Institut for Matematik og Datalogi
Syddansk Universitet

October 12, 2016
JFB

Cryptology – F16 – Assignment 2

Assignment due Wednesday, November 2, 8:15

Note that this is part of your exam project, so it must be approved in order for you to take the exam in January, and you may not work with others not in your group. If it is late, it will not be accepted (though it could become an assignment you redo). You may work in groups of two (or three), and you may write it in either Danish or English. Turn in the assignment through the SDU Assignment system in Blackboard with the program code included at the end of your report. In addition, mail me your program code. Your report should include sufficient information for me to compile it, run it, and test it easily. In your report, explain why your code does what it should.

Remember to keep your receipt from Blackboard. Turn in one PDF file per group.

By midnight on October 24, let me know what programming language you plan to use. It has to be one that works on the computer lab machines, and your program has to complile and run correctly on the computer lab machines. Program AES yourself; do not use library functions to do it or copy from elsewhere.

1. Write a program to encrypt and decrypt a text file, using AES in CBC mode. Test that it works, using two different keys. (Note that by AES, I mean the version with a 128 bit block and key length.)

   Program AES yourself; do not use library functions to do it. The tables for the AES S-box (SubBytes) and its inverse can be found in figures 7 and 14 of the description of AES on NIST's homepage:

   http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

   This link is available from this course's homepage, under "Miscellaneous".

2. Check the table for the S-box in the above link, checking that it is correct according to the definition of SubBytes in the same document (the inverse of the element represented by the eight bits, followed by the given affine transformation). Why don't you need to check the inverse S-box table for correctness now?

3. (Optional) Compare the speed of your AES encryption algorithm to that of some software implementation on the network or to that of your classmates. Do not look at other implementations you can find until you are done with your own! Could you have done something better?