Problem Set #4

Supplemental Problems

1. If $A_0 = 6A$ is the input to the Byte Substitution layer in AES, verify that the output of the S-box is $B_0 = 02$. You can use Table 4.2 to find ${A_0}^{-1}$, but you should compute the affine map by hand.

2. Suppose the input to the Byte Substitution layer of AES is the following:

A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}
$6A$	09	$A6$	72	$E3$	$6A$	$7C$	$E3$	$A6$	$A3$	72	$7C$	$A6$	82	09	$6A$

   What is the output C_0, C_6 and C_{15} from the Mix Columns layer?

   For this problem, you can use Table 4.3 to find the output from the S-box in the Byte Substitution layer.