AES-3)

$((ax^3+bx^2+cx+d)\cdot z+(ex^3+fx^2+gx+h))\cdot(xz+x^3+1)$

$= ax^6z+ax^4z^2+ax^3z+bx^3z^2+bx^2z+cx^4z+cx^2z^2+cxz+dx^3z+dxz^2+$

$dz+ex^6+ex^4z+ex^3+fx^5+fx^3z+fx^2+gx^4+gx^2z+gx+hx^3+hxz+h$

$= a(x^3+x^2)z+a(x+1)+ax^3z+b(x^2+x)z+bx^3+bx^2z+c(x+1)z+cx^2+$

$cxz+dx^3z+dxz^2+dz+e(x^3+x^2)+e(x+1)z+ex^3+f(x^2+x)+fx^3z+$

$fx^2+g(x+1)+gx^2z+gx+hx^3+hxz+h$

$= ax^3z+ax^2z+ax+a+ax^3z+bx^2z+bxz+bx^3+bx^2z+cxz+cz+cx^2+$

$cxz+dx^3z+dxz^2+dz+ex^3+ex^2+exz+ez+ex^3+fx^2+fx+fx^3z+fx^2+$

$gx+g+gx^2z+gx+hx^3+hxz+h$

$= dx^3z+fx^3z+bx^3+hx^3+ax^2z+bx^2z+gx^2z+cx^2+ex^2+bxz+exz+$

$hxz+ax+dx+fx+cz+dz+ez+a+g+h$

$d\oplus f$	$a\oplus b\oplus g$	$b\oplus e\oplus h$	$c\oplus d\oplus e$
$b\oplus h$	$c\oplus g$	$a\oplus d\oplus f$	$a\oplus g\oplus h$

$=$

$b_3\oplus b_5$	$b_0\oplus b_1\oplus b_6$	$b_1\oplus b_4\oplus b_7$	$b_2\oplus b_5\oplus b_4$
$b_1\oplus b_7$	$b_2\oplus b_4$	$b_0\oplus b_3\oplus b_5$	$b_0\oplus b_6\oplus b_7$

AES-4) $RCON(1) = 1000\,0000$ $RCON(2) = 0011\,0000$

i) $W[0] = 1011\ 1101$

$W[1] = 0010\ 0101$

$W[2] = W[0]\oplus RCON(1)\oplus Sub(Rot(W[1]))$

$Rot(W[1]) = 0101\ 0010$

$Sub(Rot(W[1])) = 0001\ 1010$

$W[2] = 1011\ 1101 \oplus 1000\ 0000 \oplus 0001\ 1010$

$= 0010\ 0111$

$W[3] = W[1] \oplus W[2] = 0010\ 0101 \oplus 0010\ 0111$

$= 0000\ 0010$

$W[4] = W[2] \oplus RCON[2] \oplus Sub(Rot(W[3]))$

$Rot(W[3]) = 0010\ 0000$

$Sub(Rot(W[3])) = 1010\ 1001$

$W[4] = 0010\ 0111 \oplus 0011\ 0000 \oplus 1010\ 1001$

$= 1011\ 1110$

$W[5] = W[3] \oplus W[4] = 0000\ 0010 \oplus 1011\ 1110$

$= 1011\ 1100$

$K_0 = 1011\ 1101\ 0010\ 0101$

$K_1 = 0010\ 0111\ 0000\ 0010$

$K_2 = 1011\ 1110\ 1011\ 1100$

$K = 1011\ 1101\ 0010\ 0101\ 0010\ 0111\ 0000\ 0010\ 1011\ 1110$
$1011\ 1100$

ii) $1011\ 1101\ 0010\ 0101 \rightarrow 1111\ 1110\ 0100\ 0001$

iii) $A_{K_0} \circ SR^{-1} \circ NS^{-1} \circ A_{C(2)^{-1}K_1} \circ MC^{-1} \circ SR^{-1} \circ NS^{-1} \circ A_{K_2}$

$CT_0 \oplus A_{K_2} = 0111\ 0001\ 0011\ 1001 \oplus 1011\ 1110\ 1011\ 1100$

$= CT_1 = 1100\ 1111\ 1000\ 0101$

$NS^{-1}(CT_1) = CT_2 =$ 1100 1110 0110 0111

$SR^{-1}(CT_2) = CT_3 =$ 1100 0111 0110 1110

$MC^{-1}(CT_3) = CT_4 =$ 1000 0001 1100 1011

$CT_4 \oplus A_{(C^{-1})^{-1}K_1} = CT_5 =$ 0111 1111 1000 1010

$NS^{-1}(CT_5) = CT_6 =$ 1111 1110 0110 0010

$SR^{-1}(CT_6) = CT_7 =$ 1111 0010 0110 1110

$CT_7 \oplus A_{K0} = PT =$ 0100 1111 0100 1011

$PT = OK$