CPS 713 Applied Cryptography, Lab 3

Background: The main purpose of this lab is for you to gain hands-on experience in the basic cryptographic algorithms used in the Advanced Encryption Standard (AES). The block cipher to be used for this lab is the *Simplified AES (S-AES)* in the textbook appendix 5B, pages 164 –173 .

Implement code that enciphers and deciphers using S-AES block cipher in C. Add suitable and clear comments to your code to make it more readable (and easier to debug for yourself!). Your submission should include all source files used, the binary generated (if any), sample files, and clear documentation on what is included and how the code can be executed. For your code development, you have to use C. You can assume that the plaintext is already in a binary form.

You have to complete this lab in the groups of two that you are assigned to. You have to ensure to coordinate your work in order to finish the lab by its deadline, and you should both work on all of its implementations. If there are any issues with your lab partner, you need to raise this to the attention of the TA and the instructor, and resolve it as soon as possible. Your completed lab, including all the files required for the two tasks listed above must be submitted as a .zip file via Blackboard by Monday, March 10th at 9 AM. There is a mandatory demo requirement for this lab. You and your lab partner should be both participate in this demo. It is important that if you do not participate in the demo, or there are discrepancies between the work submitted and demo given, you will receive a grade of zero in the lab EVEN if you have submitted a lab report. The demo for this lab may be combined with the other labs. You should check Blackboard for the info on the upcoming demo(s).