ASSIGNMENT 22B1229

21 April 2025 18:37

Encryption:

S-box

Irreducible polynomial of choice: x^3+x+1

Inv pairs

1	1
x	x^2+1
$x+1$	x^2+x
x^2	x^2+x+1
x^2+1	x
x^2+x	$x+1$
x^2+x+1	x^2

Affine Transformation:

Must be invertible over GF(8)

Must be bijective

After random guessing I got $\alpha = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$, $\beta = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ that satisfy the above two constraints

$$\alpha^{-1} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

Final Mapping

0 – 000	000	100 – 4
1 – 001	001	110 – 6
2 – 010	101	111 – 7
3 – 011	110	011 – 3
4 – 100	111	001 – 1
5 – 101	010	010 – 2
6 – 110	011	000 – 0
7 – 111	100	101 – 5
$A(x)$	$A^{-1}(x)$	$\alpha A^{-1}(x) + \beta$

Row Shift

$$\left.\begin{bmatrix} b_0 & b_3 & b_6 \\ b_1 & b_4 & b_7 \\ b_2 & b_5 & b_8 \end{bmatrix}\begin{array}{l} \leftarrow 0 \\ \leftarrow 1 \\ \leftarrow 2 \end{array}\right. \qquad \begin{bmatrix} b_0 & b_3 & b_6 \\ b_4 & b_7 & b_1 \\ b_8 & b_2 & b_5 \end{bmatrix}$$

Inv Row Shift

$$\left.\begin{bmatrix} c_0 & c_3 & c_6 \\ c_1 & c_4 & c_7 \\ c_2 & c_5 & c_8 \end{bmatrix}\begin{array}{l} \rightarrow 0 \\ \rightarrow 1 \\ \rightarrow 2 \end{array}\right. \qquad \begin{bmatrix} c_0 & c_3 & c_6 \\ c_7 & c_1 & c_4 \\ c_5 & c_8 & c_2 \end{bmatrix}$$

Mix Cols

$a(x) = a_2x^2 + a_1x + a_0$

$b(x) = b_2x^2 + b_1x + b_0$

$a(x) \cdot b(x) = c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0 \equiv d_2x^2 + d_1x + d_0 \mod x^3+x+1$

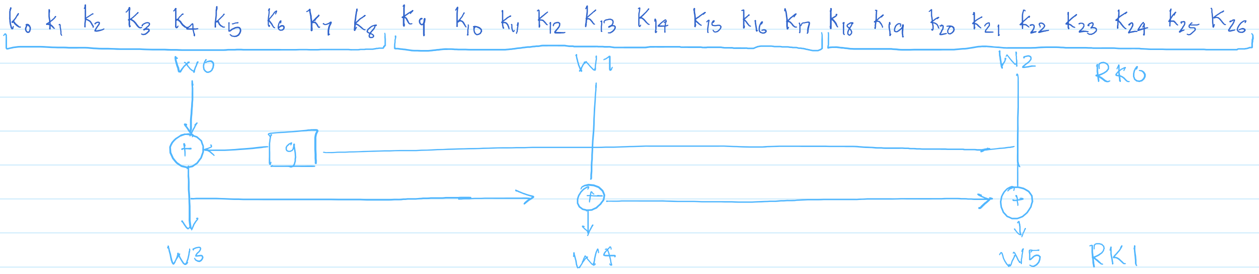
$c_4 = a_2b_2$	$d_2 = c_4 \oplus c_2$
$c_3 = a_2b_1 \oplus a_1b_2$	$d_1 = c_4 \oplus c_3 \oplus c_1$
$c_2 = a_2b_0 \oplus a_1b_1 \oplus a_0b_2$	$d_0 = c_3 \oplus c_0$
$c_1 = a_1b_0 \oplus a_0b_1$	
$c_0 = a_0b_0$	

$$\begin{bmatrix} d_2 \\ d_1 \\ d_0 \end{bmatrix} = \begin{bmatrix} a_2 \oplus a_0 & a_1 & a_2 \\ a_2 \oplus a_1 & a_2 \oplus a_0 & a_1 \\ a_1 & a_2 & a_0 \end{bmatrix} \begin{bmatrix} b_2 \\ b_1 \\ b_0 \end{bmatrix}$$

