Walkthrough of the Algorithm

We encipher with CFB mode, initial value $IV = 11110000101010001011000100001001$ and key $K = 10000001100001100110011010100011$ the message: $M_1\|M_2\|M_3 = 10110010111101101011000100100111\|01101001101001001000001101000001\|11100100000100100011110001010110$

Keyschedule:

$W_0 = 10000001$
$W_1 = 10000110$
$W_2 = 01100110$
$W_3 = 10100011$
$(l(W_0) \otimes r(W_0)) \oplus l(W_0) \oplus r(W_0) = (x^3 \otimes 1) \oplus x^3 \oplus 1 = 1$
$(l(W_1) \otimes r(W_1)) \oplus l(W_1) \oplus r(W_1) = (x^3 \otimes x^2 + x) \oplus x^3 \oplus x^2 + x = x^3 + x + 1$
$(l(W_2) \otimes r(W_2)) \oplus l(W_2) \oplus r(W_2) = (x^2 + x \otimes x^2 + x) \oplus x^2 + x \oplus x^2 + x = x^2 + x + 1$
$(l(W_3) \otimes r(W_3)) \oplus l(W_3) \oplus r(W_3) = (x^3 + x \otimes x + 1) \oplus x^3 + x \oplus x + 1 = x^2$
$K_0 = \begin{bmatrix}0001 & 0111\\1011 & 0100\end{bmatrix}$

Round 1:
$T := W_3 \lll 3 = 00011101$
$T :=$ SubBytes(0001)$\|$SubBytes(1101) :

$$\left\{\begin{array}{c} 0001^{-1} = (1)^{-1} = 1 = 0001; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix}\cdot\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\1\\1\\1\end{bmatrix}=1110\end{array}\right\}$$
$$\left\{\begin{array}{c} 1101^{-1} = (x^3+x^2+1)^{-1} = x^2 = 0100; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix}\cdot\begin{bmatrix}0\\0\\1\\0\end{bmatrix}+\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\begin{bmatrix}1\\0\\1\\0\end{bmatrix}=0101\end{array}\right\}$$

$T := T \oplus RC_1 = 11100101 \oplus 00000011 = 11100110$
$W_4 := W_0 \oplus T = 01100111$
$W_5 := W_1 \oplus W_4 = 11100001$
$W_6 := W_2 \oplus W_5 = 10000111$
$W_7 := W_3 \oplus W_6 = 00100100$
$(l(W_4) \otimes r(W_4)) \oplus l(W_4) \oplus r(W_4) =$
$(x^2 + x \otimes x^2 + x + 1) \oplus x^2 + x \oplus x^2 + x + 1 = 0$
$(l(W_5) \otimes r(W_5)) \oplus l(W_5) \oplus r(W_5) =$
$(x^3 + x^2 + x \otimes 1) \oplus x^3 + x^2 + x \oplus 1 = 1$
$(l(W_6) \otimes r(W_6)) \oplus l(W_6) \oplus r(W_6) =$
$(x^3 \otimes x^2 + x + 1) \oplus x^3 \oplus x^2 + x + 1 = x$
$(l(W_7) \otimes r(W_7)) \oplus l(W_7) \oplus r(W_7) =$
$(x \otimes x^2) \oplus x \oplus x^2 = x^3 + x^2 + x$
$K_1 := \begin{bmatrix}0000 & 0010\\0001 & 1110\end{bmatrix}$

Round 2:
$T := W_7 \lll 3 = 00100001$
$T :=$ SubBytes(0010)$\|$SubBytes(0001) :

$$\left\{\begin{array}{c} 0010^{-1} = (x)^{-1} = x^3 + 1 = 1001; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix}\cdot\begin{bmatrix}1\\0\\0\\1\end{bmatrix}+\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=0010\end{array}\right\}$$
$$\left\{\begin{array}{c} 0001^{-1} = (1)^{-1} = 1 = 0001; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix}\cdot\begin{bmatrix}1\\0\\0\\0\end{bmatrix}+\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\1\\1\\1\end{bmatrix}=1110\end{array}\right\}$$

