ECE 385 Lab 9 Report Outline

- ❏ **Introduction**
  - ❏ Briefly summarize the operation of the AES encryptor/decryptor.
- ❏ **Written Description and Diagrams of the AES encryptor/decryptor**
  - ❏ Written description of the software encryptor
    - ❏ Describe the role of the NIOS processor as well as the basic functionality of your C code
  - ❏ Written description of the hardware decryptor
    - ❏ Describe the basic steps of decryption and how this is controlled and computed in hardware
  - ❏ Written description of the IO module (io_module.sv)
    - ❏ Describe how the system sends data between the software encryptor and the hardware decryptor
  - ❏ Block diagram
    - ❏ This diagram should represent the placement of all your modules in the top level. *Please only include the top level diagram and not the RTL view of every module*. The Qsys view of the NIOS processor is not necessary for this portion.
  - ❏ State Diagram of AES decryptor controller
    - ❏ This is the state machine that was written in aes_controller.sv. You may abbreviate the 9 looping rounds in the state diagram like in figure 9 on page IAES.9 of the lab manual.
  - ❏ State Diagram of IO Module
    - ❏ As this state machine contains many states, many of which are identical to each other, you may abbreviate the diagram by writing the first and last of a sequence of similar states and place an ellipsis in between them.
  - ❏ Module Descriptions
    - ❏ A guide on how to do this was shown in the Lab 5 report outline. Do not forget to describe the Qsys generated file for your Nios system! When describing the generated NIOS file, you should describe the PIO blocks added beyond those just needed to make the NIOS system run (i.e. to_hw_sig, etc.).
- ❏ **Annotated Simulation of the AES decryptor**
  - ❏ In this simulation, you should display the input encrypted message, the input plaintext, the output decrypted message and the current state of the controller. Notate various points of interest in the simulation (such as when the decryptor finishes decrypting, etc.).
- ❏ **Post-Lab Questions**
  - ❏ Fill out the design resources and statistics table (duplicated here for convenience).

LUT	

DSP	
Memory (BRAM)	
Flip-Flop	
Frequency	
Static Power	
Dynamic Power	
Total Power	

- ❏ Which would you expect to be faster to complete encryption/decryption, the software or hardware? Is this what your results show? (List your encryption and decryption benchmark here)
- ❏ If you wanted to speed up the hardware, what would you do? (Note: restrictions of this lab do not apply to answer this question)

❏ **Conclusion**

- ❏ Discuss functionality of your design. If parts of your design didn't work, discuss what could be done to fix it
- ❏ Was there anything ambiguous, incorrect, or unnecessarily difficult in the lab manual or given materials which can be improved for next semester? You can also specify what we did right so it doesn't get changed.