Math 4175: Cryptography

Final Project

The final project in this class replaces the final exam and is due 9:45 am Saturday, December 16. (This is the latter of the exam times for the two sections, and gives me time to grade these before having to turn in final grades.)

The Project

Create a working implementation of AES, which can encrypt and decrypt messages.

Your implementation should cover all three key schedules (128-bit, 192-bit, 256-bit), and should perform in both ECB mode and CBC mode. (We haven't discussed these modes yet: ECB mode is what we've covered in class. CBC mode involves one additional XOR step per block.)

Input will be provided in the form of strings of text representing bytes in hexadecimal form. For example, one sample input could be the string "`A01478BE92570366F1D13C098726DAC5`". Output should be given in a similar format.

You may choose to convert the string into actual bytes before performing any computations.

Documentation and Style

Your code should be well-documented. Significant variables should have descriptive names, the purpose of major blocks of code should be documented, and indentation should be used to indicate where functional blocks begin and end. The quality of the documentation will be worth 20% of the project grade.

However, this is not a programming course. I won't be grading for "programming sophistication". There are good programming practices – choice of variable scope, abstraction of reused functions, closing file handles after use, etc. – for which you should strive, but I won't be grading for these.

Timetable

November 27 key expansion and schedule

December 4 encryption

December 11 decryption

I'll provide some flexibility around these dates, but these should give you time to implement the entire system without leaving too much work until the end.

Evaluation

After break, I'll provide some test files which you can use to test your code with, along with some files to encrypt and decrypt (but whose answers won't be provided.)

One of the files, when decrypted, will contain further instructions.

Your project grade will be based on these criteria:

70%	Correctness and completeness of code
20%	Documentation
10%	Successful encryption and decryption of test files, including completing the further instructions.

Honor Code

Because AES is an open standard, there are multiple implementations of AES already available online. Please do not copy them. I do not enjoy the responsibility of having to enforce the honor system, but I will do so if I have to.