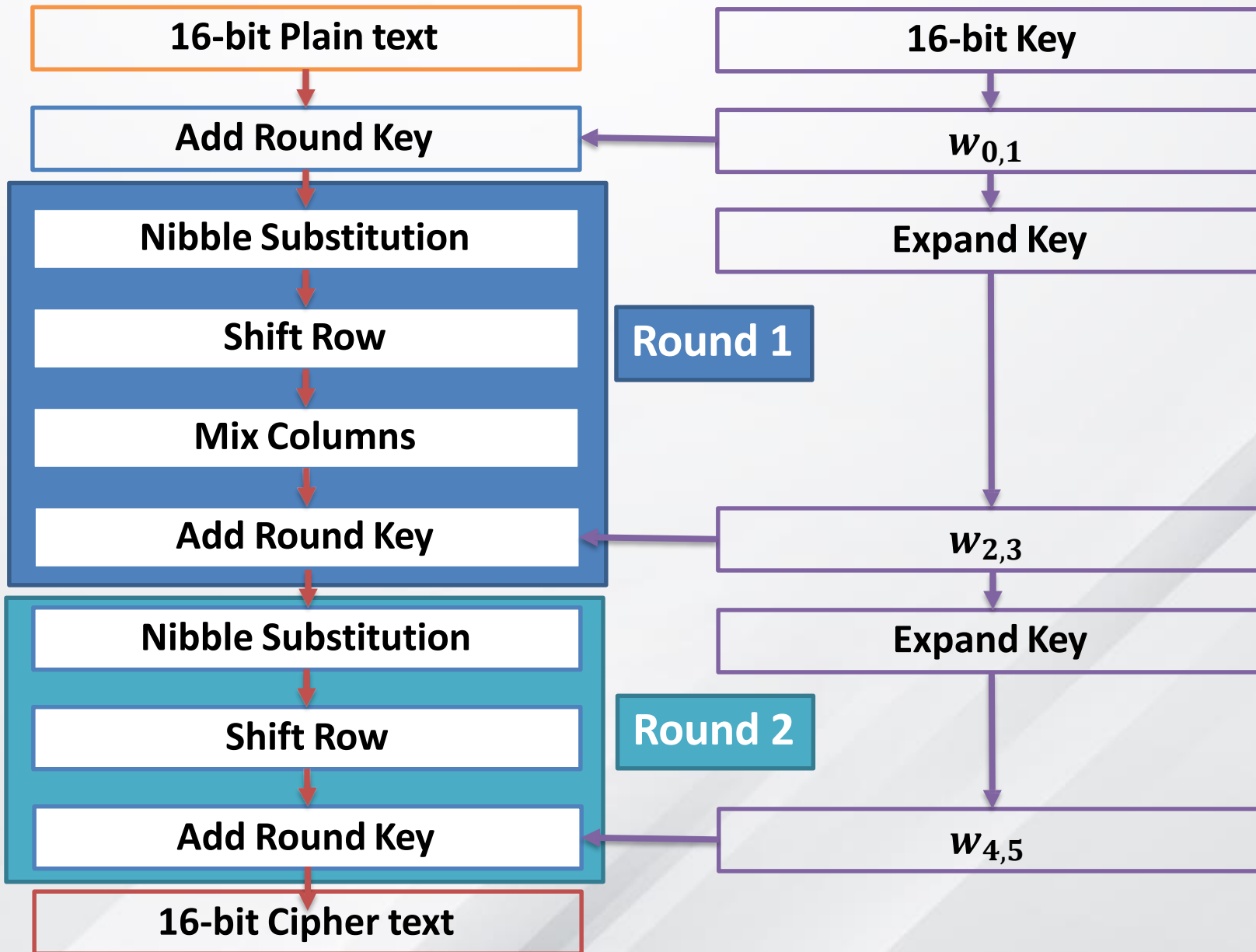
4) Add round Key1

□ Key1 = 1101 1101 0010 1000

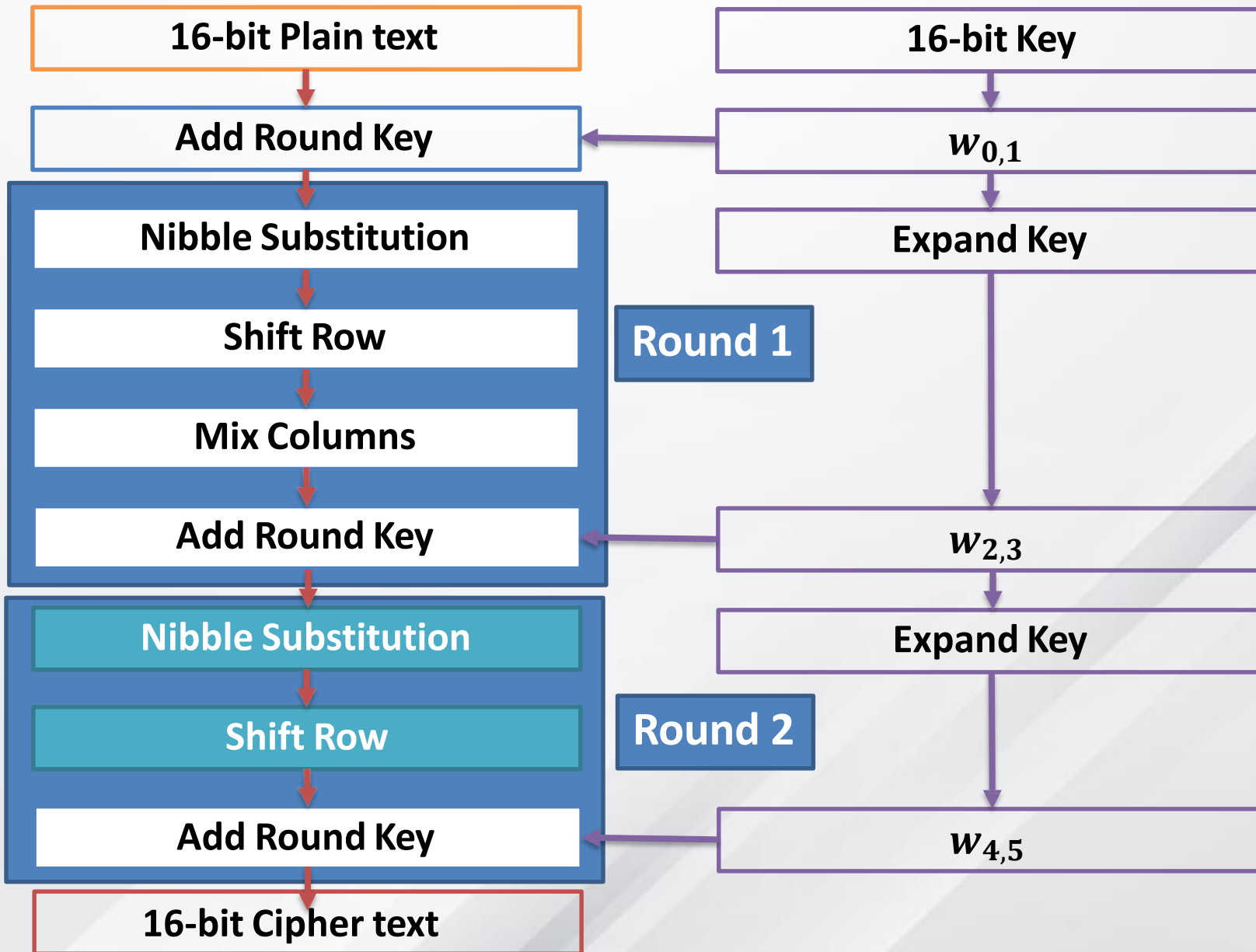
□ R1= Key1 $\oplus$ MixCol(ShRow(SubNib(R0)))

$$= 1101\ 1101\ 0010\ 1000 \oplus 1111\ 0110\ 0011\ 0011$$
$$= 0010\ 1011\ 0001\ 1011$$

