AES Cryptoware

Alan Chen Computer Engineering 2021

Task/Purpose: AES is one of the most used symmetrical encryption algorithms. To learn more about the systematic process of AES, I planned to implement AES-Cipher Block Chaining on an Adafruit M4 Metro board.
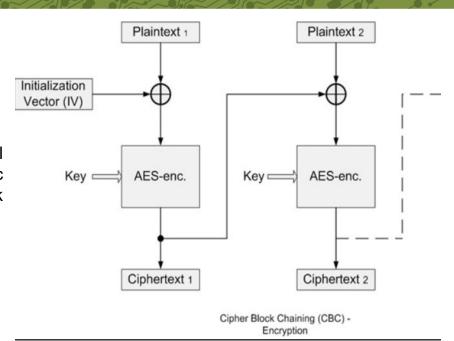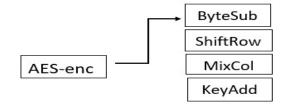
Problems:
- MicroPython vs. Python
- Lack of storage and libraries
- Overall complexity of the AES code

Solution/Results: In this project, I learned about the AES Encryption by successfully improving and modifying python codes to the most basic level, so it does not require additional libraries. Hence, it is applicable to the Adafruit M4 Metro board.

Future Goals:
- Hashing instead of padding for appropriate length
- Applying AES-enc to data from a sensor device

Cipher Block Chaining (CBC) - Encryption