$T := T \oplus RC_2 = 00101110 \oplus 00000110 = 00101000$
$W_8 := W_4 \oplus T = 01001111$
$W_9 := W_5 \oplus W_8 = 10101110$
$W_{10} := W_6 \oplus W_9 = 00101001$
$W_{11} := W_7 \oplus W_{10} = 00001101$
$(l(W_8) \otimes r(W_8)) \oplus l(W_8) \oplus r(W_8) =$
$(x^2 \otimes x^3 + x^2 + x + 1) \oplus x^2 \oplus x^3 + x^2 + x + 1 = x$
$(l(W_9) \otimes r(W_9)) \oplus l(W_9) \oplus r(W_9) =$
$(x^3 + x \otimes x^3 + x^2 + x) \oplus x^3 + x \oplus x^3 + x^2 + x = x$
$(l(W_{10}) \otimes r(W_{10})) \oplus l(W_{10}) \oplus r(W_{10}) =$
$(x \otimes x^3 + 1) \oplus x \oplus x^3 + 1 = x^3 + x$
$(l(W_{11}) \otimes r(W_{11})) \oplus l(W_{11}) \oplus r(W_{11}) =$
$(0 \otimes x^3 + x^2 + 1) \oplus 0 \oplus x^3 + x^2 + 1 = x^3 + x^2 + 1$
$K_2 := \begin{bmatrix}0010 & 1010\\0010 & 1101\end{bmatrix}$

Round 3:
$T := W_{11} \lll 3 = 01101000$
$T :=$ SubBytes(0110)$\|$SubBytes(1000) :

$$\left\{\begin{array}{c} 0110^{-1} = (x^2+x)^{-1} = x^2 + x + 1 = 0111; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix}\cdot\begin{bmatrix}1\\1\\1\\0\end{bmatrix}+\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\1\\1\end{bmatrix}=1100\end{array}\right\}$$
$$\left\{\begin{array}{c} 1000^{-1} = (x^3)^{-1} = x^3 + x^2 + x + 1 = 1111; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix}\cdot\begin{bmatrix}1\\1\\1\\1\end{bmatrix}+\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\0\\0\end{bmatrix}=0000\end{array}\right\}$$

$T := T \oplus RC_3 = 11000000 \oplus 00001100 = 11001100$
$W_{12} := W_8 \oplus T = 10000011$
$W_{13} := W_9 \oplus W_{12} = 00101101$
$W_{14} := W_{10} \oplus W_{13} = 00000100$
$W_{15} := W_{11} \oplus W_{14} = 00001001$
$(l(W_{12}) \otimes r(W_{12})) \oplus l(W_{12}) \oplus r(W_{12}) =$
$(x^3 \otimes x + 1) \oplus x^3 \oplus x + 1 = 0$
$(l(W_{13}) \otimes r(W_{13})) \oplus l(W_{13}) \oplus r(W_{13}) =$
$(x \otimes x^3 + x^2 + 1) \oplus x \oplus x^3 + x^2 + 1 = x^2 + x$
$(l(W_{14}) \otimes r(W_{14})) \oplus l(W_{14}) \oplus r(W_{14}) =$
$(0 \otimes x^2) \oplus 0 \oplus x^2 = x^2$
$(l(W_{15}) \otimes r(W_{15})) \oplus l(W_{15}) \oplus r(W_{15}) =$
$(0 \otimes x^3 + 1) \oplus 0 \oplus x^3 + 1 = x^3 + 1$
$K_3 := \begin{bmatrix}0000 & 0100\\0110 & 1001\end{bmatrix}$

Round 4:

$T := W_{15} \lll 3 = 01001000$

$T :=$ SubBytes$(0100)\|$SubBytes(1000) :

$$\left\{\begin{array}{c} 0100^{-1} = (x^2)^{-1} = x^3 + x^2 + 1 = 1101; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}1\\0\\1\\1\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\1\\1\end{bmatrix} = 1110 \end{array}\right\}$$

$$\left\{\begin{array}{c} 1000^{-1} = (x^3)^{-1} = x^3 + x^2 + x + 1 = 1111; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}1\\1\\1\\1\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\end{bmatrix} = 0000 \end{array}\right\}$$

