Instructor: Leo Goldmakher

NAME: ____________________

University of Toronto Mississauga
Department of Mathematical and Computational Sciences

MAT 302: CRYPTOGRAPHY

Problem Set 2 (due February 10th, 2011 at the start of lecture)

INSTRUCTIONS: Please attach this page as the first page of your submitted problem set.

PROBLEM	**MARK**
2.1	
2.2	
2.3	
2.4	
2.5	
2.6	
2.7	
2.8	
2.9	
2.10	
Total	

Problem Set 2

NAME: ____________________________

2.1 Part 2 of problem 2.1 in Paar-Pelzl. (There's a typo in the key: the final letter should be a 'y', not an 'a'.)

2.2 In each of the following, prove that G is a group under @.

(a) $G = (\mathbb{R} \times \mathbb{R}) \backslash \{(0,0)\}$, and $(a,b)@(c,d) = (ac - bd, ad + bc)$.

(b) G is the half-open interval $[0,1)$, and $x@y = \{x + y\}$. (Here $\{\alpha\}$ means the fractional part of α.)

2.3 Given a set S, let $E(S)$ be the set of injections $f : S \hookrightarrow S$. Is $E(S)$ a group under composition? Justify your answer.

2.4 For each of the following, list all the ways in which it fails to be a group. Whenever a group axiom fails to be satisfied, give an example illustrating the failure.

(a) $\left(\mathbb{Z}^*, \times\right)$ where $\mathbb{Z}^*$ is the set of all non-zero integers and $\times$ denotes ordinary multiplication.

(b) The set of all subsets of $\{1,2,3,4,5,6,7,8,9,10\}$ under the operation $\cap$. (Recall that given any two sets A and B, their intersection (written $A \cap B$) is the set consisting of all elements belonging to *both* A and B.)

(c) The set of all positive integers, under the operation @ defined by

$$a \,@\, b := \gcd(a,b).$$

(Recall that given two positive integers a and b, the *greatest common divisor* of a and b, denoted $\gcd(a,b)$, is the largest positive integer dividing both a and b.)

(d) The set of all positive integers, under the operation $\oplus$ defined by

$$a \oplus b := \operatorname{lcm}(a,b).$$

(Recall that given two positive integers a and b, the *least common multiple* of a and b, denoted $\operatorname{lcm}(a,b)$, is the smallest positive integer which is a multiple of both a and b.)

(e) The set of all non-negative integers (i.e. $\{0,1,2,\ldots\}$), under the operation $\odot$ defined by

$$a \odot b := |a - b|.$$

(In other words, $a \odot b$ is the distance between a and b.)

2.5 Problem 2.5 in Paar-Pelzl. (Note that the c_i are the feedback coefficients, which are called p_i on page 43 of Paar-Pelzl.)

2.6 Suppose G is a group, and $a \in G$. Show that $aG = G$, where $aG = \{ag : g \in G\}$.

In the following two problems, we make precise the intuition I gave that a group is a set in which you can get from any one element to any other. We will say that a binary operation on a set S is *left transitive* if it allows you to get from any one element to any other by left multiplication, i.e. if for any pair of elements $a, b \in S$

there exists $g \in S$ such that $ga = b$. Similarly, we say the operation is *right transitive* if there exists an $h \in S$ such that $ah = b$.

2.7 (Courtesy of J. Lagarias) The goal of this exercise is to show that associativity and one-sided transitivity do not guarantee a group structure. Let S be any set with at least two elements, and define a product on S by setting $ab = b$ for every $a, b \in S$.

(a) Prove that S is closed under this product, that associativity holds, and that the product is right transitive.

(b) Explain why S is not a group.

2.8 (Courtesy of N. Pflueger) In this exercise, you will show that associativity and two-sided transitivity guarantee a group structure. Let S be a non-empty set with a binary operation which is associative and both left *and* right transitive.

(a) If $ex = x$ for some elements $e, x \in S$, we say e is a *left identity for x*; similarly, if $xe = x$ we say e is a *right identity for x*. Prove that an element is a left identity for one element of S if and only if it is a left identity for *every* element of S. The same argument shows that the same holds for any right identity.

(b) Prove that S has a unique identity element. [*Hint: first show that a left identity exists; similarly, a right identity exists. Next, prove that given a left and a right identity, the two must be equal. Conclude.*]

(c) Deduce that S is a group under the given binary operation.

2.9 We define a linear congruential generator as follows: given a starting seed s_0 and a function $f(x) = Ax + B \pmod{p}$, let $s_{i+1} = f(s_i)$ for each $i \geq 0$. Suppose that p is prime, and $A \not\equiv 0, 1 \pmod{p}$. Show that $s_m = s_n$ whenever $m \equiv n \pmod{p-1}$.

2.10 Propose an original idea (i.e. different from any you've seen before) for a (Pseudo) Random Number Generator, and comment on its strengths and flaws. You may collaborate with other members of the class, but in this case indicate the name(s) of your collaborators.