LAB #1: Assigned 9/11/09, DUE: 9/24/09

The labs are designed to set milestones for the project

The first part of the project is to select an ‘open source’ version of an encryption algorithm. The Agrawal et al paper used the Advanced Encryption Algorithm [1] and RSA algorithm [2]. As a class, we need to decide on which (or both) algorithms we are going to use for the project. Each team will investigate this separately and make their recommendations in class on the due date. The recommendations must include a link to the source (obviously) and a high-level block diagram of the algorithm(s), along with an estimate of how many equivalent 2-input NAND gates are needed to implement the algorithm on an FPGA. Please also prepare to describe how the basic components in the block diagram operate to implement the algorithm.

The second part of the first lab is to assemble the two teams. We will discuss this in the next class so the teams can work together on choosing the most appropriate encryption algorithm

[1] Advanced encryption standard (AES). Website, Nov. 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, 21(2):120-126, February 1978