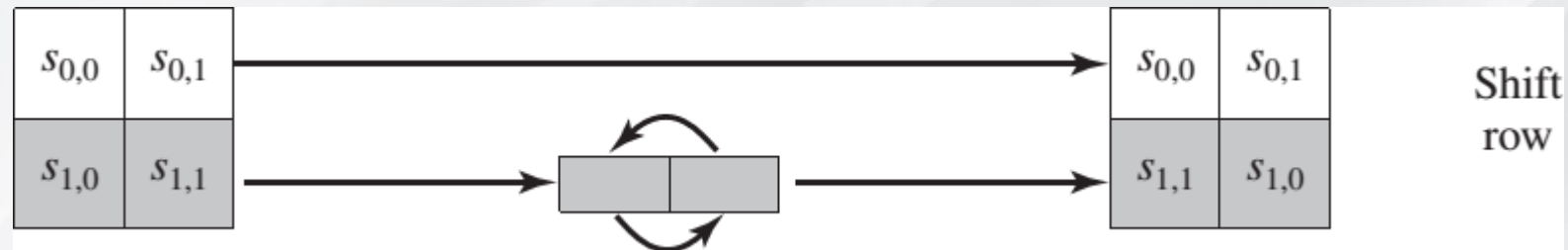
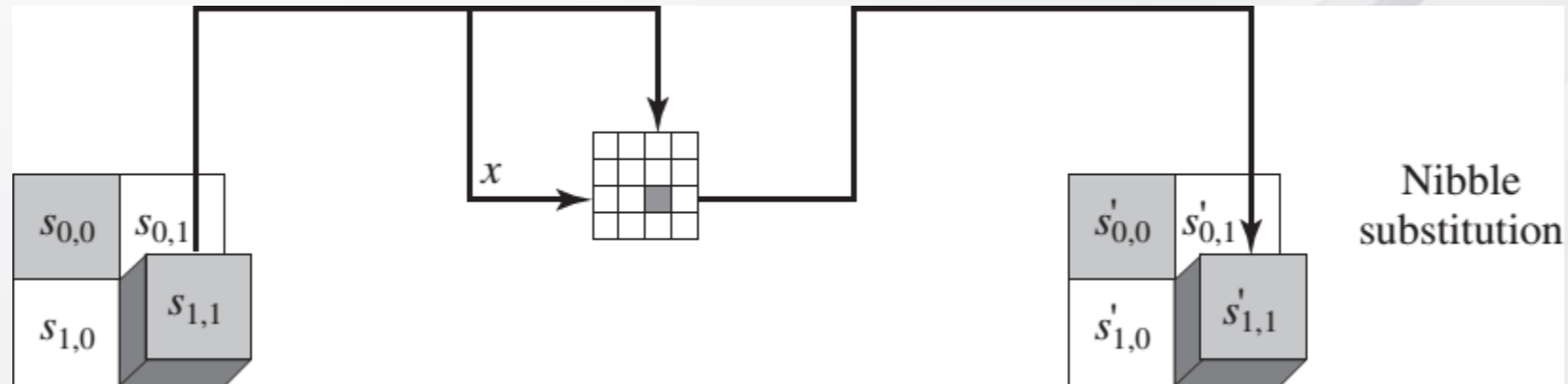
S-AES Encryption



S-AES Encryption



□ S-AES Transformation (Substitution and Shift row)



□ Round 2

1) Nibble Substitution :

□ SubNib(0010 1011 0001 1011) = 1010 0011 0100 0011

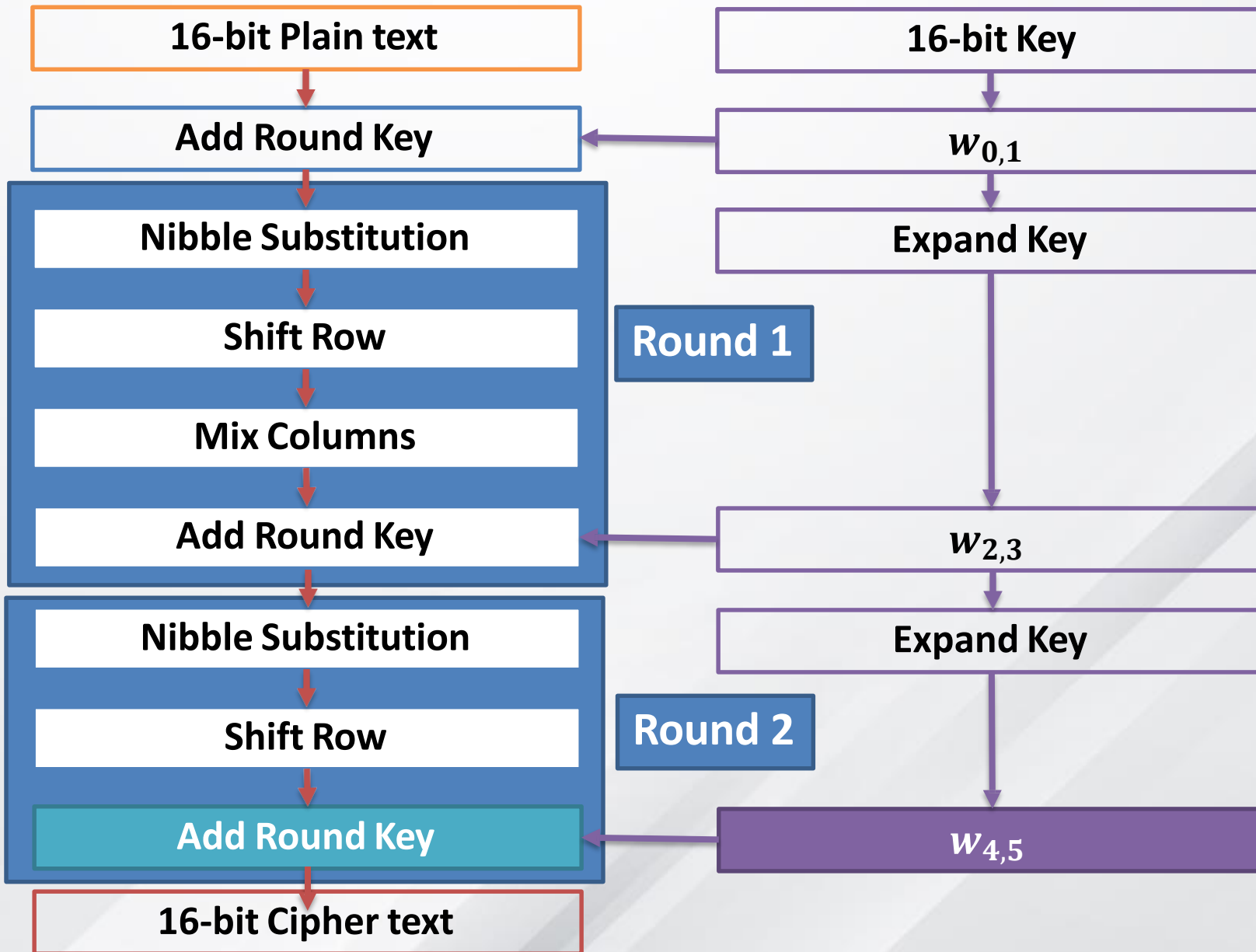
2) Shift Row:

□ Swap 2nd nibble and 4th nibble

□ ShRow(1010 0011 0100 0011)
= 1010 0011 0100 0011

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



□ Round 2

4) Add round Key2

□ Key2 = 1000 0111 1010 1111

□ R2= Key2 $\oplus$ ShRow(SubNib(R1))

