Sheet No 1 Page No 1

Name:- Muhammad Adil Arid No:- 19-Arid-917

S-AES Encryption and Decryption

Mobile No:- 0331 8981621

P= 8281 K= 8121

P= 1000^{8} 0010^{2} 1000^{8} 0001^{1}

K= 1000^{8} 0001^{1} 0010^{2} 0001^{1}

Key Expansion For S-AES

Key words

w_0 = 1000 0001 w_1 = 0010 0001

$w_2 = w_0 \oplus Rcon\,1 \oplus SubNib(RotNib(w_1))$

w_2 = 1000 0001 ⊕ 10000000 ⊕ SN(RN(0010 0001))

w_2 = 1000 0001 ⊕ 1000 0000 ⊕ SN(0001 0010)

w_2 = 1000 0001 ⊕ 1000 0000 ⊕ (4 A)

w_2 = 1000 0001 ⊕ 1000 0000 ⊕ 0100 1010

w_2 = 0100 1011

$w_3 = w_2 \oplus w_1$

w_3 = 0100 1011 ⊕ 0010 0001

w_3 = 0110 1010

$w_4 = w_2 \oplus Rcon\,2 \oplus SubNib(RotNib(w_3))$

w_4 = 0100 1011 ⊕ 0011 0000 ⊕ SN(RN(0110 1010))

w_4 = 0100 1011 ⊕ 0011 0000 ⊕ SN(1010 0110)

w_4 = 0100 1011 ⊕ 0011 0000 ⊕ 8(0 8)

w_4 = 0100 1011 ⊕ 0011 0000 ⊕ 0000 1000

w_4 = 0111 0011

$w_5 = w_4 \oplus w_3$ = 0111 0011 ⊕ 0110 1010

w_5 = 0001 1001

CamScanner

$K_0 = W_0\ W_1 = 1000\ 0001\ 0010\ 0001$

So that, $K_0 =$

8	1000	0010	2
1	0001	0001	1

$K_1 = W_2\ W_3 = 0100\ 1011\ 0110\ 1010$

So that, $K_1 =$

4	0100	0110	6
B	1011	1010	A

$K_2 = W_4\ W_5 = 0111\ 0011\ 0001\ 1001$

$K_2 =$

7	0111	0001	1
3	0011	1001	9

S-AES Encryption

$P = 8281 = 1000\ 0010\ 1000\ 0001 = P =$

8	1000	1000	8
2	0010	0001	1

Add Round Key

$P \oplus K_0$

		1000	1000	⊕	1000	0010
		0010	0001		0001	0001

$P \oplus K_0 =$

	0	A	
3	0011	0000	0

Round 1 Start

Step 1:- Nibble Subsitution

				9	0
0000	1010	NS →	1001	0000	
0011	0000				
		B	1011	1001	9

Step 2:- Shift Row

				9	0
1001	0000	SR →	1001	0000	
1011	1001				
			9	B	

Step 3:- Mix Columns

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \times \begin{bmatrix} 9 & 0 \\ 9 & B \end{bmatrix}$$

S_{00}	S_{01}
$1 \times 9 \oplus 4 \times 9$	$1 \times 0 \oplus 4 \times B$
$4 \times 9 \oplus 1 \times 9$	$4 \times 0 \oplus 1 \times B$
S_{10}	S_{11}

$\longrightarrow S_{00} = 1 \times 9 \oplus 4 \times 9$

$S_{00} = (0001)(1001) \oplus (0100)(1001)$

$S_{00} = (1)(x^3+1) \oplus (x^2)(x^3+1)$

$S_{00} = x^3+1 \oplus x^5+x^2$

x^5+x^2 to be reduced modulo x^4+x+1

$S_{00} = x^3+1 \oplus x$

$S_{00} = 1001 \oplus 0010$

$S_{00} = 1011$

$x^4+x+1 \;\big|\; x^5+x^2 \;\big|\; x$

x^5+x^2+x

x

$\longrightarrow S_{10} = 4 \times 9 \oplus 1 \times 9$ Same Solution. Like above

