CSCI 476 Computer Security

Exercise for Chapter 8, Cryptography.

(1) Perform the *MixColumns* step in AES, with the following data. What are X, Y, Z, W?

Note that all the numbers are hexadecimal, where multiplying a number by 2 is equivalent to shifting the number by one bit to the left; moreover, if the most significant (left-most) bit of the number is 1, you need to XOR the result with 00011011.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix} = \begin{bmatrix} X \\ Y \\ Z \\ W \end{bmatrix}$$