$T := T \oplus RC_4 = 11100000 \oplus 00001011 = 11101011$

$W_{16} := W_{12} \oplus T = 01101000$

$W_{17} := W_{13} \oplus W_{16} = 01000101$

$W_{18} := W_{14} \oplus W_{17} = 01000001$

$W_{19} := W_{15} \oplus W_{18} = 01001000$

$(l(W_{16}) \otimes r(W_{16})) \oplus l(W_{16}) \oplus r(W_{16}) =$

$(x^2 + x \otimes x^3) \oplus x^2 + x \oplus x^3 = x^3 + x + 1$

$(l(W_{17}) \otimes r(W_{17})) \oplus l(W_{17}) \oplus r(W_{17}) =$

$(x^2 \otimes x^2 + 1) \oplus x^2 \oplus x^2 + 1 = x^2 + x$

$(l(W_{18}) \otimes r(W_{18})) \oplus l(W_{18}) \oplus r(W_{18}) =$

$(x^2 \otimes 1) \oplus x^2 \oplus 1 = 1$

$(l(W_{19}) \otimes r(W_{19})) \oplus l(W_{19}) \oplus r(W_{19}) =$

$(x^2 \otimes x^3) \oplus x^2 \oplus x^3 = x^3 + x$

$$K_4 := \begin{bmatrix}1011 & 0001\\0110 & 1010\end{bmatrix}$$

Round 5:

$T := W_{19} \lll 3 = 01000010$

$T :=$ SubBytes$(0100)\|$SubBytes(0010) :

$$\left\{\begin{array}{c} 0100^{-1} = (x^2)^{-1} = x^3 + x^2 + 1 = 1101; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}1\\0\\1\\1\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\1\\1\end{bmatrix} = 1110 \end{array}\right\}$$

$$\left\{\begin{array}{c} 0010^{-1} = (x)^{-1} = x^3 + 1 = 1001; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}1\\0\\0\\1\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} = 0010 \end{array}\right\}$$

$T := T \oplus RC_5 = 11100010 \oplus 00000101 = 11100111$

$W_{20} := W_{16} \oplus T = 10001111$

$W_{21} := W_{17} \oplus W_{20} = 11001010$

$W_{22} := W_{18} \oplus W_{21} = 10001011$

$W_{23} := W_{19} \oplus W_{22} = 11000011$

$(l(W_{20}) \otimes r(W_{20})) \oplus l(W_{20}) \oplus r(W_{20}) =$

$(x^3 \otimes x^3 + x^2 + x + 1) \oplus x^3 \oplus x^3 + x^2 + x + 1 = x^2 + x$

$(l(W_{21}) \otimes r(W_{21})) \oplus l(W_{21}) \oplus r(W_{21}) =$

$(x^3 + x^2 \otimes x^3 + x) \oplus x^3 + x^2 \oplus x^3 + x = x^2 + x + 1$

$(l(W_{22}) \otimes r(W_{22})) \oplus l(W_{22}) \oplus r(W_{22}) =$

$(x^3 \otimes x^3 + x + 1) \oplus x^3 \oplus x^3 + x + 1 = x^2$

$(l(W_{23}) \otimes r(W_{23})) \oplus l(W_{23}) \oplus r(W_{23}) =$

$(x^3 + x^2 \otimes x + 1) \oplus x^3 + x^2 \oplus x + 1 = x^3$

$$K_5 := \begin{bmatrix}0110 & 0100\\0111 & 1000\end{bmatrix}$$

Round 0: $L_0 = 1111000010101000, R_0 = 1011000100001001$

SubBytes: Taking Inverses for each entry of $\begin{bmatrix}1011 & 0000\\0001 & 1001\end{bmatrix}$ and performing the transformation:

$$\left\{\begin{array}{c} 1011^{-1} = (x^3 + x + 1)^{-1} = x^2 + 1 = 0101; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}1\\0\\1\\0\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} = 0010 \end{array}\right\}$$

