

**CSCI 124/224 - Discrete Structures II - Fall 2007**  
**George Washington University**

**Homework 3: 100 points**

due 23 October 2007, by 6 pm in Blackboard ONLY

**Policy on collaboration:** All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the quizzes, tests or final.

You are expected to cite all your sources in any written work that is not closed book: papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

**You may not copy code from anywhere; you may not use any code you have not written except for standard libraries.**

*Any violations will be treated as violations of the Code of Academic Integrity.*

This HW will be in electronic form and will be submitted electronically, on BLACKBOARD. It will consist of a single compressed file: .rar, or .zip This file will contain a typewritten report with attached code in text readable form (that is, your .doc or .pdf document will contain text of all your code at the end). The typewritten report will contain your observations and results. The compressed file will also contain the code itself, with a simple README file with documentation and any instructions on running the code.

**All code must run on hobbes. If it doesn't run on hobbes, you will get NO credit.**

Write code, in C++, C or Java, for:

(a) The generalized euclidean inverse: given input  $a$  and  $m$ , output  $a^{-1} \bmod m$  and a text string "inverse exists" or return an error value and the text string "no inverse". Your result for  $a^{-1}$ , if it exists, should be non-negative and strictly smaller than  $m$ . You may not use code that you have not written, except code for quotients and remainders. In particular, you cannot use existing code for the euclidean algorithm that you have not written.

(b) Modify the affine cipher code written by you for HW 2 to perform the inverse cipher as well: given input  $a$ ,  $b$ ,  $m$ , and a text string saying "forward" or "inverse", output  $a \times b \bmod m$  if the string says "forward", and  $a^{-1} \times b \bmod m$  if it says "inverse". Use the code written in part (a) above. Make sure you check that  $a$  is invertible, and that both  $a$  and  $b$  are non-negative and smaller than  $m$ . Your output should be non-negative and strictly smaller than  $m$ .

(c) Write a program for fast exponentiation: given input  $a$ ,  $b$ ,  $m$ , output  $a^b \bmod m$  and the number of multiplications performed by your program. Make sure you check that both  $a$  and  $b$  are non-negative and smaller than  $m$ . Your output should be non-negative and smaller than  $m$ . You may not use code that you have not written, except code for quotients and remainders.