

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

**Homework 2: 75 points**

due 27 September 2007, by 6 pm in instructor's mailbox, or in class.

**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.*

Part A of this HW will be submitted on paper, in the instructor's mailbox or in class on the due date.

Part B will be in electronic form and will be submitted electronically, on BLACKBOARD. Part B will be 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.**

Part A.

1 (15 points) Show that the lattice  $S = \{(x, y) | x \in \mathbb{Z} \ y \in \mathbb{Z}\}$  is a group under pointwise addition:  $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ . Sketch the lattice. (That is, draw a graph showing the points in  $S$ ).

2. (10 points) Show that  $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$ , the set of non-zero integers *modulo*  $p$ , for  $p$  any prime number, is a group under multiplication.

Part B (20 points each).

Write code, in C++, C or Java, for: (a) the shift cipher: given input  $a$ ,  $b$  and  $m$ , output  $a + b \bmod m$ . Your result should be non-negative and strictly smaller than  $m$ . (b) the affine cipher: given input  $a$ ,  $b$  and  $m$ , output  $a \times b \bmod m$ . Your result should be non-negative and strictly smaller than  $m$ .