$$\left\{\begin{array}{c} 0000^{-1} = (0)^{-1} = 0 = 0000; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}0\\0\\0\\0\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = 1001 \end{array}\right\}$$

$$\left\{\begin{array}{c} 0001^{-1} = (1)^{-1} = 1 = 0001; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\1\\1\end{bmatrix} = 1110 \end{array}\right\}$$

$$\left\{\begin{array}{c} 1001^{-1} = (x^3 + 1)^{-1} = x = 0010; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}0\\1\\0\\0\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}1\\1\\1\\0\end{bmatrix} = 0111 \end{array}\right\}$$

results in the matrix $\begin{bmatrix}0010 & 1001\\1110 & 0111\end{bmatrix}$

MultRoundKey: $\begin{bmatrix}1 & x^2 + x + 1\\x^3 + x + 1 & x^2\end{bmatrix} \cdot \begin{bmatrix}x & x^3 + 1\\x^3 + x^2 + x & x^2 + x + 1\end{bmatrix} = \begin{bmatrix}x^3 + x^2 + x & x^3 + x^2 + x + 1\\x^3 & x + 1\end{bmatrix}$

MixColumns: Remember that the matrix operations are performed in $\mathbb{F}_{2^4}$!

$$\begin{bmatrix} 0x03 & 0x07 \\ 0x04 & 0x03 \end{bmatrix} \cdot \begin{bmatrix} b_{0,1} \\ b_{1,1} \end{bmatrix} = \begin{bmatrix} x+1 & x^2+x+1 \\ x^2 & x+1 \end{bmatrix} \cdot \begin{bmatrix} x^3+x^2+x \\ x^3 \end{bmatrix} = \begin{bmatrix} 1100 \\ 0110 \end{bmatrix}$$

$$\begin{bmatrix} 0x03 & 0x07 \\ 0x04 & 0x03 \end{bmatrix} \cdot \begin{bmatrix} b_{0,2} \\ b_{1,2} \end{bmatrix} = \begin{bmatrix} x+1 & x^2+x+1 \\ x^2 & x+1 \end{bmatrix} \cdot \begin{bmatrix} x^3+x^2+x+1 \\ x+1 \end{bmatrix} = \begin{bmatrix} 1011 \\ 1100 \end{bmatrix}$$

The new state matrix is then $A := \begin{bmatrix} 1100 & 1011 \\ 0110 & 1100 \end{bmatrix}$.

ShiftRows: $A := \begin{bmatrix} 1100 & 1011 \\ 1100 & 0110 \end{bmatrix} = \begin{bmatrix} x^3+x^2 & x^3+x+1 \\ x^2+x & x^3+x^2 \end{bmatrix}$

$L_1 = 1011000100001001, R_1 = L_0 \oplus R_0 = 1111000010101000 \oplus 1100110010110110 = 0011110000011110$

Round 1: $L_1 = 1011000100001001, R_1 = 0011110000011110$

SubBytes: Taking Inverses for each entry of $\begin{bmatrix} 0011 & 0001 \\ 1100 & 1110 \end{bmatrix}$ and performing the transformation:

$$\left\{ \begin{array}{c} 0011^{-1} = (x+1)^{-1} = x^3+x^2+x = 1110; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = 0111 \end{array} \right\} \quad \left\{ \begin{array}{c} 0001^{-1} = (1)^{-1} = 1 = 0001; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = 1110 \end{array} \right\} \quad \left\{ \begin{array}{c} 1100^{-1} = (x^3+x^2)^{-1} = x^3+x = 1010; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 1011 \end{array} \right\}$$

$$\left\{ \begin{array}{c} 1110^{-1} = (x^3+x^2+x)^{-1} = x+1 = 0011; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 0000 \end{array} \right\}$$

results in the matrix $\begin{bmatrix} 0111 & 1110 \\ 1011 & 0000 \end{bmatrix}$

MultRoundKey: $\begin{bmatrix} 0 & x \\ 1 & x^3+x^2+x \end{bmatrix} \cdot \begin{bmatrix} x^2+x+1 & x^3+x^2+x \\ x^3+x+1 & 0 \end{bmatrix} = \begin{bmatrix} x^2+1 & 0 \\ x^3+x^2+x+1 & x^3+x^2+x \end{bmatrix}$

