Cryptography I, homework sheet 8

Due: 26 September 2013, 10:45

Please submit your homework electronically; the TAs do not want to receive homework on paper. Please bundle your scans into one pdf file. Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. To submit your homework, email it to `crypto13@tue.nl`. You may use computer algebra systems such as mathematica and sage; please submit your code as part of your homework.

1. Explain what the lookup-table structure of the 4 tables T_0, T_1, T_2, and T_3 in AES 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.