This time Ruben corrects the homework.

1. Explain what the lookup-table structure of the 4 tables $T_0, T_1, T_2,$ and $T_3$ looks like; recall that these are the tables that combine SubBytes, ShiftRows, and MixColumns.

2. A message of length 64 bytes is encrypted with AES and sent via a network. During the transmission one bit in the second block is flipped. Explain for each of the 5 modes of operation

   (a) how many bits are potentially different in the deciphered text compared to the initial plaintext;

   (b) how many bits are definitely different in the deciphered text compared to the initial plaintext.