MAS433 Cryptography: Assignment 1

Submission Instructions:

1. Submission deadline: 10PM, 02 October 2011 (Sunday).
2. You need to email your answers (report, the source code) to the instructor (wuhj@ntu.edu.sg) with the email subject "MAS433 Assignment 1".

Exercise 1. Implement AES-128 in C, C++ (or MATLAB).

1.1 AES-128 is AES with 128-bit key. The detailed specifications of AES are given in the file "fips-197.pdf".

1.2 You need to compute Sbox and the inverse of Sbox in your program. You also need to compute MixColumns in your program.

1.3 You need to ensure that AES-128 is implemented correctly. To check whether your AES implementation is correct or not, you can refer to the test vectors given in the Appendix C of "fips-197.pdf".

1.4 Your program should include both encryption and decryption of AES-128. For encryption, your program needs to get a key and a 128-bit plaintext block, then gives the ciphertext block. For decryption, your program needs to get a key and a 128-bit ciphertext block, then gives the plaintext block.

1.5 Explain in your report how to use your program.

Exercise 2. Encrypt a file on harddisk.

2.1 Explain in your report how to generate IV for CBC mode.

2.2 Normally a decryption program needs to check whether the input key is correct or not before performing decryption. Describe in your report how to implement the key checking in a secure way.

========== The following is optional ========

2.3 AES-128 in CBC mode should be used for encryption in this exercise. You can refer to the test vectors given in the Appendix F.2 of "sp800-38a.pdf".

2.4 Your program needs to obtain a key from the user of your program for encryption. You do not need to modify the original file.

2.5 Note that if the message length is not multiple of 128 bits, you can simply pad bits '0' to the end of the message so that the length of the padded message is multiple of 128 bits. Explain in the report how to decrypt the ciphertext with the padding being introduced.

2.6 Your program can be used to decrypt a file that was encrypted by your program, and obtain the original message. Your program needs to obtain a key from the user of your program for decryption.

2.7 Explain in your report how to use your program.