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

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

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

Simplified Advanced Encryption Standard

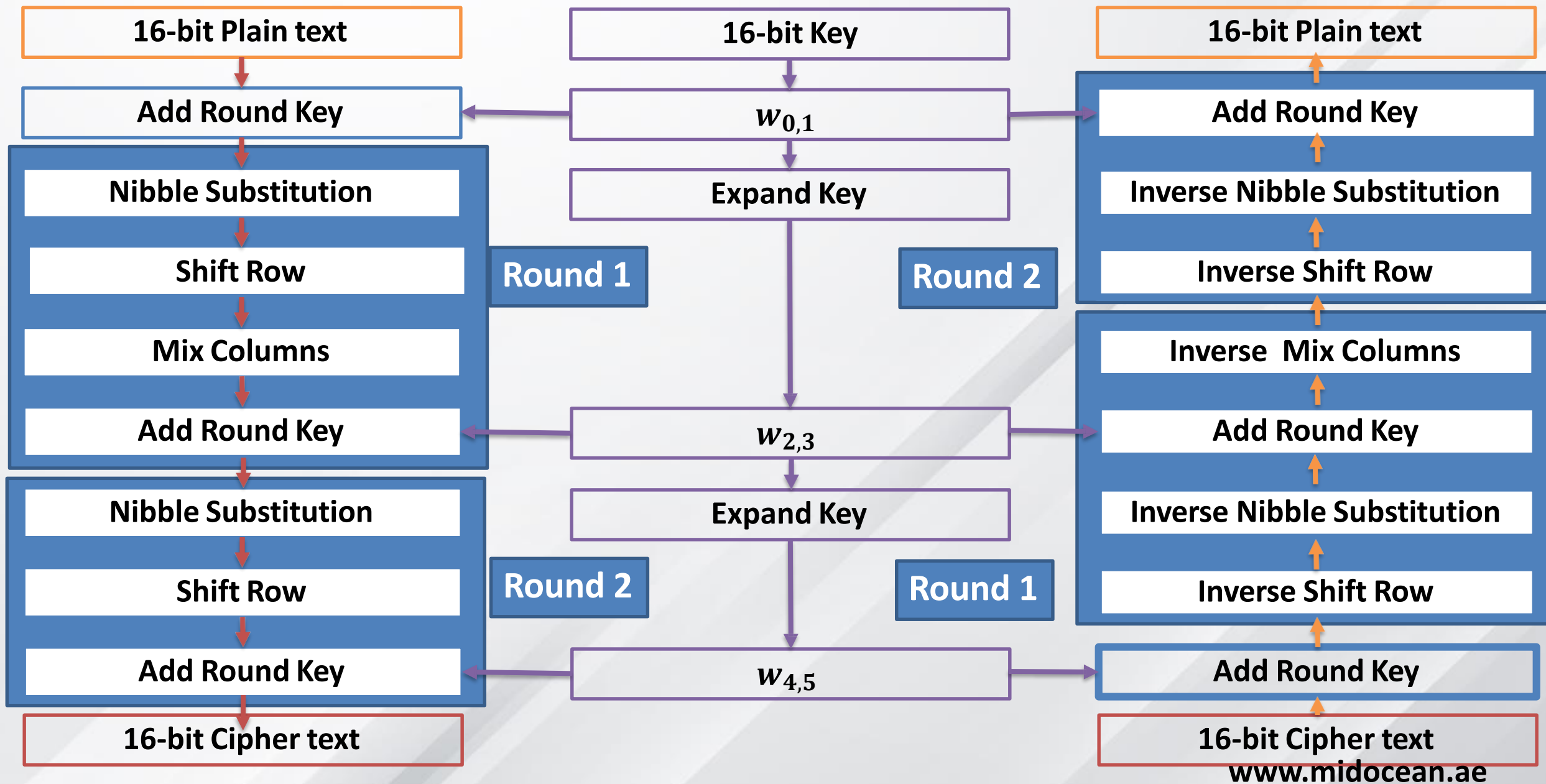
S-AES Encryption and Decryption

S-AES Key Generation

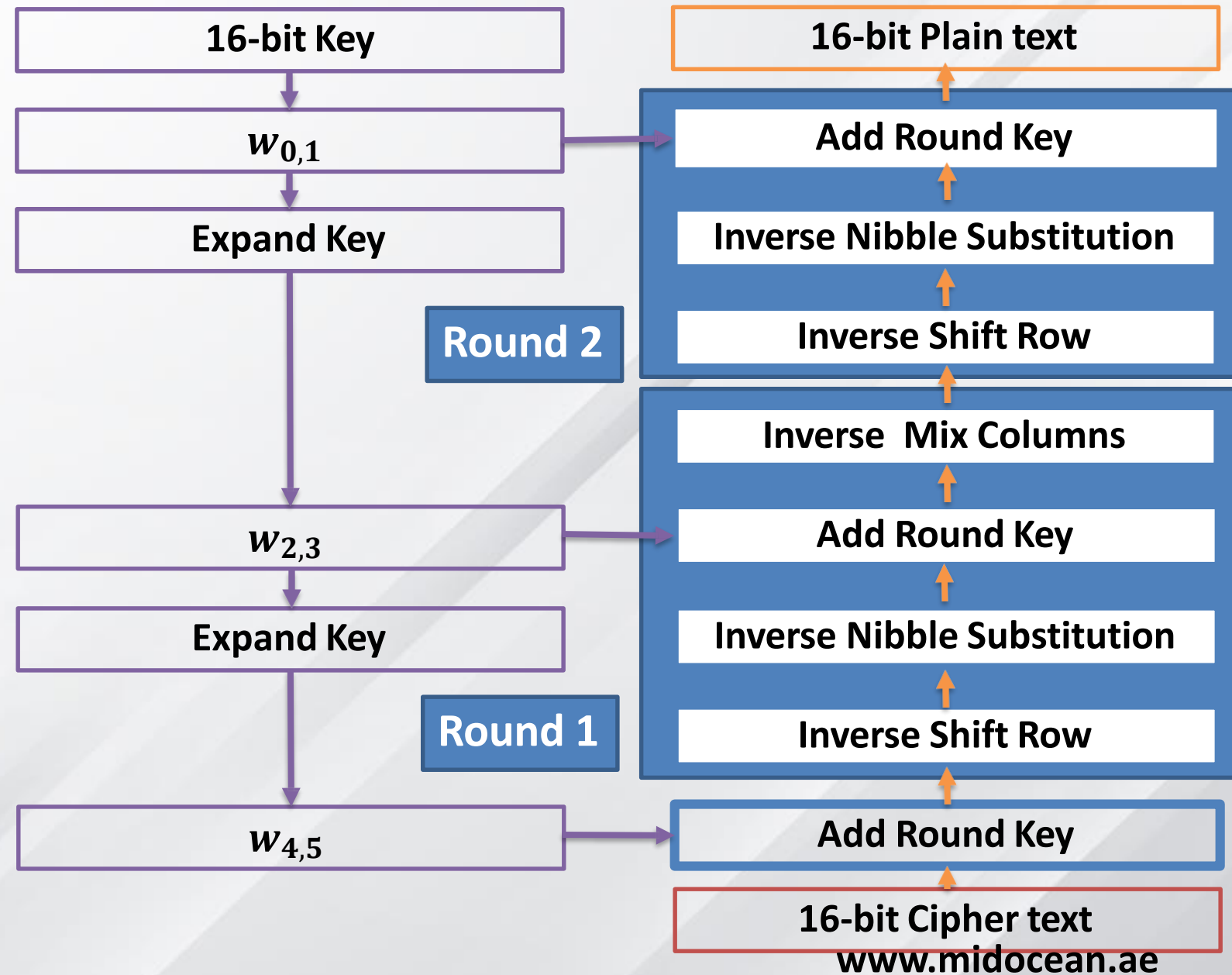
S-AES Encryption

S-AES Decryption

S-AES Encryption and Decryption



S-AES Decryption



