Intro to Cryptography

Mark Anderson
Problem 4

May 16, 2019

1. When deciding where to allocate most of my time I decided I understood AES, and Rabin encrpytion better than DES, so much of the work done for DES was trivial and implemented towards the beginning. The only work I was able to complete andhave fully working was the permutation from the prompt to generate new SBOXes. I believe much of the confusion in understanding DES vs understanding AES was lack of quality material outside of the textbook. For AES I was able to find articles and examples for every single function in AES done mathematically, and this helped out immensely for the functions like MixColumns() and KeyExpansion(). The MixFunctions examples I was able to read included before and after states for the block, as well as why each step is computed the way it is in the Galois Field. On top of this, the NIST pdf we were given included examples for KeyExpansion, as well as an example for an entire round of encryption, using these materials I was able to debug much easier and better than I would have been able to do with DES.