$S_{10} = 1011$

$\longrightarrow S_{01} = 1 \times 0 \oplus 4 \times B$

$S_{01} = (0001)(0000) \oplus (0100)(101)$

$S_{01} = 0000 \oplus (x^2)(x^3+x+1)$

$S_{01} = 0000 \oplus x^5+x^3+x^2$

$x^5+x^3+x^2$ to be reduced modulo x^4+x+1

$S_{01} = 0000 \oplus x^3 + x$

$S_{01} = 0000 \oplus 1010$

$S_{01} = 1010$

$x^4 + x + 1 \;\big|\; x^5 + x^3 + x^2 \;\big|\; x$

$x^5 + x^2 + x$

$x^3 + x$

$\rightarrow S_{11} = 4x0 \oplus 1xB$

$S_{11} = (0100)(0000) \oplus (0001)(1011)$

$S_{11} = 0000 \oplus (1)(x^3 + x + 1)$

$S_{11} = 0000 \oplus 1011$

$S_{11} = 1011$

So that Resultant State Matrix After Mix column

B	1011	1010	A
B	1011	1011	B

Step 4 :- Add Round Key (K_1)

B	1011	1010	A	$\oplus$	4	0100	0110	6
B	1011	1011	B		B	1011	1010	A

F	1111	1100	C
0	0000	0001	1

Finish Round 1
for S-AES
Encryption

Start Round 2

Step:-1 Nibble Subsitution

1111	1100	NS →	0111	1100	7	C
0000	0001		1001	0100	9	4

Step:-2 Shift Row

0111	1100	SR →	0111	1100	7	C
1001	0100		0100	1001	4	9

Step:-3 Add Round Key (K_2)

0111	1100	⊕	0111	0001	7	C	7	1
0100	1001		0011	1001	4	9	3	9

0	0000	1101	D
7	0111	0000	0

So that,

Cipher Text in Binary:-

C = 0000 0111 1101 0000

Cipher Text in Hexa:- Encryption

C = 0 7 D 0 Ans.

S-AES Decryption

C = 0000 0111 1101 0000 = 07D0

K_0 = 1000 0001 0010 0001 = 8121

K_1 = 0100 1011 0110 1010 = 4B6A

K_2 = 0111 0011 0001 1001 = 7319

Add Round Key (K_2)

C		⊕	K_2	
0000	1101	⊕	0111	0001
0111	0000		0011	1001

7	0111	1100	C
4	0100	1001	9

Start Round 1

Step 1 :- Inverse Shift Row

	7	c			7	c	
	0111	1100	ISR →		0111	1100	
4	0100	1001	9	9	1001	0100	4

Step 2:- Inverse Nibble Subsitition

7	c		F	c
0111	1100	INS →	1111	1100
1001	0100		0000	0001
9	4		0	1

Step 3:- Add Round Key (K_1)

1111	1100	⊕	0100	0110
0000	0001		1011	1010

B	1011	1010	A
B	1011	1011	B

Step 4: Inverse Mix Column

$$\begin{bmatrix} 9 & 2 \\ 2 & 9 \end{bmatrix} \times \begin{bmatrix} B & A \\ B & B \end{bmatrix}$$

$$\begin{bmatrix} S_{00} & S_{01} \\ 9\times B \oplus 2\times B & 9\times A \oplus 2\times B \\ 2\times B \oplus 9\times B & 2\times A \oplus 9\times B \\ S_{10} & S_{11} \end{bmatrix}$$

$\longrightarrow S_{00} = 9\times B \oplus 2\times B$

$S_{00} = (1001)(1011) \oplus (0010)(1011)$

$S_{00} = (x^3+1)(x^3+x+1) \oplus (x)(x^3+x+1)$

$S_{00} = x^6 + x^4 + x^3 + x^3 + x + 1 \oplus x^4 + x^2 + x$

$S_{00} = x^6 + x^4 + x + 1 \oplus x^4 + x^2 + x$

(x^6+x^4+x+1) and (x^4+x^2+x) to be reduced

modulo x^4+x+1

$$x^4+x+1 \;\big)\; x^6+x^4+x+1 \;\big)\; x^2+1$$

$$x^6 + x^3 + x^2$$

$$x^4 + x^3 + x^2 + x + 1$$

$$x^4 + \qquad x + 1$$

$$x^3 + x^2$$

$$x^4+x+1 \;\big)\; x^4+x^2+x \;\big)\; 1$$

$$x^4 + x + 1$$

$$x^2 + 1$$

$S_{00} = x^3 + x^2 \oplus x^2 + 1$

$S_{00} = 1100 \oplus 0101$

$\boxed{S_{00} = 1001}$

$\rightarrow S_{10} = 2XB \oplus 9XB$ Same Solution like above.

