Jake Hemmerle
Project 1 Report
Network Security
Professor Boyang Wang
2/25/20

AES Project 1

Project Structure:

- **aes/** - has __init__.py which contains the AES class
- **CryptoEngine.py** – a container class that utilizes the AES implementation, has some utilities for managing multiple blocks, padding, key management, a KDF, etc.
- **tests/** - contains tests for the AES and CryptoEngine classes
- **data/** - these project specific files

Running:

To run the project, run ‘’’python CryptoEngine.py’’’ in the root of the folder.

Tests:

You can run all the tests at once by running ‘’’python -m unittest discover -s tests’’’

NOTE: I know the AES MixColumn function is not working properly. There are one or two bytes that are off. After several hours, I decided to move on to other things.