MixColumns: Remember that the matrix operations are performed in $\mathbb{F}_{2^4}$!

$$\begin{bmatrix} 0x03 & 0x07 \\ 0x04 & 0x03 \end{bmatrix} \cdot \begin{bmatrix} b_{0,1} \\ b_{1,1} \end{bmatrix} = \begin{bmatrix} x+1 & x^2+x+1 \\ x^2 & x+1 \end{bmatrix} \cdot \begin{bmatrix} x^2+1 \\ x^3+x^2+x+1 \end{bmatrix} = \begin{bmatrix} 0100 \\ 0101 \end{bmatrix}$$

$$\begin{bmatrix} 0x03 & 0x07 \\ 0x04 & 0x03 \end{bmatrix} \cdot \begin{bmatrix} b_{0,2} \\ b_{1,2} \end{bmatrix} = \begin{bmatrix} x+1 & x^2+x+1 \\ x^2 & x+1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ x^3+x^2+x \end{bmatrix} = \begin{bmatrix} 1100 \\ 0001 \end{bmatrix}$$

The new state matrix is then $A := \begin{bmatrix} 0100 & 1100 \\ 0101 & 0001 \end{bmatrix}$.

ShiftRows: $A := \begin{bmatrix} 0100 & 1100 \\ 0001 & 0101 \end{bmatrix} = \begin{bmatrix} x^2 & x^3+x^2 \\ x^2+1 & 1 \end{bmatrix}$

$L_2 = 0011110000011110, R_2 = L_1 \oplus R_1 = 1011000100001001 \oplus 0100000111000101 = 1111000011001100$

Round 2: $L_2 = 0011110000011110, R_2 = 1111000011001100$

SubBytes: Taking Inverses for each entry of $\begin{bmatrix} 1111 & 1100 \\ 0000 & 1100 \end{bmatrix}$ and performing the transformation:

$$\left\{\begin{array}{c} 1111^{-1} = (x^3+x^2+x+1)^{-1} = x^3 = 1000; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}0\\0\\0\\1\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}1\\0\\1\\0\end{bmatrix} = 0101 \end{array}\right\} \quad \left\{\begin{array}{c} 1100^{-1} = (x^3+x^2)^{-1} = x^3+x = 1010; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}0\\1\\0\\1\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}1\\1\\0\\1\end{bmatrix} = 1011 \end{array}\right\} \quad \left\{\begin{array}{c} 0000^{-1} = (0)^{-1} = 0 = 0000; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}0\\0\\0\\0\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = 1001 \end{array}\right\}$$

$$\left\{\begin{array}{c} 1100^{-1} = (x^3+x^2)^{-1} = x^3+x = 1010; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}0\\1\\0\\1\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}1\\1\\0\\1\end{bmatrix} = 1011 \end{array}\right\} \quad \text{results in the matrix } \begin{bmatrix}0101 & 1011\\1001 & 1011\end{bmatrix}$$

MultRoundKey: $\begin{bmatrix}x & x^3+x\\x & x^3+x^2+1\end{bmatrix} \cdot \begin{bmatrix}x^2+1 & x^3+x+1\\x^3+1 & x^3+x+1\end{bmatrix} = \begin{bmatrix}x^3+x^2+x+1 & x^2+x+1\\x^2+1 & x+1\end{bmatrix}$

MixColumns: Remember that the matrix operations are performed in $\mathbb{F}_{2^4}$!

$$\begin{bmatrix}0x03 & 0x07\\0x04 & 0x03\end{bmatrix} \cdot \begin{bmatrix}b_{0,1}\\b_{1,1}\end{bmatrix} = \begin{bmatrix}x+1 & x^2+x+1\\x^2 & x+1\end{bmatrix} \cdot \begin{bmatrix}x^3+x^2+x+1\\x^2+1\end{bmatrix} = \begin{bmatrix}1010\\0110\end{bmatrix}$$

$$\begin{bmatrix}0x03 & 0x07\\0x04 & 0x03\end{bmatrix} \cdot \begin{bmatrix}b_{0,2}\\b_{1,2}\end{bmatrix} = \begin{bmatrix}x+1 & x^2+x+1\\x^2 & x+1\end{bmatrix} \cdot \begin{bmatrix}x^2+x+1\\x+1\end{bmatrix} = \begin{bmatrix}0000\\1010\end{bmatrix}$$

The new state matrix is then $A := \begin{bmatrix}1010 & 0000\\0110 & 1010\end{bmatrix}$.