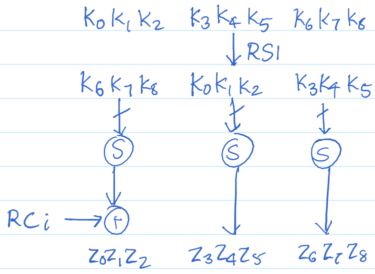
Choosing $a_2 = 5$, $a_1 = 2$, $a_0 = 1$ gives

Mix Col $= \begin{bmatrix} 4 & 2 & 5 \\ 3 & 4 & 2 \\ 2 & 5 & 1 \end{bmatrix}$, $MC^{-1} = \begin{bmatrix} 2 & 3 & 0 \\ 5 & 2 & 3 \\ 3 & 0 & 2 \end{bmatrix}$

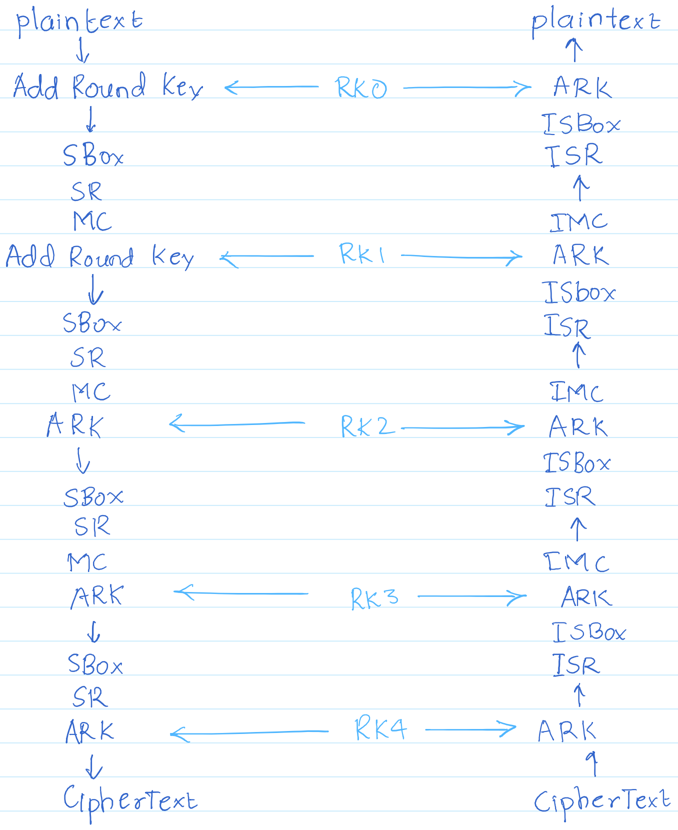
Key Gen


k_0 k_1 k_2 k_3 k_4 k_5 k_6 k_7 k_8 k_9 k_{10} k_{11} k_{12} k_{13} k_{14} k_{15} k_{16} k_{17} k_{18} k_{19} k_{20} k_{21} k_{22} k_{23} k_{24} k_{25} k_{26}
W0
W1
W2
RK0
g
W3
W4
W5
RK1

g function


$k_0 k_1 k_2$ $k_3 k_4 k_5$ $k_6 k_7 k_8$
RS1
$k_6 k_7 k_8$ $k_0 k_1 k_2$ $k_3 k_4 k_5$
S
S
S
RC_i
$z_0 z_1 z_2$
$z_3 z_4 z_5$
$z_6 z_7 z_8$

AES Overview



Example

plaintext	= 0,0,0, 0, 0, 0,0,0,0
key	= 1,2,3, 4, 5, 6, 7, 0, 1
ARK0	1,2,3, 4, 5,6, 7, 0, 1
SB1	6,7,3, 1,2, 0, 5,4,6
SR1	6,7,3, 2,0,1, 6,5,4
MC1	4,0,3, 3,3,4, 6,2, 7
ARK1	0,4,5, 3,2,4, 1,3,6
SB2	4, 1,2,3, 7,1, 6, 3,0
SR2	4, 1,2, 7, 1,3, 0,6, 3
MC2	3,1,5, 0,6,3,1, 5,3
ARK2	3,3, 6,0,5,0, 6,7,1
SB3	3, 3,0, 4, 2, 4,0,5,6
SR3	3,3,0, 2, 4, 4, 6,0,5
MC3	6,2,2, 7, 3,7, 5,0,7
ARK3	5,7,4, 4,5,2, 1,4,0
SB4	2,5,1, 1,2,7, 6, 1,4
SR4	2,5,1, 2,7,1, 4,6,1
ARK4	5,2,0,7, 6, 2,1,2,6

