Muhammad Izham Bin Norhamadi
B032020039
S2G1
BITZ

Tutorial 3a: AES S-box

1. Take $a = 100 + y$, convert to hexa, take $a^{-1} \pmod b$ from an inverse table

y = 39

a = 139 = $10001011_2 = 8B_{16}$

$a^{-1} = D9_{16}$

2. An irreducible polynomial $b(x) = x^8 + x^4 + x^3 + x + 1$ where $b(2) = 283_{10}$.
3. Plug in an inverse into an Affine Transform to get an output for AES S-box.

$a^{-1} = D9_{16} = 11011001_2$

$b(x) = x^8 + x^4 + x^3 + x + 1 = 100011011_2 = 11B_{16}$

$$\begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

= 00111101 = $3D_{16}$