ECE: Intro Information and Network Security
Computer Project 1, Due Date: April 24, 2008
Spring 2008

Project Description

In this project, your team (consisting of at most two students) will conduct timing measurements for various different cryptographic primitives. You are allowed to use whatever language you desire, and whatever library you desire. Of course, some languages will have advantages over other languages.

You are to conduct the following tests

1. Choose two different symmetric encryption operations (such as DES, AES, SERPENT, Twofish, Blowfish, etc.) and measure the time needed to encrypt a block of plaintext. Report your findings, and what the block sizes of the different cipher schemes were that you used.

2. Choose two different public key encryption algorithms (such as RSA and ElGamal) and conduct timing measurements.

3. Finally, choose two different hash functions (such as SHA-1, MD5, and RIPEMD), and measure the time needed to hash different message sizes for each scheme.

You should make an effort to conduct a thorough analysis of the timing needed. This might involve varying the key size or varying the message size. Additionally, you should explain how you arrived at your estimates (note: you will want to average over many iterations to arrive at timing estimates).

Your team will turn in a short report (roughly 6 pages) that describes the approach you used and the explains your observations. Make certain to describe which language and libraries you used (if they are public), and attach a copy of your code. Your grade will be based upon the clarity and thoroughness of your report. Be sure to include the name of all team members on the report.