ASSIGNMENT 22B1229

21 April 2025 19:15

Output of one round encryption is as follows

$$\begin{tikzcd}
P \arrow[r] & \oplus \arrow[r] & \text{Sbox} \arrow[r] & \text{Shift Rows} \arrow[r] & \text{Mix Cols} \arrow[r] & \oplus \arrow[r] & C \\
 & RK0 \arrow[u] & & & & RK1 \arrow[u] &
\end{tikzcd}$$

For two given plain text, we get encrypted text C_1, C_2

Define $\beta = C_1 \oplus C_2 = \cancel{RK1} \oplus MC(SR(SBox(P_1 \oplus RK0)))$
$\oplus$
$\cancel{RK1} \oplus MC(SR(SBox(P_2 \oplus RK0)))$

$$\beta = MC(SR(SBox(P_1 \oplus RK0))) \oplus MC(SR(SBox(P_2 \oplus RK0)))$$

$$\beta = MC(SR(SBox(P_1 \oplus RK0) \oplus SBox(P_2 \oplus RK0)))$$

$$SR^{-1}(MC^{-1}(\beta)) = SBox(P_1 \oplus RK0) \oplus SBox(P_2 \oplus RK0)$$

Construct PDT table as

	0	1	2	3	4	5	6	7
0	0,0	1,2	2,3	3,7	4,5	5,6	6,4	7,1
1	1,2	0,0	3,1	2,5	5,7	4,4	7,6	6,3
2	2,3	3,1	0,0	1,4	6,6	7,5	4,7	5,2
3	3,7	2,5	1,4	0,0	7,2	6,1	5,3	4,6
4	4,5	5,7	6,6	7,2	0,0	1,3	2,1	3,4
5	5,6	4,4	7,5	6,1	1,3	0,0	3,2	2,7
6	6,4	7,6	4,7	5,3	2,1	3,2	0,0	1,5
7	7,1	6,3	5,2	4,6	3.4	2,7	1,5	0,0

Each cell (x,y) is filled as $(x \oplus y,\ Sbox(x) \oplus Sbox(y))$

For any given key, let round one outputs of $P_1 = 0,0,0,0,0,0,0,0,0$
$P_2 = 1,0,0,0,0,0,0,0,0$

be $C_1 = 5,2,0,7,6,2,1,2,6$
$C_2 = 4,2,0,5,6,2,5,2,6$
$\beta = 1,0,0,2,0,0,4,0,0$
$SR^{-1}(MC^{-1}(\beta)) = 2,0,0,0,0,0,0,0,0$

Hence for input diff of $1 (P_1 \oplus P_2)$, I get output diff of $2 (Sbox(P_1 \oplus RK0) \oplus Sbox(P_2 \oplus RK0))$

$\Rightarrow$ $P_1 \oplus RK0 = 0/1$ only 0,1 pair gives 1,2 from DDT
or $P_2 \oplus RK0 = 1/0$ $\Rightarrow RK0[0] = 0,1$

To know which is which run the same procedure with $P_1 = 0,0,0,0,0,0,0,0,0$
$P_3 = 2,0,0,0,0,0,0,0,0$

to get $C_1 = 5,2,0,7,6,2,1,2,6$
$C_3 = 7,2,0,3,6,2,2,2,6$
$\beta = 2,0,0,4,0,0,1,0,0$
$SR^{-1}(MC^{-1}(\beta)) = 5,0,0,0,0,0,0,0,0$

$\Rightarrow$ $P_1 \oplus RK0 = 3/1$ only 1,3 pair gives 2,5 from DDT
$P_3 \oplus RK0 = 1/3$ $\Rightarrow RK0[0] = 1,3$

Comparing with above $RK0[0] = 1$
Doing the same 0,1,0,0,0,0,0,0,0 gives RK0[1] and so on,
0,2,0,0,0,0,0,0,0
we get key = 1,2,3,4,5,6,7,0,1
Total 3 plaintext, 9 nibbles, - entire key recovered without bruteforce in 19 plaintext attempts