CECS 285: Lab 10 Bonus (25 points possible)
Using Encryption Key File

OBJECTIVES:

- Enable the ability to use a key file to encrypt/decrypt

ACTIVITY 1: Lab 10 is designed originally to use a hard coded key defined in the program to perform encryption and decryption. This makes testing the encryption program with different key files a cumbersome task because the key must be changed in software, then the hex file must be rebuilt, and then the new hex file must be loaded onto 8051, and finally you can proceed with testing encryption with the new key.

A better approach rather than hard coding the key is to allow a key file to be sent before the file that must be encrypted or decrypted. The key file can be a null terminated series of values or ascii characters. Some other terminating character can be used as well.

Here is a description about how this can be accomplished:

- When the 8051 starts up, display a prompt stating something like "Send keyfile"
- Then when the key file has been received you can display an acknowledgement message or light an LED to give some visible feedback
- Next you are ready to encrypt/decrypt a message contained in a text file. Optionally you can display another prompt to "Send the message for encryption/decryption"
- At this point you may proceed to:
    - begin the file capture operation
    - send the file to be encrypted/decrypted
    - end the file capture operation
- Then you can use the reset button to restart your program or *you can design your program so the main program loop does not reach a halting point and will return to where it is ready to receive another keyfile and encrypt again.*

Deliverables: Upload a Single Word Doc or PDF which contains

- Completed program source with full comments
- Screenshots specified in Activity 2
- Flow Chart to model the functionality of your entire program

Not all of the extra credit points are guaranteed.
Additional bonus points may be awarded for the implementation of more features beyond the description of this document.