$\boxed{S_{10} = 1001}$

$\rightarrow S_{01} = 9XA \oplus 2XB$

$S_{01} = (1001)(1010) \oplus (0010)(1011)$

$S_{01} = (x^3+1)(x^3+x) \oplus 0101$

$S_{01} = x^6 + x^4 + x^3 + x \oplus 0101$

$x^6 + x^4 + x^3 + x$ to be reduced modula $x^4 + x + 1$

$x^4+x+1 \;\big|\; x^6 + x^4 + x^3 + x \;\big|\; x^2 + 1$

$x^6 + x^3 + x^2$

$x^4 + x^2 + x$

$x^4 + x + 1$

$x^2 + 1$

$S_{01} = x^2 + 1 \oplus 0101$

$S_{01} = 0101 \oplus 0101$

$\boxed{S_{01} = 0000}$

$\rightarrow S_{11} = 2XA \oplus 9XB$

$S_{11} = (0010)(1010) \oplus (1001)(1010)$

$S_{11} = (x)(x^3+x) \oplus 1100$

$S_{11} = (x^4 + x^2) \oplus 1100.$

$x^4 + x^2$ to be reduced modula $x^4 + x + 1$

CamScanner

$x^4+x+1 \overline{)\ x^4+x^2\ } 1$

x^4+x+1

x^2+x+1

$S_{11} = x^2+x+1 \oplus 1100$

$S_{11} = 0111 \oplus 1100$

$\boxed{S_{11} = 1011}$

So that, Resultant State Matrix After Mix Column

9	1001	0000	0
9	1001	1011	B

Start Round 2

Step 1 :- Inverse Shift Row

9	0		9	0
1001	0000	I R →	1001	0000
1001	1011		1011	1001
9	B		B	9

Step 2 :- Inverse Nibble Subsitution

9	0		0	A
1001	0000	INS →	0000	1010
1011	1001		0011	0000
B	9		3	0

Step 3 :- Add Round Key (K_0)

0	A		8	2
0000	1010	⊕	1000	0010
0011	0000		0001	0001
3	0		1	1

8	1000	1000	8
2	0010	0001	1

So that,

Plain Text in Binary:-

P = 1000 0010 1000 0001

Plain Text in Hexa:-

P = 8281

Decryption
Ans

Extra work
using Table to Solve Mix Column
for S-AES Encryption and Decryption

*	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		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 → Mix Column

→ $\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \times \begin{bmatrix} 9 & 0 \\ 9 & B \end{bmatrix}$

→ $\begin{bmatrix} S_{00} & S_{01} \\ 1\times9 \oplus 4\times9 & 1\times0 \oplus 4\times B \\ 4\times9 \oplus 1\times9 & 4\times0 \oplus 1\times B \end{bmatrix}$

→ $\begin{bmatrix} S_{10} & S_{11} \\ 9 \oplus 2 & 0 \oplus A \\ 2 \oplus 9 & 0 \oplus B \end{bmatrix}$

→ $\begin{bmatrix} 1001 \oplus 0010 & 0000 \oplus 1010 \\ 0010 \oplus 1001 & 0000 \oplus 1011 \end{bmatrix}$

→ $\begin{bmatrix} 1011 & 1010 \\ 1011 & 1011 \end{bmatrix}$ → $\begin{bmatrix} B & A \\ B & B \end{bmatrix}$

S-AES Decryption → Mix Column

→ $\begin{bmatrix} 9 & 2 \\ 2 & 9 \end{bmatrix} \times \begin{bmatrix} B & A \\ B & B \end{bmatrix}$