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

❑ $\text{Key}_0 = w_0w_1$

$= 0100\ 1010\ 1111\ 0101$

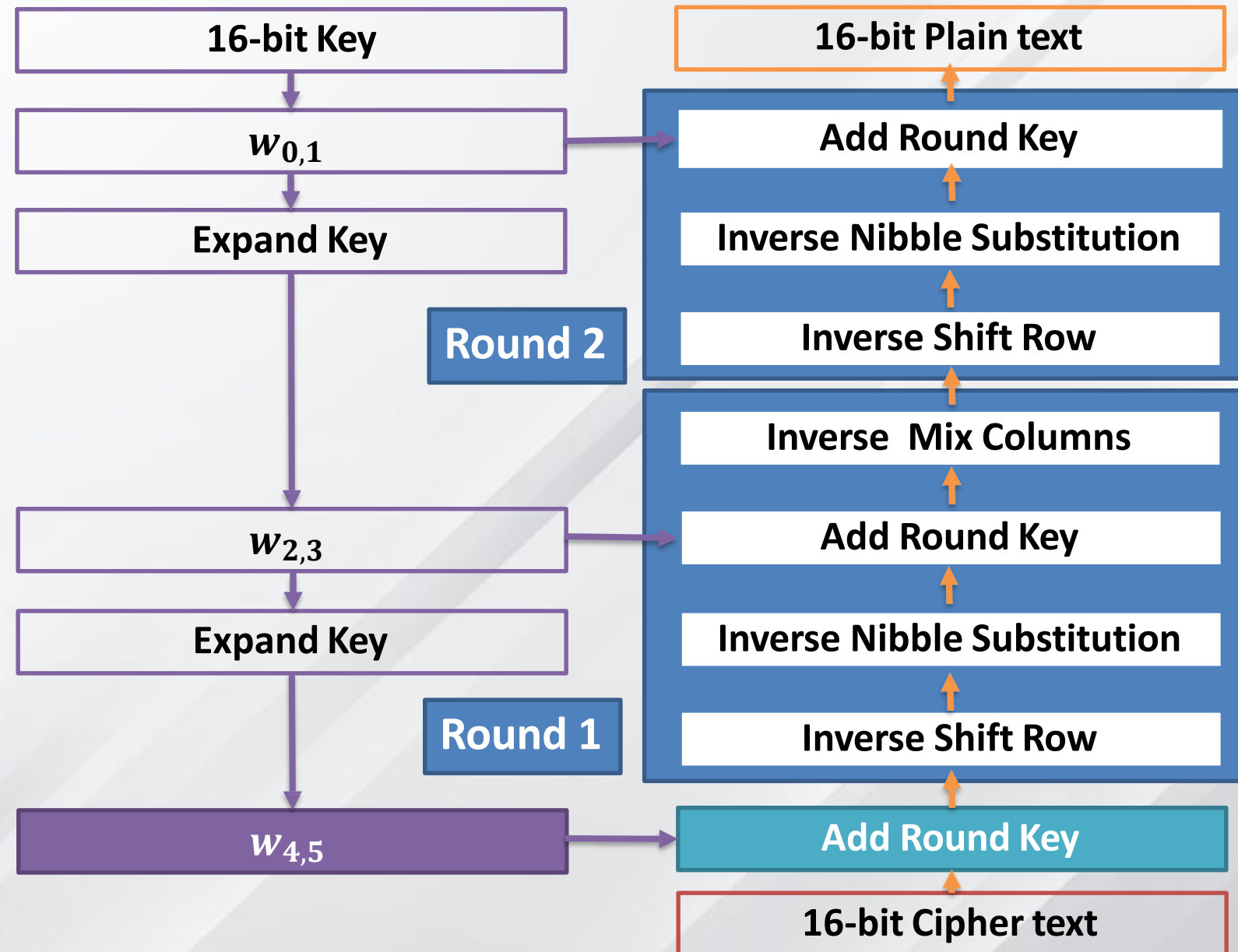
❑ $\text{Key}_1 = w_2w_3$

$= 1101\ 1101\ 0010\ 1000$

❑ $\text{Key}_2 = w_4w_5$

$= 1000\ 0111\ 1010\ 1111$

S-AES Decryption



$$\square \text{Key2} = w4w5$$

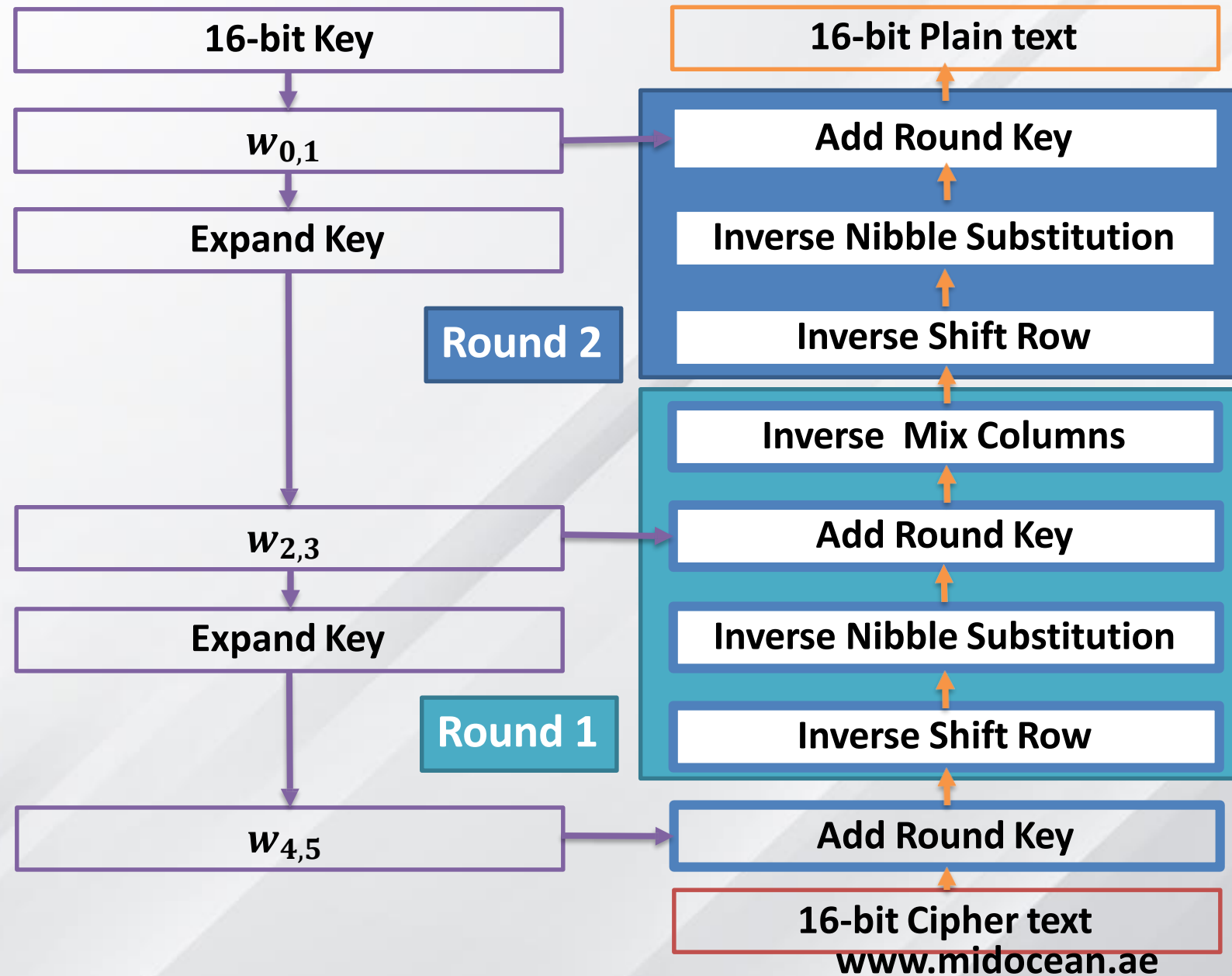
$$= 1000 \ 0111 \ 1010 \ 1111$$

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

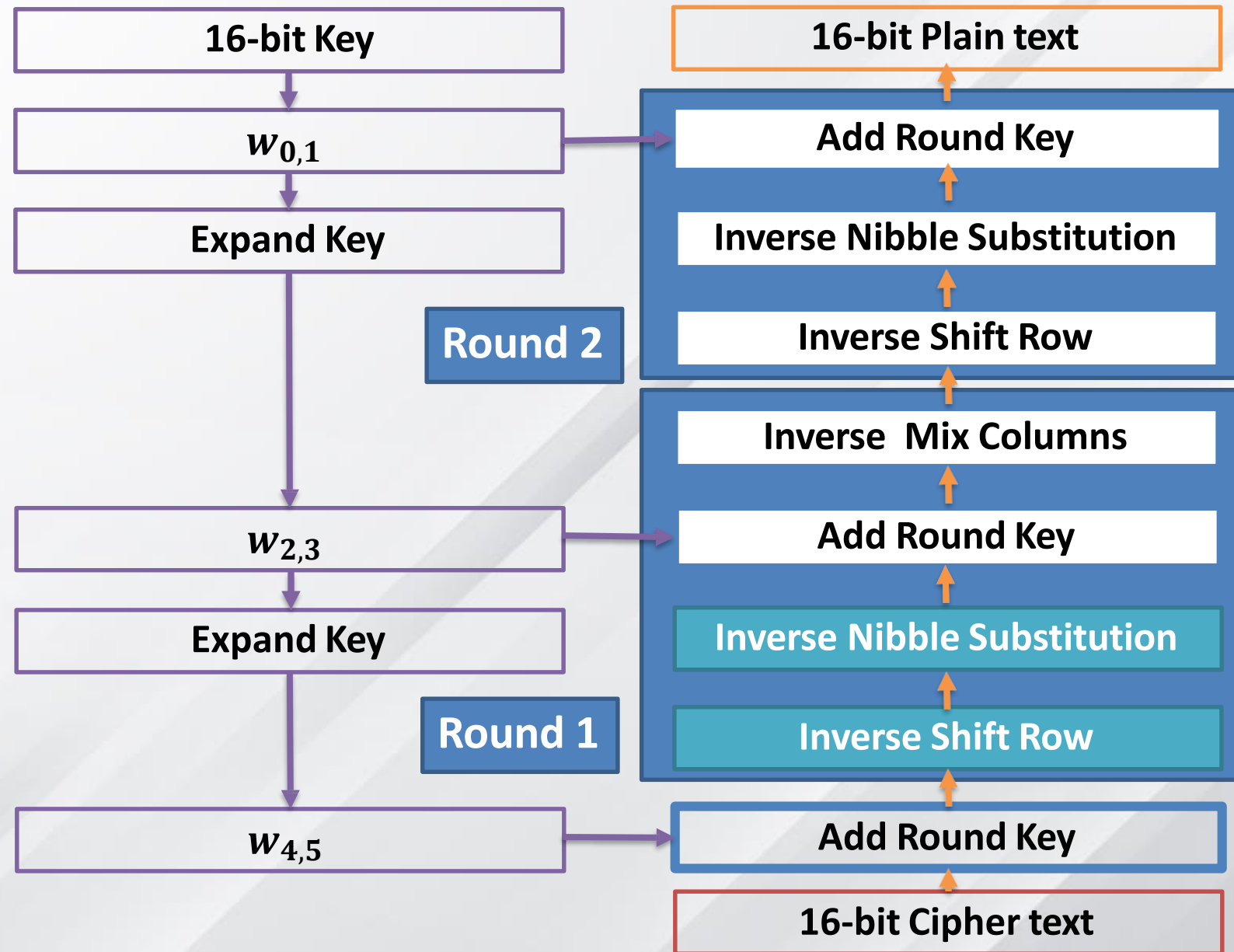
