The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/6360 Data Security
Assignment 2

Due on Friday, 19th May 2017, in the Assignment2 in Blackboard.
Total mark: 100

Note:

Before you start working on the Assignment please read the information on academic integrity, which can be found at http://www.newcastle.edu.au/service/academic-integrity/. All available strategies will be used for detecting possible plagiarism and all suspicious cases will be referred to the SACO (Student Academic Conduct Officer).

Description

In this assignment, you will implement AES encryption and decryption in each of the following modes of operation: Electronic Codebook (ECB) mode, Cipher Block Chaining (CBC) mode, Cipher Feedback (CFB) mode and Output Feedback (OFB) mode.

For encryption, your program will take as input:

- a 0 to indicate we are encrypting (note this parameter will be 1 for decryption);
- the mode of operation, ECB, CFB, CBC or OFB, indicated by a 0, 1, 2 and 3, respectively;
- the transmission size (s), which must be between 1 and 16 bytes - if not applicable, should be set to 0;
- 32-byte plaintext P;
- a 16-byte key K;
- a 16-byte initialization vector (IV) - if not applicable, should be set to 0

and produce as output:

- 32-byte ciphertext C.

For decryption your program will take similar input, except you will be producing plaintext as output rather than ciphertext, and the first parameter will be 1 to indicate decryption.

Your program should be well commented and easy to understand. You MUST NOT use any available AES code or a portion of it (including AES libraries). You must implement the algorithm from scratch.

SAMPLE INPUT FILE

The following is an example of an input file.

```
0
0
0
5A 67 F0 12 CF 98 AB CD 00 E4 35 FF 01 35 78 91 FA C2 CF 98 AB CD 00 E4 35 FF
01 35 00 E4 35 FF
00 E4 35 FF 01 35 78 91 AB CD 00 E4 67 F0 12 CF
0
```

The first line in this file indicates an AES encryption, the second line indicates ECB mode, size s is not applicable and thus the third line contains 0, the fourth line contains a 32-byte plaintext, the fifth line contains a 16-byte key, and the sixth and the final line contains 0 as the IV is not applicable.

Program Requirements

You can implement you assignment in either Java or C++. Please note that if you choose to implement in C++ your submission should compile and run on university computers.

Your main runnable class should be called AESInterface. You should submit all source code and if you implement your assignment in C++ also submit a makefile. For all submission please also include a README.txt file clearly outlining the various classes submitted and the main functionality of each. One or two lines per class will suffice.

Be sure to submit a filled in Assessment Item Coversheet with your assignment submission. Note for electronic submissions there is no need to sign.

Assessment criteria

You will NOT be assessed on running time of your algorithm. However, you should make some attempt to keep your code efficient where possible. Most marks will be awarded for ECB mode as that is where your AES encryption and decryption will be assessed.

1. For ECB mode, for encryption and decryption:
   a. Quality of code: Code style, structure and commenting → **5*2=10**
   b. Implementation and Execution of Program: Logic and compilation → **10*2=20**
   c. Working code that outputs correct result: Encryption/ Decryption working correctly → **17*2=34**
2. For each of CFB, CBC and OFB mode, for encryption and decryption:
   a. Quality of code: Code style, structure and commenting → **1*2 =2**
   b. Implementation and Execution of Program: Logic and compilation → **2*2=4**
   c. Working code that outputs correct result: Encryption/ Decryption working correctly → **3*2=6**

TOTAL: **100** marks