**Laboratory Assignment #1**

**(CSE 178: Computers and Networks Security)**

**(Due on Monday November 23, 2015)**

**(Maximum points 50)**

Implement the encryption algorithm of the Advanced Encryption System (AES) for 128 bit key and thoroughly test it for correctness. Your code should be well-structured and well-documented. You are free to choose any programming language, however, C/C++ is recommended. Assume that the plaintext input message is always of length 128 bits.

You will need to submit the following:

1. Complete source code of your program.
2. A 2-4 page write up explaining your implementation.
3. Two test cases (and the corresponding outputs) that you used to test your code.