ShiftRows: $A := \begin{bmatrix}1010 & 0000\\1010 & 0110\end{bmatrix} = \begin{bmatrix}x^3+x & 0\\x^2+x & x^3+x\end{bmatrix}$

$L_3 = 1111000011001100, R_3 = L_2 \oplus R_2 = 0011110000011110 \oplus 1010101000000110 = 1001011000011000$

Round 3: $L_3 = 1111000011001100, R_3 = 1001011000011000$

SubBytes: Taking Inverses for each entry of $\begin{bmatrix}1001 & 0001\\0110 & 1000\end{bmatrix}$ and performing the transformation:

$$\left\{\begin{array}{c} 1001^{-1} = (x^3+1)^{-1} = x = 0010; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}0\\1\\0\\0\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}1\\1\\1\\0\end{bmatrix} = 0111 \end{array}\right\} \quad \left\{\begin{array}{c} 0001^{-1} = (1)^{-1} = 1 = 0001; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\1\\1\end{bmatrix} = 1110 \end{array}\right\} \quad \left\{\begin{array}{c} 0110^{-1} = (x^2+x)^{-1} = x^2+x+1 = 0111; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}1\\1\\1\\0\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\1\\1\end{bmatrix} = 1100 \end{array}\right\}$$

$$\left\{\begin{array}{c} 1000^{-1} = (x^3)^{-1} = x^3+x^2+x+1 = 1111; \\ \begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&1\\0&1&1&1\end{bmatrix} \cdot \begin{bmatrix}1\\1\\1\\1\end{bmatrix} + \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\end{bmatrix} = 0000 \end{array}\right\} \quad \text{results in the matrix } \begin{bmatrix}0111 & 1110\\1100 & 0000\end{bmatrix}$$

MultRoundKey: $\begin{bmatrix}0 & x^2\\x^2+x & x^3+1\end{bmatrix} \cdot \begin{bmatrix}x^2+x+1 & x^3+x^2+x\\x^3+x^2 & 0\end{bmatrix} = \begin{bmatrix}x^2+1 & 0\\x^2+x+1 & x\end{bmatrix}$

MixColumns: Remember that the matrix operations are performed in $\mathbb{F}_{2^4}$!

$$\begin{bmatrix}0x03 & 0x07\\0x04 & 0x03\end{bmatrix} \cdot \begin{bmatrix}b_{0,1}\\b_{1,1}\end{bmatrix} = \begin{bmatrix}x+1 & x^2+x+1\\x^2 & x+1\end{bmatrix} \cdot \begin{bmatrix}x^2+1\\x^2+x+1\end{bmatrix} = \begin{bmatrix}1001\\1110\end{bmatrix}$$

$$\begin{bmatrix}0x03 & 0x07\\0x04 & 0x03\end{bmatrix} \cdot \begin{bmatrix}b_{0,2}\\b_{1,2}\end{bmatrix} = \begin{bmatrix}x+1 & x^2+x+1\\x^2 & x+1\end{bmatrix} \cdot \begin{bmatrix}0\\x\end{bmatrix} = \begin{bmatrix}1110\\0110\end{bmatrix}$$

The new state matrix is then $A := \begin{bmatrix} 1001 & 1110 \\ 1110 & 0110 \end{bmatrix}$.

