CS 741 Assignment 2 Due Date 12/03/21

Write a program to compute the bias of each combination of inputs and outputs to/from the AES S-Box (note that each combination should include at least one of the 8 inputs and at least one of the 8 outputs). Plot a histogram of the biases and also include a table showing the biases and the number of combinations with that bias. (The biases should be positive (even – why?) integers).

Given an n X n S-Box, the number of stages in the SPN (Substitution Permutation Network) and the plaintext/ciphertext block size, write a program to obtain a linear expression with the maximum possible bias. The expression should be a XOR of bits of the plaintext, bits of the ciphertext and bits of the round keys (all but the last round).

"A greedy strategy will always work." Examine the validity of this claim.

Extra Credit: Implement Step 2 of the linear cryptanalysis attack to deduce bits of the last round key.