AES-5) IV= 1000 1101 0000 1011

K= 1100 1011 1111 1110

$COEN_{PT}$ = 01000011 01001111 01000101 00001010

$W[0]$ = 1100 1011

$W[1]$ = 1111 1110

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

$$\begin{array}{r} = 11001011 \oplus \\ 1110\ 1111 \\ \oplus\ \underline{1111\ 0111} \\ 11010011 \end{array}$$

= 1101 0011

$W[3] = W[1] \oplus W[2]$ = $\begin{array}{r} 1111\ 1110 \\ \underline{1101\ 0011} \\ 00101101 \end{array}$ = 0010 1101

$W[4] = W[2] \oplus RCON(2) \oplus Sub(RCON(2))$ = $\begin{array}{r} 11010011 \\ 0011\ 1101 \\ \oplus\ \underline{1011\ 1110} \\ 01010000 \end{array}$

= 0101 0000

$W[5] = W[3] \oplus W[4]$ = $\begin{array}{r} 00101101 \\ \oplus\ \underline{01010000} \\ 01111101 \end{array}$

K_0 = 1100 1011 1111 1110

K_1 = 1101 0011 0010 1101

K_2 = 0101 0000 0111 1101

$A_{K2} \circ SR \circ NS \circ A_{K1} \circ ML \circ SR \circ NS \circ A_{K0}$

CO

$CT_0 =$ 01000011 01001111

10001101 00001011

11001110 01000100

$CT_1 = CT_0 \oplus K_0 =$ 11001110 01000100

11001011 11111110

00000101 1011 1010

$CT_2 = NS(CT_1) =$ S(0000) = 1001 S(1011) = 0011

S(0101) = 0001 S(1010) = 0000

$CT_3 = RS(CT_2) =$

0 1 2 3 0 1 2 3

1001 0011

0000 0001

4 5 6 7 4 5 6 7

$CT_4 = ML(CT_3) =$ 1001 0111

0010 1101

$CT_5 = CT_4 \oplus K_1 =$ 1001 0010 0111 1101

$\oplus$ 1101 0011 0010 1101

0100 0001 0101 0000

0 1 2 3

$CT_6 = NS(CT_5) =$ 1101 0100 0001 1001

$CT_7 = SR(CT_6) =$ 1101 1001 0001 0100