ShiftRows: $A := \begin{bmatrix} 1001 & 1110 \\ 0110 & 1110 \end{bmatrix} = \begin{bmatrix} x^3+1 & x^3+x^2+x \\ x^3+x^2+x & x^2+x \end{bmatrix}$

$L_4 = 1001011000011000, R_4 = L_3 \oplus R_3 = 1111000011001100 \oplus 1001011011101110 = 0110011000100010$

Round 4: $L_4 = 1001011000011000, R_4 = 0110011000100010$

SubBytes: Taking Inverses for each entry of $\begin{bmatrix} 0110 & 0010 \\ 0110 & 0010 \end{bmatrix}$ and performing the transformation:

$$\left\{ \begin{array}{c} 0110^{-1} = (x^2+x)^{-1} = x^2+x+1 = 0111; \\ \begin{bmatrix} 1&0&0&0 \\ 1&1&0&0 \\ 1&1&1&1 \\ 0&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = 1100 \end{array} \right\} \quad \left\{ \begin{array}{c} 0010^{-1} = (x)^{-1} = x^3+1 = 1001; \\ \begin{bmatrix} 1&0&0&0 \\ 1&1&0&0 \\ 1&1&1&1 \\ 0&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = 0010 \end{array} \right\} \quad \left\{ \begin{array}{c} 0110^{-1} = (x^2+x)^{-1} = x^2+x+1 = 0111; \\ \begin{bmatrix} 1&0&0&0 \\ 1&1&0&0 \\ 1&1&1&1 \\ 0&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = 1100 \end{array} \right\}$$

$$\left\{ \begin{array}{c} 0010^{-1} = (x)^{-1} = x^3+1 = 1001; \\ \begin{bmatrix} 1&0&0&0 \\ 1&1&0&0 \\ 1&1&1&1 \\ 0&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = 0010 \end{array} \right\} \quad \text{results in the matrix } \begin{bmatrix} 1100 & 0010 \\ 1100 & 0010 \end{bmatrix}$$

MultRoundKey: $\begin{bmatrix} x^3+x+1 & 1 \\ x^2+x & x^3+x \end{bmatrix} \cdot \begin{bmatrix} x^3+x^2 & x \\ x^3+x^2 & x \end{bmatrix} = \begin{bmatrix} 1 & x^2+x+1 \\ x^3+x^2+x+1 & x^3+x+1 \end{bmatrix}$

MixColumns: Remember that the matrix operations are performed in $\mathbb{F}_{2^4}$!

$$\begin{bmatrix} 0x03 & 0x07 \\ 0x04 & 0x03 \end{bmatrix} \cdot \begin{bmatrix} b_{0,1} \\ b_{1,1} \end{bmatrix} = \begin{bmatrix} x+1 & x^2+x+1 \\ x^2 & x+1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ x^3+x^2+x+1 \end{bmatrix} = \begin{bmatrix} 1000 \\ 0110 \end{bmatrix}$$

$$\begin{bmatrix} 0x03 & 0x07 \\ 0x04 & 0x03 \end{bmatrix} \cdot \begin{bmatrix} b_{0,2} \\ b_{1,2} \end{bmatrix} = \begin{bmatrix} x+1 & x^2+x+1 \\ x^2 & x+1 \end{bmatrix} \cdot \begin{bmatrix} x^2+x+1 \\ x^3+x+1 \end{bmatrix} = \begin{bmatrix} 1101 \\ 0001 \end{bmatrix}$$

The new state matrix is then $A := \begin{bmatrix} 1000 & 1101 \\ 0110 & 0001 \end{bmatrix}$.

ShiftRows: $A := \begin{bmatrix} 1000 & 1101 \\ 0001 & 0110 \end{bmatrix} = \begin{bmatrix} x^3 & x^3+x^2+1 \\ x^2+x & 1 \end{bmatrix}$

$L_5 = 0110011000100010, R_5 = L_4 \oplus R_4 = 1001011000011000 \oplus 1000000111010110 = 0001011111001110$

