Muhammad Izham Bin Norhamadi  
B032020039  
S2G1

BITZ

**Tutorial 3a: AES S-box**

1. Take *a* = 100 + y, convert to hexa, take *a*1 (mod *b*) from an inverse table

y = 39

a = 139 = 100010112 = 8B16

*a*-1 = D916

1. An irreducible polynomial *b*(*x*) = *x* 8+ *x*4+ *x*3+*x*+1 where *b*(2) = 28310.
2. Plug in an inverse into an Affine Transform to get an output for AES S-box.

*a*-1 = D916 = 110110012

*b*(*x*) = *x* 8+ *x*4+ *x*3+*x*+1 = 1000110112 = 11B16

= 00111101 = 3D16