$$\square R0 = C \oplus \text{Key2} = 0010 \ 0100 \ 1110 \ 1100 \oplus 1000 \ 0111 \ 1010 \ 1111$$

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

S-AES Decryption



S-AES Decryption



□ Round 1

1) Inverse Shift Row

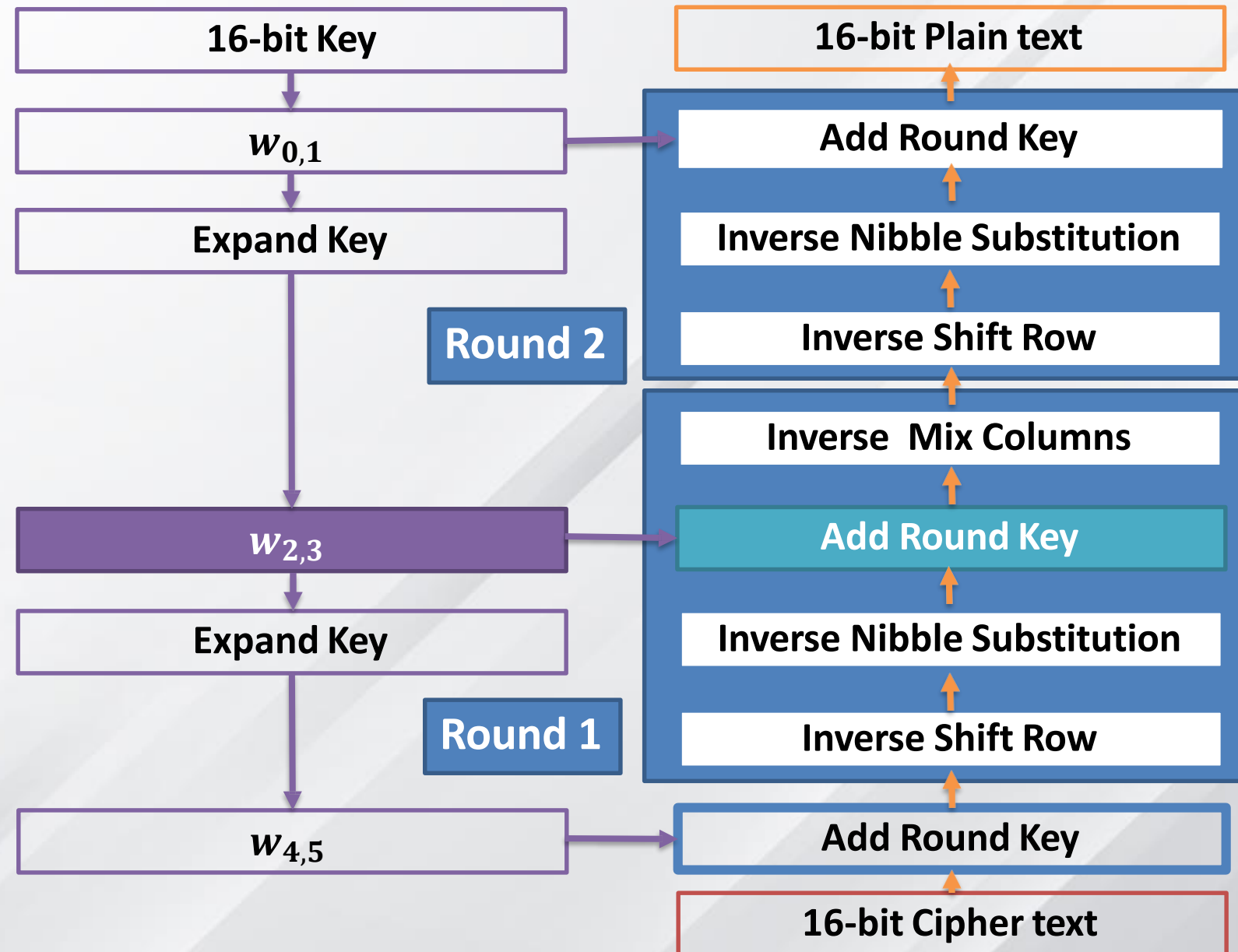
$$\begin{aligned} \square \text{IShRow}(R_0) &= \text{IShRow}(1010 \text{ } 0011 \text{ } 0100 \text{ } 0011) = \\ &= 1010 \text{ } 0011 \text{ } 0100 \text{ } 0011 \end{aligned}$$

