Network Security

Exercises 2
Question 2

Tobias Famos
16-933-764

March 13, 2022

1 Initail State

The initial state

$$\begin{bmatrix} 0F & 0E & 0D & 0C \\ 0B & 0A & 09 & 08 \\ 07 & 06 & 05 & 04 \\ 03 & 02 & 01 & 00 \end{bmatrix}$$

The Key:

$$\begin{bmatrix} 02 & 02 & 02 & 02 \\ 02 & 02 & 02 & 02 \\ 02 & 02 & 02 & 02 \\ 02 & 02 & 02 & 02 \end{bmatrix}$$

After First Roundkey

$$\begin{bmatrix} 0D & 0C & 0F & 0E \\ 09 & 08 & 0B & 0A \\ 05 & 04 & 07 & 06 \\ 01 & 00 & 03 & 02 \end{bmatrix}$$

After Sub Bytes

$$\begin{bmatrix} D7 & FE & 76 & AB \\ 01 & 30 & 2B & 67 \\ 6B & F2 & C5 & 6F \\ 7C & 63 & 7B & 77 \end{bmatrix}$$

After Shift Rows

$$\begin{bmatrix} D7 & FE & 76 & AB \\ 30 & 2B & 67 & 01 \\ C5 & 6F & 6B & F2 \\ 77 & 7C & 63 & 7B \end{bmatrix}$$

After Mix columns

$$\begin{bmatrix} 7A & 68 & EF & C6 \\ FD & 1D & E8 & FE \\ F6 & 7B & DC & 01 \\ 68 & 8C & FA & EA \end{bmatrix}$$