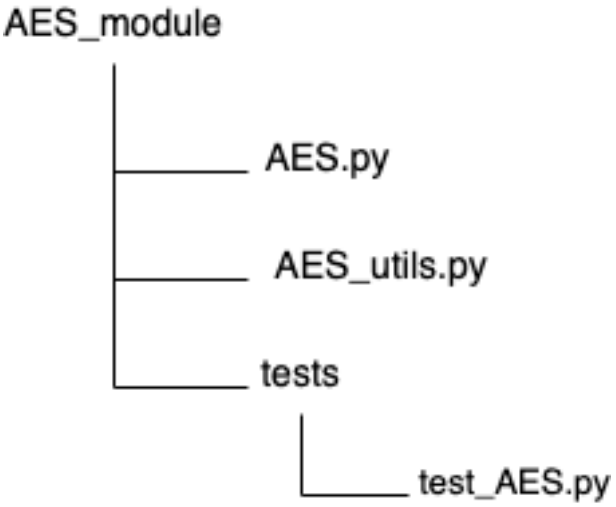
CSCI 663G Group 3 Project Proposal

GitHub

Project design for AES:
Directory Structure

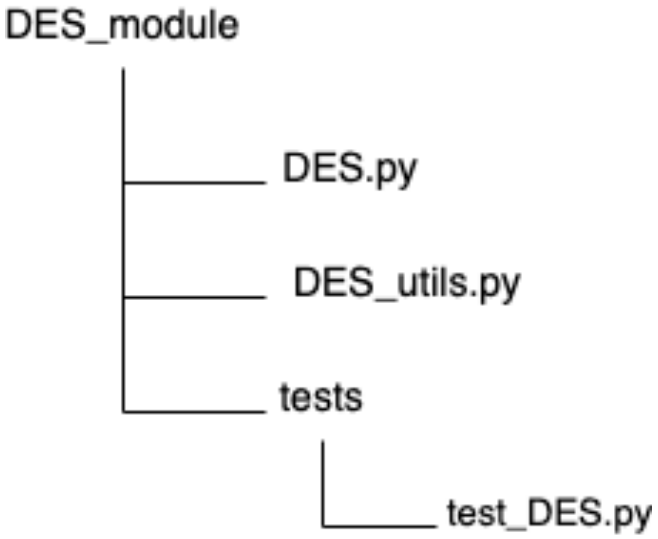


AES.py: The primary implementation of the AES encryption and decryption algorithms is located in aes.py, which is most likely the main module of your project. The components that would be included are the logic responsible for expanding the key, the primary encryption and decryption operations.
def encrypt
def decrypt
def expand_key

AES_utils.py: This module includes utility functions and assistants that provide support for the primary AES operations implemented in AES.py. This may involve operations such as converting data formats, padding and unpadding messages, or executing mathematical operations that are specific to AES.

tests/: directory that contains the test file which might have system and unit test.
test_AES.py: this file has unit tests for the aes.py module. These tests would focus on function of the program to make sure that encryption, decryption to ensure it functional as expected.
def test_encryption
def test_decryption
def test_expand

Project design for DES:
Directory Structure



DES.py: The DES encryption and decryption methods are built into this file, which is the core module. The DES algorithm works with 64-bit blocks and a 56-bit key (plus 8 parity bits). This module would have the logic for the first permutation, the 16 rounds of processing (which include expanding, substituting, permuting, and mixing with the subkeys), and the last permutation.
def encrypt
def decrypt
def generate_round_key

DES_utils.py: This module should provide utility functions and assist DES.py DES operations. Key scheduling (creating the 16 subkeys used in encryption and decryption), bit manipulations (permutations and selections), and DES data format conversions may be involved.

tests/: directory that contains the test file which might have system and unit test.
test_des.py: This file would provide unit tests for the des.py module, testing DES algorithm components.
def test_encryption
def test_decryption
def test_key_generation