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



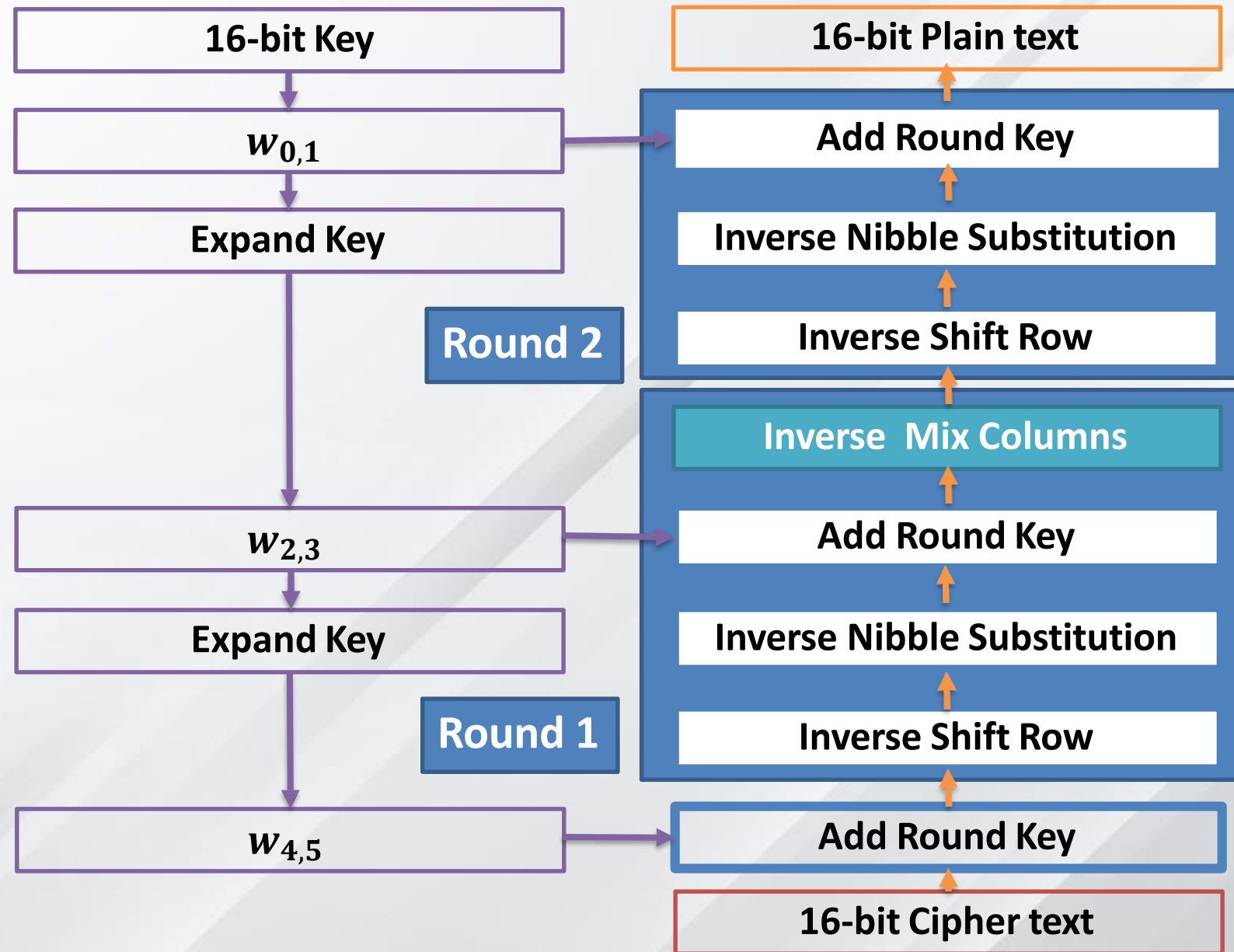
3) Add Round 1 Key

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

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

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

S-AES Decryption



S-AES Decryption

❑ Round 1

4) Inverse Mix Columns :

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

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

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

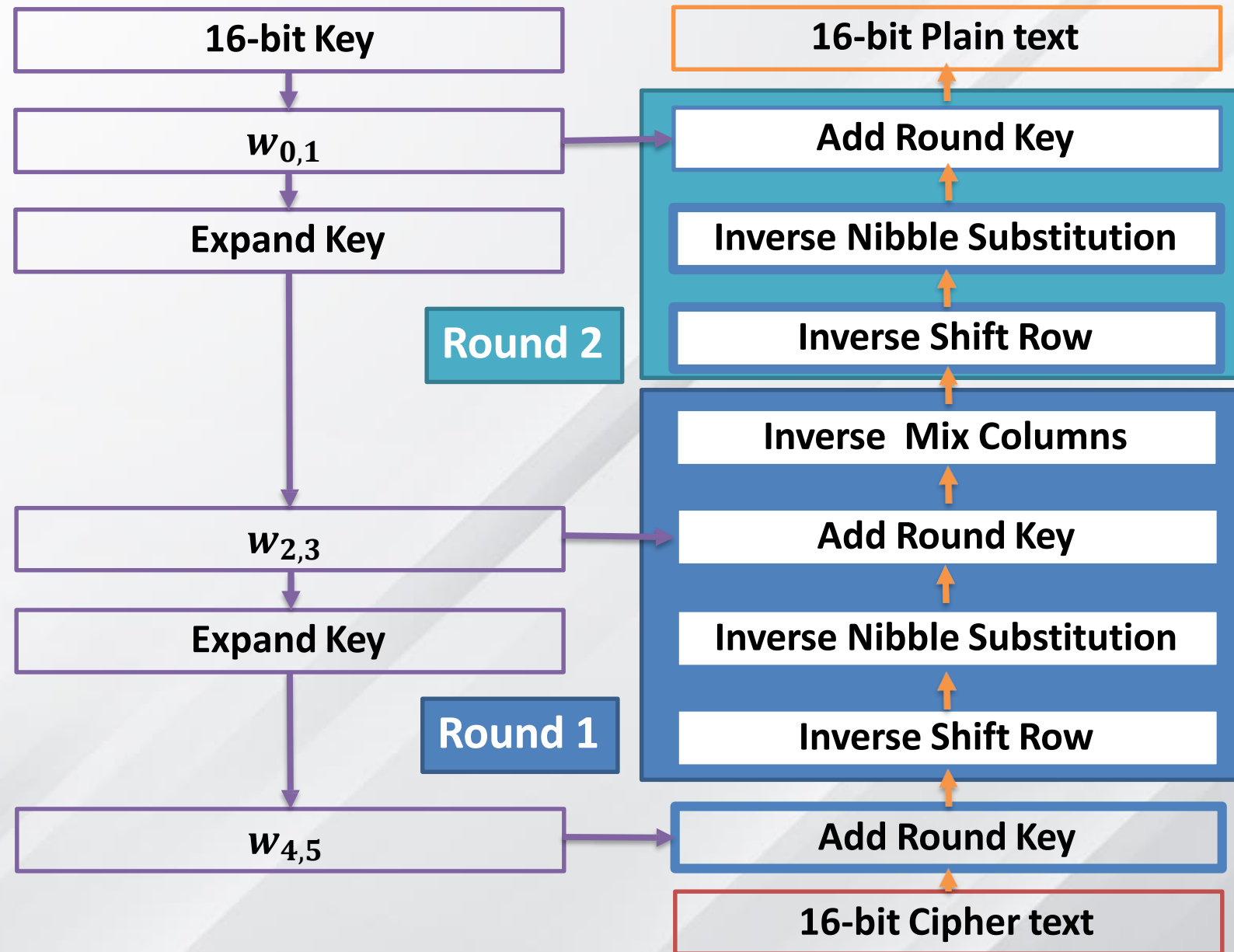
$$\text{❑} = \begin{pmatrix} (1110 \oplus 1100) & (1000 \oplus 0110) \\ (1101 \oplus 0011) & (0110 \oplus 1000) \end{pmatrix}$$

*	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

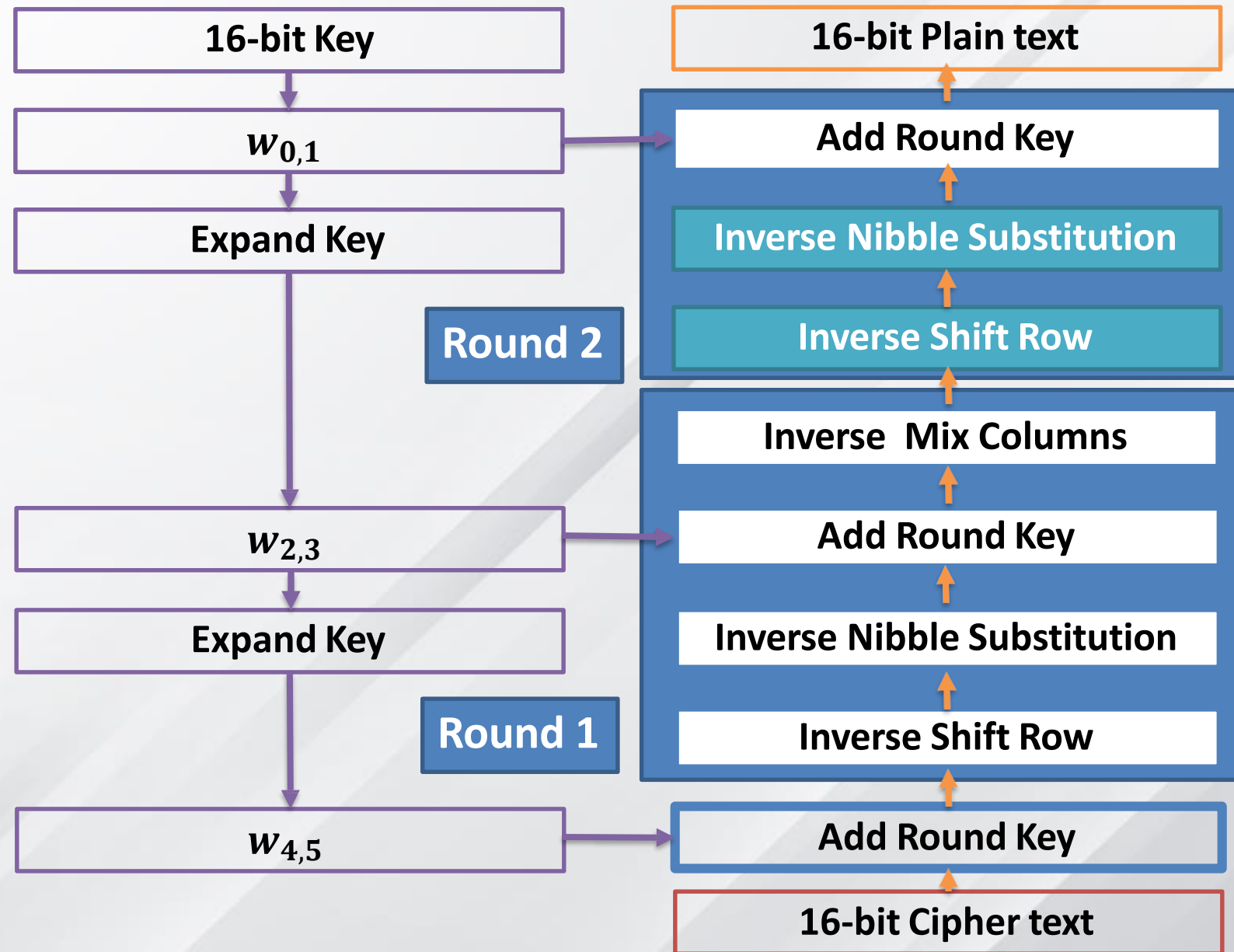
$$\square \begin{pmatrix} (1110 \oplus 1100) & (1000 \oplus 0110) \\ (1101 \oplus 0011) & (0110 \oplus 1000) \end{pmatrix} = \begin{pmatrix} 0010 & 1110 \\ 1110 & 1110 \end{pmatrix}$$

