CS122 Homework #2

Erik Steggall
esteggall@soe.ucsc.edu

Fall 2014

Problem 1

Problem 2

The substitution box is necessary because it has an inverse substitution box that corresponds to it. This allows the AES algorithm to be reversed, which is necessary for decryption. It is necessary to have 2^8 bytes because this contains all possible 8-bit values (256). This formula also makes the algorithm easier to understand, since one can simply view the hex number on the left and the hex number on the right to determine where in the S-box to go, and as was stated in class, it's best to have an algorithm that is easily understood so it's weaknesses can be discovered if they exist.

Problem 3

We can replace the XOR function of the DES encryption mechanism with a hash function?
We can use the hash function as a key for DES?

Problem 6

No this is not a secure method because the attacker can use statistical analysis to determine the original message.