Problem Set #4

Supplemental Problems

1. Use the values of $A_0, A_1, \ldots, A_{15}$ given in the Week 4 Tutorial Problem 2.

   Compute the value of the bytes C_1, C_7, and C_{14} from the MixColumns layer.
   You can use Table 4.3 to find the output from the S-box in the Byte Substitution layer.

2. The purpose of this problem is for you to explore the diffusion properties of AES.

   For this problem, use the AES calculator at `http://testprotect.com/appendix/AEScalc` with a key of

   $$k = E0E1E2E3E4E5E6E7E8E9EAEBECEDEEEF$$

   (a) Encrypt the plaintext $x_0 = 00000000000000000000000000000000$. What is the ciphertext y_0?

   (b) Encrypt the plaintext $x_1 = 00000000000000000000000000000001$. What is the ciphertext y_1?

   (c) Notice we changed a single bit from x_0 to x_1. How many bits differ in y_0 and y_1?
   You can certainly do this by hand, but you might also find the *Mathematica* notebook posted useful.

   (d) Repeat this process for at least 10 other values of plaintext x_i that differ from x_0 by a single bit.
   Build a table where each row gives x_i , y_i, and the number of bits that y_i differs from y_0.

   (e) Discuss your results. Do you think AES does a good job of diffusion?

3. This problem involves the *Playfair cipher* with key k =“TOPHBEIFONG”.

   You will need to do some research to understand how the cipher works.
   In this implementation, we are replacing ‘J’ by ‘I’.

   You receive the encrypted message

   ```
   EA DZ SV QT OB FM EQ IB FG NB TQ IF TA TG YF AF MH QP VN LP HN FO YZ HP VI SU
   ```

   Decrypt the message. Who said this?

   Be sure to explain how you decrypted so that someone else can follow, and recreate, your process.