1. *a. The elements of GF(19) would be* **{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18} with p = 19**

   b. The additive inverse of 9 on Gf(19) would be calculated with: **-9+19, with the additive inverse coming out as 10.**

   *C. For the multiplicative inverse, we keep plugging 9*x mod 19 until we get 1, so:*

   *9 mod 19 = 9 | 9*2 mod 19 = 1.* **The multiplicative inverse of 9 in GF(19) is 1**

2. *a. the Extension field of GF(2^6) with A(x) = 17 would be:*

   A = x^4 + 1, with X being 2 from the GF. 2^4 *= 2*2=4*2=8*2=16 + 1 = 17*

   (I struggled to understand this one, so I don't know how to properly write it.)

   b. for B(x) = 8, it would look like

   B = x^3 + 0, X being 2 again. 2*2 = 4 *2 = 8

   c. *for C(x) = 1, it would be*

   C = x^0, X again being 2, but 2^0 comes out as 1

   d. *A(x) + B(x) in poly form would be:* **x^4 + x^3 + 1, and the integer it comes out to would be 25.**

   e. *B(x) + C(x) in poly form would be:* **x^3 + x^0 , it the integer would comes out to 9.**

   3. If GF(2^8), determine the multiplicative inverses of $4D_{16}$ and $4E_{16}$ would be:

   4D: x=2, y=5 | 4E: x= E, y= 9

   4. If GF(2^8), determine the AES S-box substitutions of $5E_{16}$ and $5F_{16}$:

   5E: x=9, y=D | 5F: x=8, y=4

5.

E5	B0	7B	92
C2	C8	1F	33
D6	F9	8E	74
A8	9C	06	85

After shifting, it becomes:

E5	**B0**	**7B**	**92**
C8	**1F**	**33**	**C2**
8E	**74**	**D6**	**F9**
85	**A8**	**9C**	**06**