Round 5: $L_5 = 0110011000100010, R_5 = 0001011111001110$

SubBytes: Taking Inverses for each entry of $\begin{bmatrix} 0001 & 1100 \\ 0111 & 1110 \end{bmatrix}$ and performing the transformation:

$$\left\{ \begin{array}{c} 0001^{-1} = (1)^{-1} = 1 = 0001; \\ \begin{bmatrix} 1&0&0&0 \\ 1&1&0&0 \\ 1&1&1&1 \\ 0&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = 1110 \end{array} \right\} \quad \left\{ \begin{array}{c} 1100^{-1} = (x^3+x^2)^{-1} = x^3+x = 1010; \\ \begin{bmatrix} 1&0&0&0 \\ 1&1&0&0 \\ 1&1&1&1 \\ 0&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 1011 \end{array} \right\} \quad \left\{ \begin{array}{c} 0111^{-1} = (x^2+x+1)^{-1} = x^2+x = 0110; \\ \begin{bmatrix} 1&0&0&0 \\ 1&1&0&0 \\ 1&1&1&1 \\ 0&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 1011 \end{array} \right\}$$

$$\left\{ \begin{array}{l} 1110^{-1} = (x^3+x^2+x)^{-1} = x+1 = 0011; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 0000 \end{array} \right\} \qquad \text{results in the matrix } \begin{bmatrix} 1110 & 1011 \\ 1011 & 0000 \end{bmatrix}$$

MultRoundKey: $\begin{bmatrix} x^2+x & x^2 \\ x^2+x+1 & x^3 \end{bmatrix} \cdot \begin{bmatrix} x^3+x^2+x & x^3+x+1 \\ x^3+x+1 & 0 \end{bmatrix} = \begin{bmatrix} x^3 & x^3+x^2+x+1 \\ x^3+x+1 & x^2 \end{bmatrix}$

MixColumns: Remember that the matrix operations are performed in $\mathbb{F}_{2^4}$!

$$\begin{bmatrix} 0x03 & 0x07 \\ 0x04 & 0x03 \end{bmatrix} \cdot \begin{bmatrix} b_{0,1} \\ b_{1,1} \end{bmatrix} = \begin{bmatrix} x+1 & x^2+x+1 \\ x^2 & x+1 \end{bmatrix} \cdot \begin{bmatrix} x^3 \\ x^3+x+1 \end{bmatrix} = \begin{bmatrix} 1111 \\ 1000 \end{bmatrix}$$
$$\begin{bmatrix} 0x03 & 0x07 \\ 0x04 & 0x03 \end{bmatrix} \cdot \begin{bmatrix} b_{0,2} \\ b_{1,2} \end{bmatrix} = \begin{bmatrix} x+1 & x^2+x+1 \\ x^2 & x+1 \end{bmatrix} \cdot \begin{bmatrix} x^3+x^2+x+1 \\ x^2 \end{bmatrix} = \begin{bmatrix} 1101 \\ 0101 \end{bmatrix}$$

The new state matrix is then $A := \begin{bmatrix} 1111 & 1101 \\ 1000 & 0101 \end{bmatrix}$.

ShiftRows: $A := \begin{bmatrix} 1111 & 1101 \\ 0101 & 1000 \end{bmatrix} = \begin{bmatrix} x^3+x^2+x+1 & x^3+x^2+1 \\ x^3 & x^2+1 \end{bmatrix}$

$L_6 = 0001011111001110, R_6 = L_5 \oplus R_5 = 0110011000100010 \oplus 1111010111011000 = 1001001111111010$

$$E_K(11110000101010001011000100001001) = 10010011111110100001011111001110$$

$$C_1 = E_K(IV) \oplus M_1 = 10010011111110100001011111001110 \oplus 10110010111101101011000100100111 = 00100001000011001010011011101001$$

...and so on using CFB mode of operation, omitting the cipher output now ...

$$E_K(00100001000011001010011011101001) = 01101100011101001010000001000110$$

$$C_2 = E_K(C_1) \oplus M_2 = 01101100011101001010000001000110 \oplus 01101001101001001000001101000001 = 00000101110100000010001100000111$$

$$E_K(00000101110100000010001100000111) = 10100001101101010101001011000001$$

$$C_3 = E_K(C_2) \oplus M_3 = 10100001101101010101001011000001 \oplus 11100100000100100011110001010110 = 01000101101001110110111010010111$$

$$C_1 \| C_2 \| C_3 = 00100001000011001010011011101001 \| 00000101110100000010001100000111 \| 01000101101001110110111010010111$$