

Programming Exercise 1

Exercise Problems

Please commit the answers to these problems with your code via boss.

- (a) $M = 10100111110011010110011000110100\ 00101100100000100110110110001011$
 $00101011110100101110010000010010,$
 $K = 01100100011010001111110101101110,$
 $IV = 01101100000011011111000000110010.$
- (b) $M = 11001100000110101000100101011001\ 00001000001001100011001010000010$
 $01010001000010010111001100110000,$
 $K = 01001101010010100010110110111110,$
 $IV = 10110100101111110110111110100111.$
- (c) $M = 00001011110100011110001101100100\ 00100110001011000101010101100100$
 $00011000110111011010000011001001,$
 $K = 01000110111001000110110010110000,$
 $IV = 11011111010101110111111011000010.$
- (d) $M = 11110101101000010100101110101011\ 10000000111100000000100110001000$
 $10100111110111101001111101001100\ 11001100010001010000110010111010,$
 $K = 11001010110011100001100101101001,$
 $IV = 11100000111000001101010010101101.$
- (e) $M = 11011001011000001000100111000101\ 00110110010000001010110001001100$
 $11101111000110100010111001101101\ 10101110011011011001010000100110,$
 $K = 000010010010010001100110100011111,$
 $IV = 01011100011111011100001110000000.$
- (f) $M = 11000001111110110100000111000010\ 10111101100110110000111011001101$
 $1011111000111101110110111111100\ 01111001100010011100100011101110,$
 $K = 10101101110000011001011001011011,$
 $IV = 01100110000100111011101001000110.$
- (g) $M = 01100110110111001110010000110111\ 01100001111000001001001001000100$
 $00010011011100101000110110010000\ 11000011001011100000101010010100$
 $00111101011010110010010100101001,$
 $K = 10000011011001000101001001110011,$
 $IV = 00100011010101000000111000001110.$
- (h) $M = 01000000110000011011100100000100\ 00101111000101001001010010111001$
 $10000001001110001010110000000010\ 00111101011011011000011101010101$
 $11010010100101100011110011110101,$
 $K = 00001010010111000101000010010100,$
 $IV = 00011111100100011101010001100100.$

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:

$$T := W_3 \lll 3 = 00011101$$

$$T := \text{SubBytes}(0001) || \text{SubBytes}(1101) :$$

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

$$T := T \oplus RC_1 = 11100101 \oplus 00000011 = 11100110$$

$$W_4 := W_0 \oplus T = 01100111$$

$$W_5 := W_1 \oplus W_4 = 11100001$$

$$W_6 := W_2 \oplus W_5 = 10000111$$

$$W_7 := W_3 \oplus W_6 = 00100100$$

$$(l(W_4) \otimes r(W_4)) \oplus l(W_4) \oplus r(W_4) =$$

$$(x^2 + x \otimes x^2 + x + 1) \oplus x^2 + x \oplus x^2 + x + 1 = 0$$

$$(l(W_5) \otimes r(W_5)) \oplus l(W_5) \oplus r(W_5) =$$

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

$$(l(W_6) \otimes r(W_6)) \oplus l(W_6) \oplus r(W_6) =$$

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

$$(l(W_7) \otimes r(W_7)) \oplus l(W_7) \oplus r(W_7) =$$

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

$$K_1 := \begin{bmatrix} 0000 & 0010 \\ 0001 & 1110 \end{bmatrix}$$

Round 2:

$$T := W_7 \lll 3 = 00100001$$

$$T := \text{SubBytes}(0010) || \text{SubBytes}(0001) :$$

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

$$T := T \oplus RC_2 = 00101110 \oplus 00000110 = 00101000$$

$$W_8 := W_4 \oplus T = 01001111$$

$$W_9 := W_5 \oplus W_8 = 10101110$$

$$W_{10} := W_6 \oplus W_9 = 00101001$$

$$W_{11} := W_7 \oplus W_{10} = 00001101$$

$$(l(W_8) \otimes r(W_8)) \oplus l(W_8) \oplus r(W_8) =$$

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

$$(l(W_9) \otimes r(W_9)) \oplus l(W_9) \oplus r(W_9) =$$

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

$$(l(W_{10}) \otimes r(W_{10})) \oplus l(W_{10}) \oplus r(W_{10}) =$$

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

$$(l(W_{11}) \otimes r(W_{11})) \oplus l(W_{11}) \oplus r(W_{11}) =$$

$$(0 \otimes x^3 + x^2 + 1) \oplus 0 \oplus x^3 + x^2 + 1 = x^3 + x^2 + 1$$

$$K_2 := \begin{bmatrix} 0010 & 1010 \\ 0010 & 1101 \end{bmatrix}$$

Round 3:

$$T := W_{11} \lll 3 = 01101000$$

$$T := \text{SubBytes}(0110) || \text{SubBytes}(1000) :$$

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

$$T := T \oplus RC_3 = 11000000 \oplus 00001100 = 11001100$$

$$W_{12} := W_8 \oplus T = 10000011$$

$$W_{13} := W_9 \oplus W_{12} = 00101101$$

$$W_{14} := W_{10} \oplus W_{13} = 00000100$$

$$W_{15} := W_{11} \oplus W_{14} = 00001001$$

$$(l(W_{12}) \otimes r(W_{12})) \oplus l(W_{12}) \oplus r(W_{12}) =$$

$$(x^3 \otimes x + 1) \oplus x^3 \oplus x + 1 = 0$$

$$(l(W_{13}) \otimes r(W_{13})) \oplus l(W_{13}) \oplus r(W_{13}) =$$

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

$$(l(W_{14}) \otimes r(W_{14})) \oplus l(W_{14}) \oplus r(W_{14}) =$$

$$(0 \otimes x^2) \oplus 0 \oplus x^2 = x^2$$

$$(l(W_{15}) \otimes r(W_{15})) \oplus l(W_{15}) \oplus r(W_{15}) =$$

$$(0 \otimes x^3 + 1) \oplus 0 \oplus x^3 + 1 = x^3 + 1$$

$$K_3 := \begin{bmatrix} 0000 & 0100 \\ 0110 & 1001 \end{bmatrix}$$

Round 4:

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

$$T := \text{SubBytes}(0100) \parallel \text{SubBytes}(1000) :$$

$$\left\{ \begin{array}{l} 0100^{-1} = (x^2)^{-1} = x^3 + x^2 + 1 = 1101; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = 1110 \\ 1000^{-1} = (x^3)^{-1} = x^3 + x^2 + x + 1 = 1111; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 0000 \end{array} \right\}$$

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

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

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

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

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

$$(l(W_{16}) \otimes r(W_{16})) \oplus l(W_{16}) \oplus r(W_{16}) = (x^2 + x \otimes x^3) \oplus x^2 + x \oplus x^3 = x^3 + x + 1$$

$$(l(W_{17}) \otimes r(W_{17})) \oplus l(W_{17}) \oplus r(W_{17}) = (x^2 \otimes x^2 + 1) \oplus x^2 \oplus x^2 + 1 = x^2 + x$$

$$(l(W_{18}) \otimes r(W_{18})) \oplus l(W_{18}) \oplus r(W_{18}) = (x^2 \otimes 1) \oplus x^2 \oplus 1 = 1$$

$$(l(W_{19}) \otimes r(W_{19})) \oplus l(W_{19}) \oplus r(W_{19}) = (x^2 \otimes x^3) \oplus x^2 \oplus x^3 = x^3 + x$$

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

Round 5:

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

$$T := \text{SubBytes}(0100) \parallel \text{SubBytes}(0010) :$$

$$\left\{ \begin{array}{l} 0100^{-1} = (x^2)^{-1} = x^3 + x^2 + 1 = 1101; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = 1110 \\ 0010^{-1} = (x)^{-1} = x^3 + 1 = 1001; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = 0010 \end{array} \right\}$$

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

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

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

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

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

$$(l(W_{20}) \otimes r(W_{20})) \oplus l(W_{20}) \oplus r(W_{20}) = (x^3 \otimes x^3 + x^2 + x + 1) \oplus x^3 \oplus x^3 + x^2 + x + 1 = x^2 + x$$

$$(l(W_{21}) \otimes r(W_{21})) \oplus l(W_{21}) \oplus r(W_{21}) = (x^3 + x^2 \otimes x^3 + x) \oplus x^3 + x^2 \oplus x^3 + x = x^2 + x + 1$$

$$(l(W_{22}) \otimes r(W_{22})) \oplus l(W_{22}) \oplus r(W_{22}) = (x^3 \otimes x^3 + x + 1) \oplus x^3 \oplus x^3 + x + 1 = x^2$$

$$(l(W_{23}) \otimes r(W_{23})) \oplus l(W_{23}) \oplus r(W_{23}) = (x^3 + x^2 \otimes x + 1) \oplus x^3 + x^2 \oplus x + 1 = x^3$$

