College of Computer and Information Science
Northeastern University
Fall 2004
CSG252: Cryptography and Communication Security

Problem Set 4
Due 11/15/2004
Send to ati@ccs.neu.edu, with CC to noubir@ccs.neu.edu

1. Implement AES for 128 bit key length.
2. Provide an API for AES-CBC and AES-ECB modes.
3. Minimize the cost of computation by using 4-precomputed tables of 256 entries. State if your optimization works for an 8 bit processor or a 32 bit processor.

Note:

1. Provide a readme file that allows the TA to run your program easily.
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 make your own.