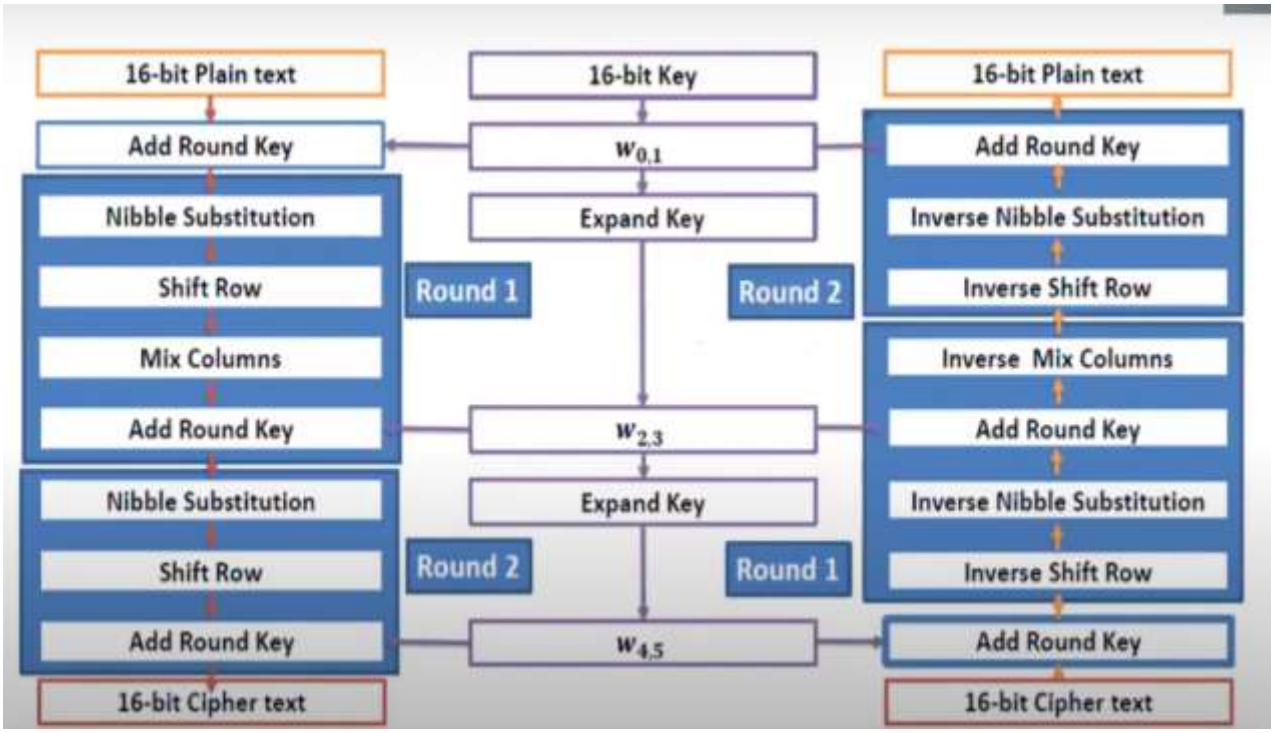
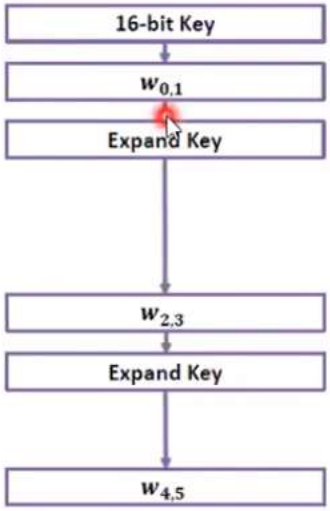
SAES Example



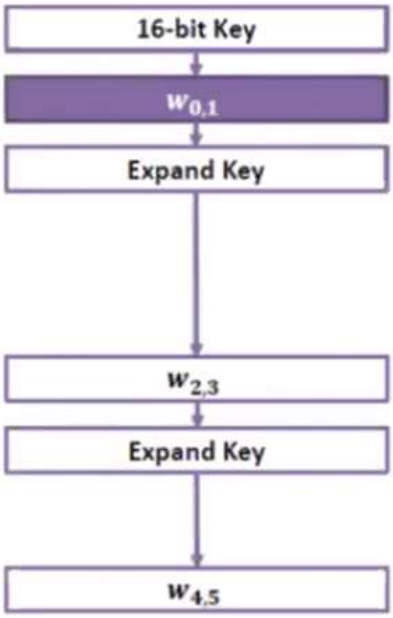
S-AES Encryption Example

- 16-bit Plaintext, P= D728 = 1101011100101000
- 16-bit Key, K= 4AF5 = 0100101011110101