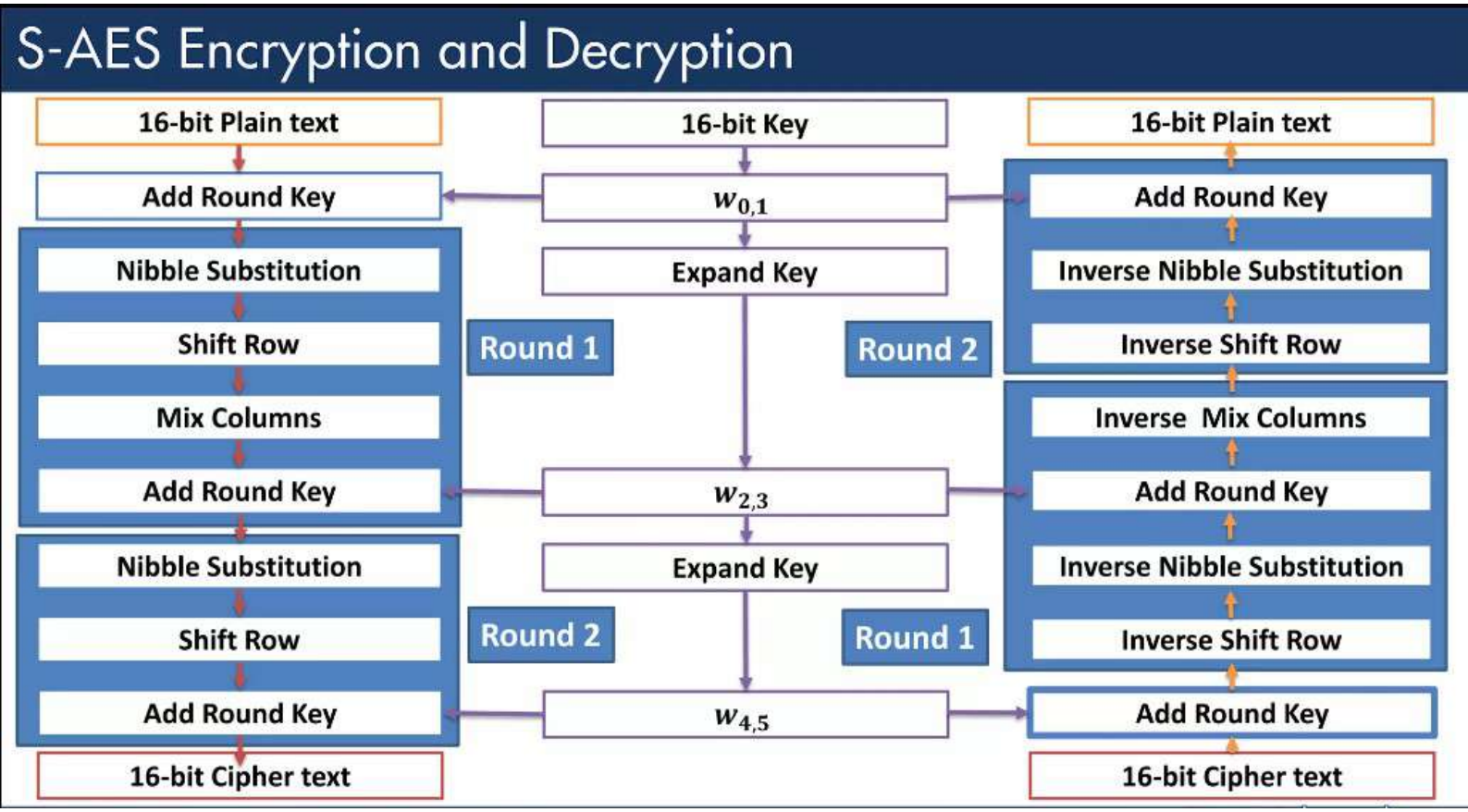
→ $\begin{bmatrix} 9 \times B \oplus 2 \times B & 9 \times A \oplus 2 \times B \\ 2 \times B \oplus 9 \times B & 2 \times A \oplus 9 \times B \end{bmatrix}$

→ $\begin{bmatrix} C \oplus 5 & 5 \oplus 5 \\ 5 \oplus C & 7 \oplus C \end{bmatrix}$

→ $\begin{bmatrix} 1100 \oplus 0101 & 0101 \oplus 0101 \\ 0101 \oplus 1100 & 0111 \oplus 1100 \end{bmatrix}$

→ $\begin{bmatrix} 1001 & 0000 \\ 1001 & 1011 \end{bmatrix}$ → $\begin{bmatrix} 9 & 0 \\ 9 & B \end{bmatrix}$

S-AES Encryption and Decryption



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

Inv S-Box

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

- Round 1

4) Inverse Mix Columns :

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

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

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

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

*	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