$CT_8 = CT_7 \oplus K_2 = 1101\ 1001\ 0001\ 0100$

$0101\ 0000\ 0111\ 1101$ $\quad\underline{0101\ 0000\ 0111\ 1101}$

$1000\ 1001\ 0110\ 1001$

EN

$A_{K2} \circ SR \circ NS \circ A_{K1} \circ ML \circ SR \circ NS \circ A_{K0}$

$CT_0 = \quad 01000101\ 00001010$

$\oplus\ \underline{10001101\ 00001011}$

$11001000\ 00000001$

$K_0 = 11001011\ 11111110$

$K_1 = 11010011\ 00101101$

$K_2 = 01010000\ 01111101$

$CT_1 = CT_0 \oplus K_0 = 1100\ 1000\ 0000\ 0001$

$\underline{1100\ 1011\ 1111\ 1110}$

$0000\ 0011\ 1111\ 1111$

$CT_2 = NS(CT_1) = 0000\ 1111\ 1111\ 0011$

$0\ 1\ 2\ 3\quad 4\ 5\ 6\ 7\quad 0\ 1\ 2\ 3\quad 4\ 5\ 6\ 7$

$CT_3 = SR(CT_2) = 1001\ 0111\ 0111\ 1011$

$CT_4 = ML(CT_3) = 1010\ 0100\ 1101\ 1100$

$CT_5 = CT_4 \oplus K_1 = 1010\ 0100\ 1101\ 1100$

$\oplus\ \underline{1101\ 0011\ 0010\ 1101}$

$0111\ 0111\ 1111\ 0001$

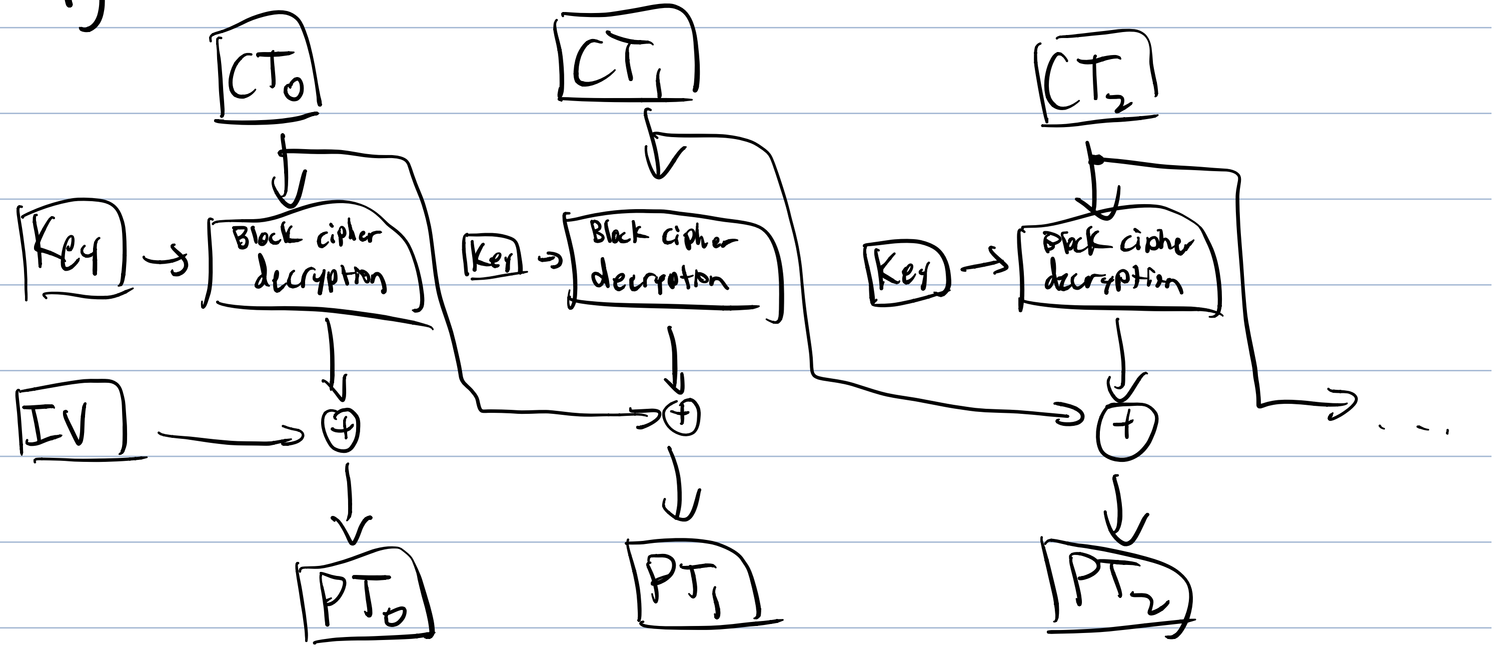
$CT_6 = NS(CT_5) = 0111\ 0001\ 1111\ 0111$

$CT_7 = SR(CT_6) = 0101\ 0100\ 0111\ 0101$

$$
\begin{array}{rl}
CT_8 = CT_7 \oplus K_2 = & 0101\ 0100\ 0111\ 0101 \\
\oplus & 0101\ 0000\ 0111\ 1101 \\
\hline
& 0000\ 0100\ 0000\ 1000
\end{array}
$$

AES-8)

i)



ii) Bob would only be able to correctly determine PT1 - PT3, due to the fact a single bit can chang all resulting bits in the next CT/PT, or diffusion in AES.

iii) Bob would still would still only beable to determine PT1 - PT3, as AES diffusion still affects all resulting bits if a single bit is messed up.