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

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:

$$\left\{ \begin{array}{l} 1011^{-1} = (x^3 + x + 1)^{-1} = x^2 + 1 = 0101; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = 0010 \\ 1001^{-1} = (x^3 + 1)^{-1} = x = 0010; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = 0111 \end{array} \right\}$$

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

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

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

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

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:

$$\left\{ \begin{array}{l} 0011^{-1} = (x+1)^{-1} = x^3+x^2+x = 1110; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = 0111 \end{array} \right\}$$

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

$$\left\{ \begin{array}{l} 1100^{-1} = (x^3+x^2)^{-1} = x^3+x = 1010; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 1011 \end{array} \right\}$$

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

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:

$$\left\{ \begin{array}{l} 1111^{-1} = (x^3 + x^2 + x + 1)^{-1} = x^3 = 1000; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 0101 \end{array} \right\}$$

$$\left\{ \begin{array}{l} 1100^{-1} = (x^3 + x^2)^{-1} = x^3 + x = 1010; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 1011 \end{array} \right\}$$

$$\left\{ \begin{array}{l} 1100^{-1} = (x^3 + x^2)^{-1} = x^3 + x = 1010; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 1011 \end{array} \right\}$$

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

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:

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

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

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

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

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:

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

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

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

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:

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

$$\left\{ \begin{array}{l} 0111^{-1} = (x^2 + x + 1)^{-1} = x^2 + x = 0110; \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 1011 \end{array} \right\}$$

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

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

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 $A := \begin{bmatrix} 1111 & 1101 \\ 1000 & 0101 \end{bmatrix}$.

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

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

$$E_K(11110000101010001011000100001001) = 10010011111110100001011111001110$$

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

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

$$E_K(00100001000011001010011011101001) = 01101100011101001010000001000110$$

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

$$E_K(00000101110100000010001100000111) = 10100001101101010101001011000001$$

$$C_3 = E_K(C_2) \oplus M_3 = 101000011011010101001011000001 \oplus 11100100000100100011110001010110 = 01000101101001110110111010010111$$

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

Debugging Examples

Here are some debug examples for the cipher:

- $M = 01010111001000111000010011010100$, $K = 11100000011100110010110010001000$,
 $C = 10100111100011110110110111000011$.
- $M = 10010101110101000001101101101000$, $K = 11001110111001001001011011000011$,
 $C = 10100100111101101101010101110000$.
- $M = 00111001010010111011110101010010$, $K = 00000100100011001101010001111100$,
 $C = 01101100111000000110001011101001$.
- $M = 11000000010100110000100110111110$, $K = 11010010001111010010110101100011$,
 $C = 10101110001110011101111010100010$.
- $M = 01000001010011011110100111000101$, $K = 11010010001000101001111100100011$,
 $C = 10011010101011000110101010110000$.

Here are some debug examples for CFB mode with the cipher:

- $M = 10110010111101101011000100100111\ 01101001101001001000001101000001$
 $11100100000100100011110001010110$,
 $K = 10000001100001100110011010100011$,
 $IV = 11110000101010001011000100001001$,
 $C = 00100001000011001010011011101001\ 00000101110100000010001100000111$
 $01000101101001110110111010010111$.
- $M = 10010100101110011001001110101010\ 10001100000101100101000100110100$
 $00101000011101100111011000111100$,
 $K = 01101100010101001000110010001111$,
 $IV = 11110101100101000001111101100001$,
 $C = 11100011111000001101010101110111\ 00001001101000100001100001111100$
 $11000111101110001101000001011011$.
- $M = 00100110001110000010000111001010\ 001111010111010111000001000000010$
 $01000001111011000000111110000100$,
 $K = 00100011011111001110010000101110$,
 $IV = 11000011000000001101000100011011$,
 $C = 01110001101000000010011010101000\ 01111111000111101011011110010101$
 $11110001010000001100000001110111$.
- $M = 11101000010010010000110111011100\ 00110010010101000001000011100001$
 $11011001001101010010111101101010\ 01000000010001110000100000001010$,
 $K = 00110111100111001110011000100111$,
 $IV = 01011001100110001000100100111001$,
 $C = 11110101010001101000101101001010\ 01100001101110101000000000010100$
 $11111001001100100101011100001010\ 00110110111010000011000111101001$.

- $M = 11000111011001011101011100011111\ 01111001001010010111010100100111$
 $11111100110010100010011101110011\ 01011010000001100101101110010111,$
- $K = 11110100011111000000100000011101,$
- $IV = 10011101101101010001101010000101,$
- $C = 01000000100100010111011001101000\ 11101001110110011000110010000001$
 $01110011110111000010000000011010\ 1110011101011010111010111111101.$