R1 = 0010 1110 1110 1110

S-AES Decryption



S-AES Decryption



□ Round 2

1) Inverse Shift Row

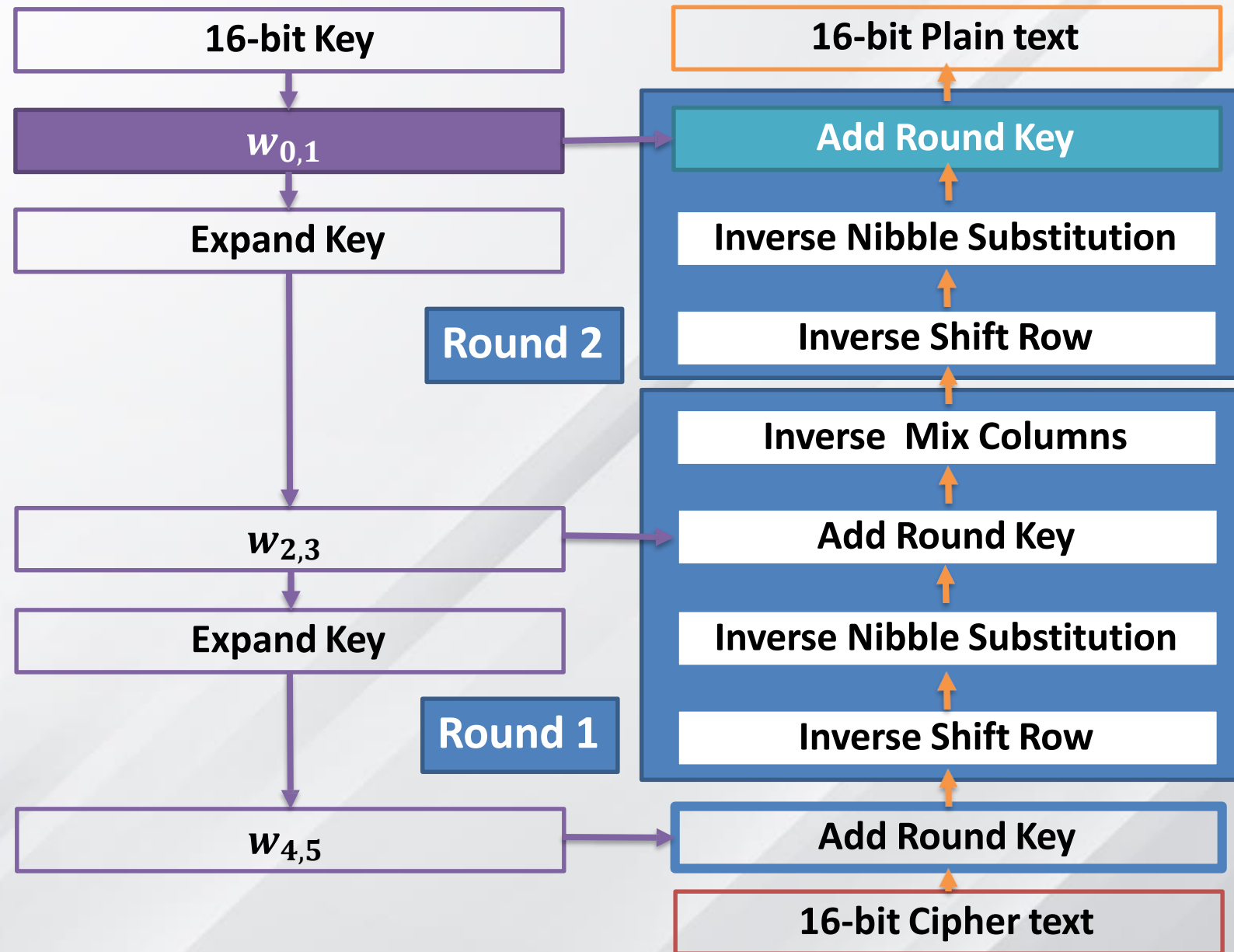
$$\begin{aligned} \square \text{IShRow}(R1) &= \text{IShRow}(0010 \text{ } 1110 \text{ } 1110 \text{ } 1110) = \\ &= 0010 \text{ } 1110 \text{ } 1110 \text{ } 1110 \end{aligned}$$

2) Inverse Nibble Sub

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

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



3) Add Round 2 Key

$$\square R2 = 1001\ 1101\ 1101\ 1101 \oplus \text{Key0}$$

$$= 1001\ 1101\ 1101\ 1101 \oplus 0100\ 1010\ 1111\ 0101$$

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

$$\text{Plaintext} = 1101\ 0111\ 0010\ 1000 = \text{D7 28}$$

Simplified Advanced Encryption Standard S_AES

RSA

RSA

RSA Key generation

RSA Encryption

RSA Decryption

A Real World Example

RSA Security

RSA

RSA Key generation

RSA Encryption

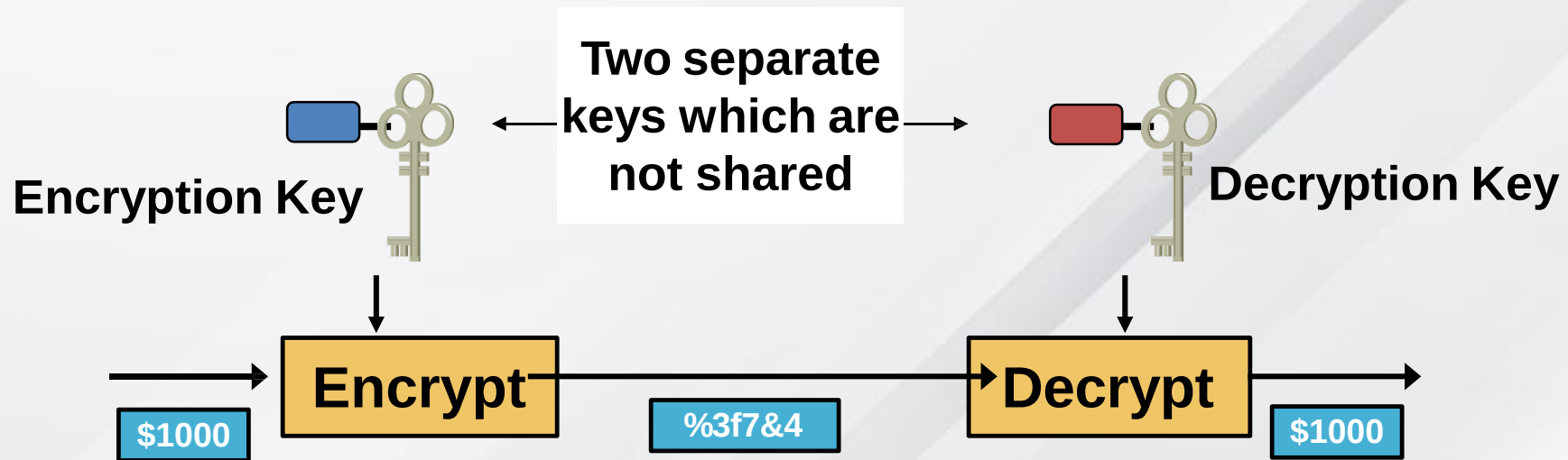
RSA Decryption

A Real World Example

RSA Security

- ❑ RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission.
- ❑ RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977

