CSCI 531 Programming Assignment 1 (100 points)

Note: this assignment is not as rigorous as usual CS projects. Your task is to implement the AES-128 with ECB mode algorithm.

Project Details

In this assignment you must write your own code (you *cannot* use any external code/library that implements AES functionality). However, you can use built-in libraries to generate a random string for cryptographic key. Python os.urandom() function is used to generate the string of size random bytes suitable for cryptographic use. Make sure your programs work correctly on input longer than 128 bits.

To complete the project, you will need to write three Python 3 programs:

1. **aesencrypt.py** encrypts a given input. This program takes two arguments (a secret key a string to encrypt) and returns encrypted string.

2. **aesdecrypt.py** decrypts a given input. This program takes two argument (a secret key a string to decrypt) and returns decrypted string.

3. **aestest.py** demonstrates your AES implementation. This program takes a string as input. It generates a secret key and calls aesencrypt.py. Next the program calls aesdecrypt.py.

Assignment Submission

Submit the assignment on DEN D2L. The submission will consist of four files:

1. A design document in PDF format providing a brief description of the design of your programs and including a screen capture of the working programs.
2. The program aesencrypt.py.
3. The program aesdecrypt.py.
4. The program aestest.py.

Grading

1. Design document (15 points)
2. Correct implementation of aesencrypt.py (40 points)
3. Correct implementation of aesdecrypt.py (40 points)
4. Correct implementation of aestest.py (5 points)

Resources

- AES Standard: https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf
- How to do MixColumns: https://crypto.stackexchange.com/questions/2402/how-to-solve-mixcolumns