S-AES Key Generation



Continued

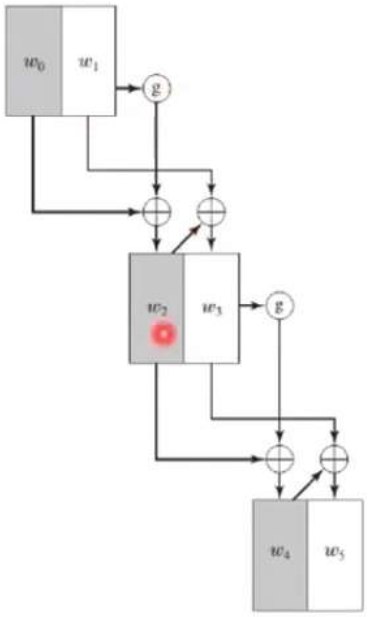


- K = 4AF5 = 0100101011110101
- The input key, K, is split into 2 words, w_0 and w_1:

- w_0=01001010
- w_1=11110101

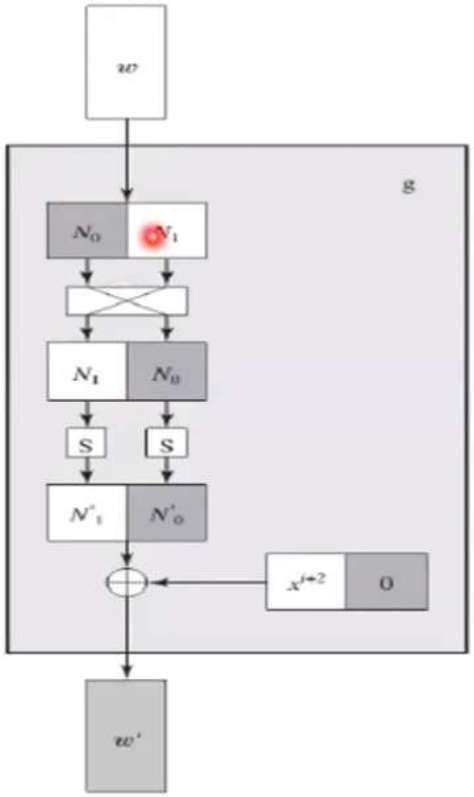
Continue

- S-AES Key Expansion



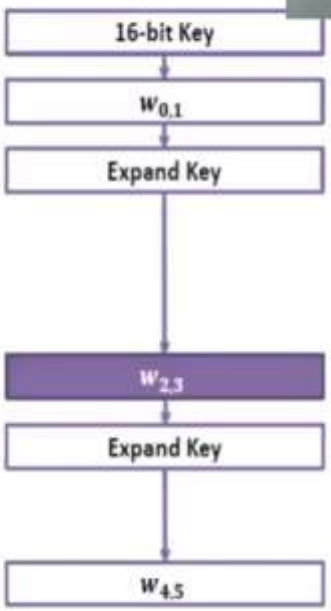
Function g

Function g



Continue

- w0 = 0100 1010, w1 = 1111 0101
- w2 = w0 ⊕ Rcon(1) ⊕ SubNib(RotNib(w1))
- **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"
- RotNib(w1) = 0101 1111
- SubNib(0101 1111) = 0001 0111
- Rcon(1) = 10000000



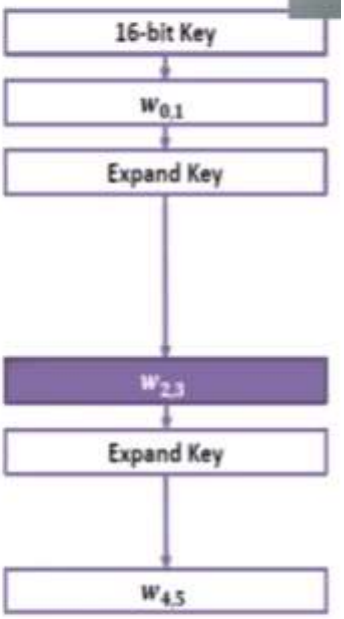
S-Box

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

o

Continue

- w0 = 0100 1010, w1 = 1111 0101
- w2 = w0 ⊕ Rcon(1) ⊕ SubNib(RotNib(w1))
- **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"
- RotNib(w1) = 0101 1111
- SubNib(0101 1111) = 0001 0111
- Rcon(1) = 10000000



