Problem Set 4
Due 11/10/2005
Send to tmorgan@ccs.neu.edu, with CC to noubir@ccs.neu.edu

1. Implement AES for 128 bit key length.
2. Optimize your implementation for the following types of processors. Provide the code for both optimizations:
    a. 8-bits processor.
    b. 32-bits processor. Hint: minimize the cost of computation by using 4-precomputed tables of 256 entries.
3. Run both optimized version on a 32 bits processor. What data rates are you able to achieve with each version (e.g, 100Mbytes per second). Also compare when using the same key for all packets (i.e., single-connection) and when you change the key for each packet (i.e., multi-connection). State the characteristics of the machine over which you are running the code (e.g., Intel Pentium 4 processor, 1GB RAM, Windows XP, single application running).

4. Provide an API for AES-CBC and AES-ECB modes.

Note:

1. Follow the instructions given by the grader (Tim Morgan) for problem set submission.
2. For testing purpose you can use the following link to obtain some test vectors: http://csrc.nist.gov/CryptoToolkit/aes/rijndael/.
3. There are many implementations available on the web, however you have to do your own implementation.