# ECE 332:491 Information and Network Security
# Computer Project 1, Due Date: February 13, 2006

Spring 2006

**Project Description**

In this project, your team will build a basic large-integer arithmetic library for MATLAB. This library will allow you to represent large integers, which serve as a fundamental building block for many cryptographic and security algorithms. We will use this library several times throughout the semester.

Your library must:

1. Be written in MATLAB.
2. Provide the ability to represent any size of integer (hence you will be able to represent 512 bit integers, 1024 bit integers, and larger!)
3. For large integers $a$ and $b$, the library will support the following basic arithmetic operations:
   (a) Decide whether $a > b$ , $a = b$, or $a < b$.
   (b) Calculate $c = a + b$, $c = a - b$, and $c = ab$.
   (c) Suppose $a = qb + r$, calculate $q = a$ DIV $b$ and $r = a$ MOD $b$.
4. Provide the ability to generate a random $B$ bit large integer (where $B$ could be any input parameter).
5. Provide a function that will display a random large integer on the screen.

**What to Turn In**

Having completed implementing your function library, you must test the validity of your library.

Your team will turn in a short report (less than 6 pages) that describes the design approach you used in implementing your function library. Explain any data structures you used (especially the data structure used to represent large integers). Additionally, explain the techniques you used to validate your library. In addition to your report, you must attach a print-out of your library's source 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.

**Important Note:**

The source code from different teams **will** be compared in order to see if there is any plagiarism. Duplication of source code or homework solutions or any other other course work will not be tolerated. Any perceived plagiarism will be directed to appropriate departmental and college-level (Engineering or FAS) officials for evaluation.