S-Box

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

Continue

- w0 = 0100 1010, w1 = 1111 0101
- w2 = w0 ⊕ Rcon(1) ⊕ SubNib(RotNib(w1))

  = 0100 1010 ⊕ 1000 0000 ⊕ 0001 0111

  = 0100 1010 ⊕ **1001 0111**=1101 1101
- w2 =1101 1101
- w3 = w2 ⊕ w1 = 1101 1101 ⊕ 1111 0101= 0010 1000
- w3 = 0010 1000

Continue

- w2 = 1101 1101, w3 = 0010 1000
- w4 = w2 ⊕ Rcon(2) ⊕ SubNib(RotNib(w3))

  = 1101 1101 ⊕ 0011 0000 ⊕ SubNib(1000 0010)

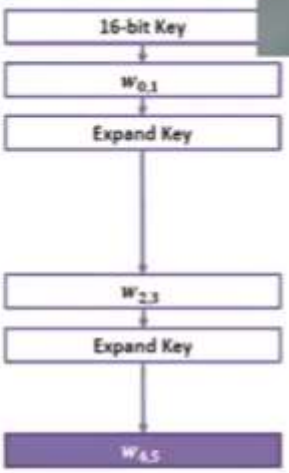
  = 1110 1101 ⊕ 0011 0000 ⊕ 0110 1010

  = 1110 1101 ⊕ 0101 1010

  = 1011 0111
- w5 = w4 ⊕ w3

  =1011 0111 ⊕ 0010 1000

  =1001 1111



S-Box

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

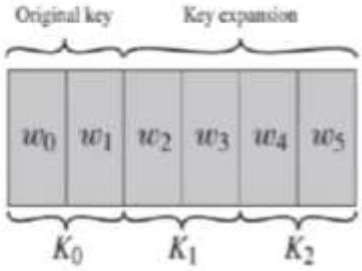
Continue

- Key
- Key0 = w0w1

  = 0100 1010 1111 0101
- Key1 = w2w3

  = 1101 1101 0010 1000
- Key2 = w4w5

  = 1011 0111 1001 1111



Continued

- Assume: P= 1101 0111 0010 1000
- Key0 = w0w1

  = 0100 1010 1111 0101
- Key1 = w2w3

  = 1101 1101 0010 1000
- Key2 = w4w5

  = 1000 0111 1010 1111

15

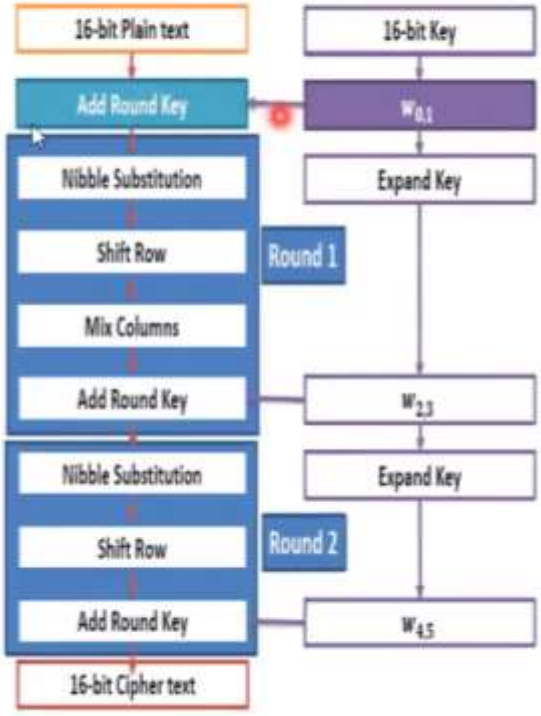
Add Round key

- Round 0
- P= 1101 0111 0010 1000
- Key0 = 0100 1010 1111 0101
- R0= P ⊕ Key0

  = 1101 0111 0010 1000 ⊕

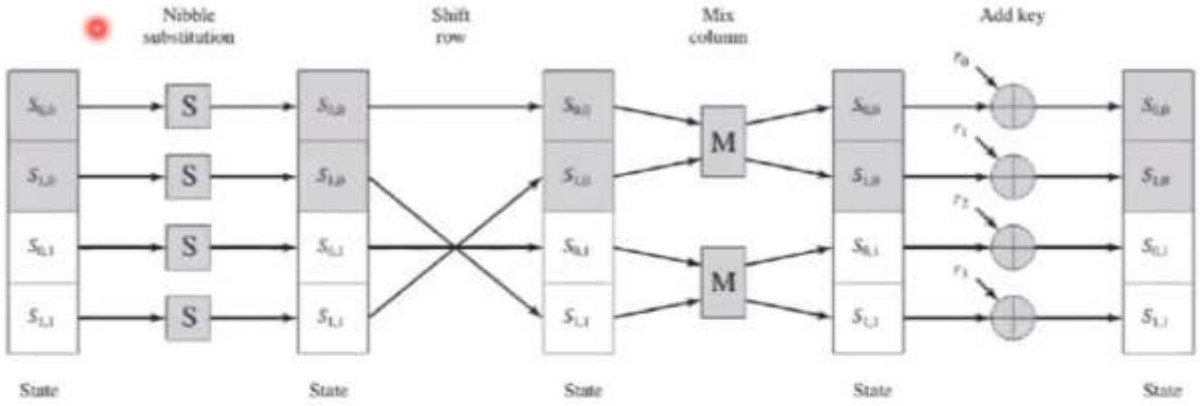
  0100 1010 1111 0101

  = 1001 1101 1101 1101



S-AES Encryption Round