❑ RSA is Asymmetric Encryption



RSA

RSA Key generation

RSA Encryption

RSA Decryption

A Real World Example

RSA Security

RSA Key Generation

- 1) Choose two distinct prime numbers p and q
- 2) Compute $n = p * q$
- 3) Compute $Z = (p - 1) * (q - 1)$
- 4) Choose e such that $1 < e < Z$ and e and n are prime.
- 5) Compute a value for d such that $(d * e) \% Z = 1$
 - ❑ Public key is (e, n)
 - ❑ Private key is (d, n)

RSA Key Generation Example

Choose $p = 3$ and $q = 11$

Compute $n = p * q = 3 * 11 = 33$

Compute $\varphi(n) = (p - 1) * (q - 1) = 2 * 10 = 20$

Choose e such that $1 < e < \varphi(n)$ and e and n are prime. Let $e = 7$

Compute a value for d such that $(d * e) \% \varphi(n) = 1$. One solution is $d = 3$ $[(3 * 7) \% 20 = 1]$

Public key is $(e, n) \Rightarrow (7, 33)$

Private key is $(d, n) \Rightarrow (3, 33)$

RSA

RSA Key generation

RSA Encryption

RSA Decryption

A Real World Example

RSA Security

m = plaintext

Public key is (e, n)

C = Ciphertext

$$C = m^e \% n$$

RSA Encryption Example

$$m = 2$$

Public key is $(e, n) \Rightarrow (7, 33)$

$$C = 2^{7\%} 33 = 29$$

RSA

RSA Key generation

RSA Encryption

RSA Decryption

A Real World Example

RSA Security

- C= Ciphertext
- m = plaintext
- Private key is (d, n)
- $m = C^d \% n$

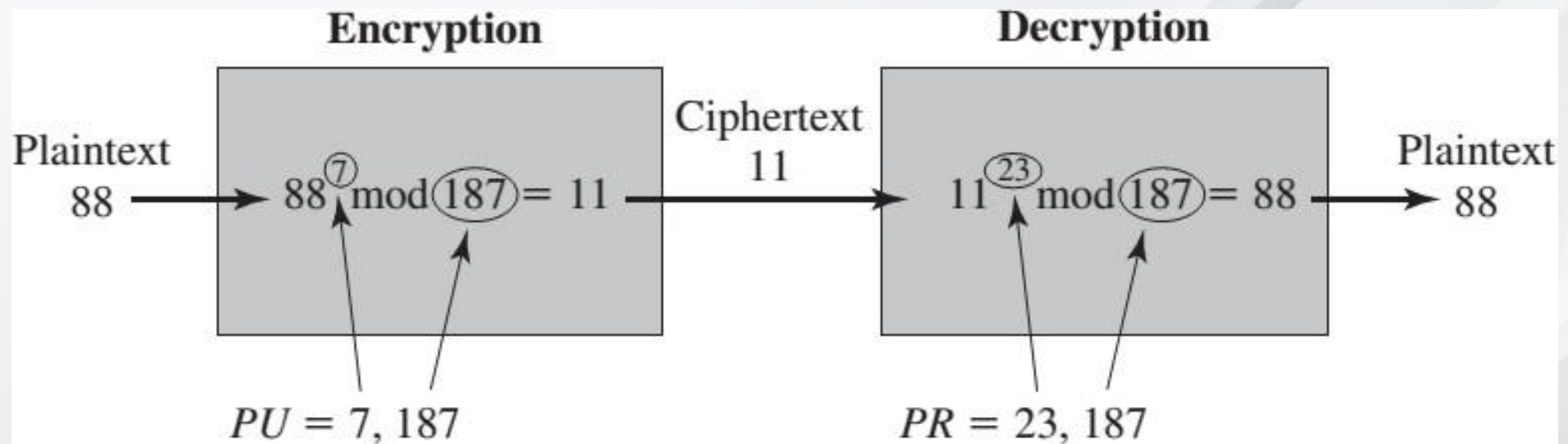
RSA Decryption Example

- $C = 29$
- Private key is $(d, n) \Rightarrow (3, 33)$
- $m = C^3 \% 33 = 2$

RSA another Example

- Select two prime numbers, $p = 17$ and $q = 11$.
- Calculate $n = pq = 17 * 11 = 187$.
- Calculate $Z = (p - 1)(q - 1) = 16 * 10 = 160$.
- Select e such that e is relatively prime to
- $Z = 160$ and less than Z ; we choose $e = 7$.
- Determine d such that $d.e \pmod{160} = 1$ and $d < 160$. The correct value is $d = 23$, because $23 * 7 = 161 = (1 * 160) + 1$
- Public Key = $\{7, 187\}$ and Private Key = $\{23, 187\}$

RSA another Example



RSA

RSA Key generation

RSA Encryption

RSA Decryption

A Real World Example

RSA Security

RSA another Example

- ❑ lets encrypt the message "attack at dawn"
- ❑ Convert the message into a numeric format. Each letter is represented by an ASCII character.
- ❑ "attack at dawn" becomes 1976620216402300889624482718775150

□ p=

12131072439211271897323671531612440428472427633701410
92563454931230196437304208561932419736532241686654101
7057361365214171711713797974299334871062829803541

□ q=

12027524255478748885956220793734512128733387803682075
43365389998395517985098879789986914690080913161115334
6817050832096022160146366346391812470987105415233

□ $n=145906768007583323230186939349070$

6352924018723753571643995818

7101987343879900535893836957140267014980212181808629246742282815

7022922076746906543401224889672472407926969987100581290103199317

8587536637108623576565105078837142971156373427889114635351027120

32765166518411726859837988672111837205085526346618740053

□ $Z=14590676800758332323018693934907063529240187237535716439958$

1871019873438799005358938369571402670149802121818086292467422828

1570229220767469065434012248896483138112322799663173013977778523

6530154784827347887129722205858745715289160645926971811926897116

3555070802643999529549644116811947516513938184296683521280

□ $e = 65537$

□ $d = 89489425009274444368228545921773093919669586065884$
25744549785445648767483962981839093494197326287961679
79706089172836798754993315741611138540888132754881105
88247193077582527278437906504015680623423550067240042
46666565423238350292221549362328947213886644581878912
7946123407807725702626644091036502372545139713

❑ **Encryption:** $C = 1976620216402300889624482718775150^{e \% n}$

❑ $C =$

35052111338673026690212423937053328511880760811579981
62064280234668581062310985023594304908097338624111378
40407947041939782153784997654130836464387847409523069
32534945195080183861574225226218879827232453912820596
88644037753608246568175007441745915148540744586251102
3472235560823053497791518928820272257787786

❑ Decryption: $P =$

35052111338673026690212423937053328511880760811579981620642
80234668581062310985023594304908097338624111378404079470419
39782153784997654130836464387847409523069325349451950801838
61574225226218879827232453912820596886440377536082465681750
07441745915148540744586251102347223556082305349779151892882
0272257787786 $^d \% n$

❑ $P = 1976620216402300889624482718775150$ (which is our plaintext "attack at dawn")

RSA

RSA Key generation

RSA Encryption

RSA Decryption

A Real World Example

RSA Security

- ❑ Two approaches to attacking RSA:
- ❑ brute force key search (infeasible given size of numbers)
- ❑ mathematical attacks (based on difficulty of computing Z , by factoring modulus N)



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

