Instructor: Leo Goldmakher

NAME: ____________________

University of Toronto Mississauga
Department of Mathematical and Computational Sciences

MAT 302: CRYPTOGRAPHY

Problem Set 5 (due March 29th, 2011 at the start of lecture)

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

PROBLEM	**MARK**
5.1	
5.2	
5.3	
5.4	
5.5	
5.6	
5.7	
5.8	
Total	

Problem Set 5

5.1 Problem 8.1 from Paar-Pelzl.

5.2 Let $p(n)$ denote the smallest prime factor of n. For example, $p(6) = 2$.

(a) If N is the product of two primes (as in RSA), prove that $p(N) \leq \sqrt{N}$.

(b) What can you say about $p(N)$ if N is the product of three primes? Prove your assertion.

5.3 Let $\varphi(n)$ and $\mu(n)$ be as in previous lectures and assignments.

(a) Prove that for all n,

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$$

[*Hint: You may find it helpful to recall problem 3.2*]

(b) Deduce that for all n,

$$\sum_{d|n} \varphi(d) = n$$

[*Hint: You may find it helpful to use the group structure you explored in problem 3.5*]

5.4 Suppose G is a finite abelian group with N elements.

(a) For all $d \mid N$, let $G_d = \{x \in G \;:\; x^d = 1\}$. Prove that $G_d \leq G$.

(b) Suppose that for some $g \in G$ we have $|g| = d$. Determine and prove a formula for $|g^k|$, where k is an arbitrary positive integer.

5.5 Problem 8.5 from Paar-Pelzl.

5.6 Prove that $(x+1)^n \equiv x^n + 1 \pmod{n}$ if and only if n is prime.

5.7 In class, we stated the Fermat test in terms of verifying $a^{n-1} \equiv 1 \pmod{n}$ for many values of a. Recall that a Carmichael number n satisfies this congruence for every $a \in \mathbb{Z}_n^\times$.

(a) Prove that $a^{n-1} \equiv 1 \pmod{n}$ for *every* $a \in \mathbb{Z}_n$ if and only if n is prime.

(b) As we discussed in lecture, 561 is a Carmichael number – it fools the Fermat test. Does 561 also fool Miller-Rabin?

5.8 Determine all solutions to the following congruences:

(a) $3^x \equiv 5 \pmod{7}$

(b) $3^x \equiv 5 \pmod{13}$