❑ S-AES Encryption Round



Continue

- 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)

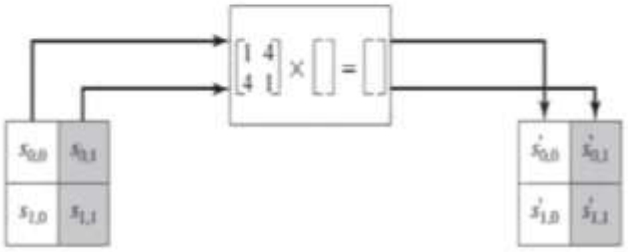
  = 0010 1110 1110 1110

S-Box

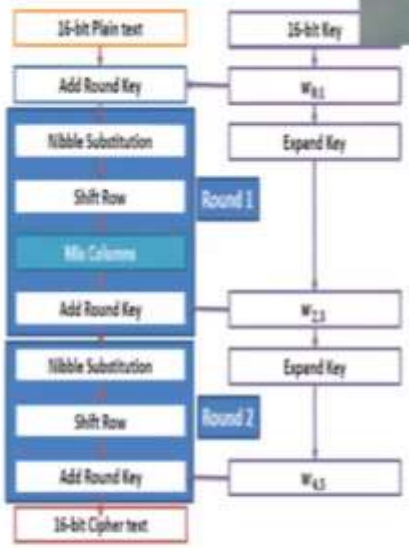
i \ j	00	01	10	11
00	9	4	A	B
01	D	1	8	5
10	6	2	0	3
11	C	E	F	7

Continued

- S-AES Transformation (Mix Column)



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

Continued

- Round 1

3) Mix Columns:

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

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

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

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

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

$= 1111\ 0110\ 0011\ 0011$

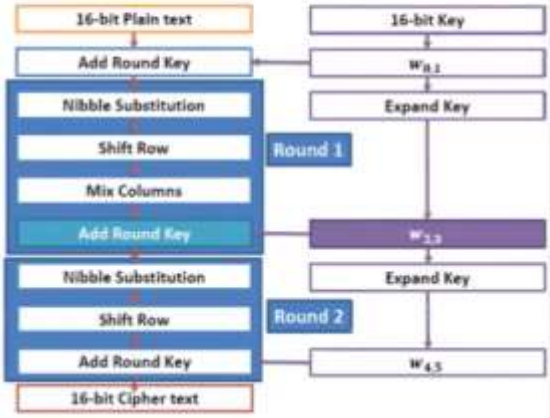
- Round 1

4) Add round Key1

- Key1 = 1101 1101 0010 1000
- R1= Key1 ⊕ MixCol(ShRow(SubNib(R0)))

= 1101 1101 0010 1000 ⊕ 1111 0110 0011 0011

= 0010 1011 0001 1011



- 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	00	01	10	11
00	9	4	A	B
01	D	1	8	5
10	6	2	0	3
11	C	E	F	7

Round 2

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

Continued

- Round 2

4) Add round Key2

- Key2 = 1000 0111 1010 1111
- R2= Key2 ⊕ ShRow(SubNib(R1))

= 1101 1101 0010 1000 ⊕ 1010 0011 0100 0011

= 0010 0100 1110 1100

Ciphertext = 0010 0100 1110 1100