IS-2150/TEL-2810 Introduction to Security

Homework 1

Due Date: By Midnight of September 17, 2006

1) **Do the following from Chapter 1** **[30 Points]**

From section 1.11, do exercises 1, 4, 5, 7, 9, 15

2) **Exercise on Propositional/Predicate logic** **[30 Points]**

(a) Prove that $A \oplus B \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)$.

(b) Use the logical connectives of propositional logic to express the following sentences in propositional logic. Be sure to define all propositional atoms.
   i) If the sun shines, we can make hay
   ii) If you do all the homework, read the text, and study the lecture notes, then you will be prepared for the midterm exam. Otherwise, you may not be prepared for the exam.

(c) Use predicate logic to state the following sentences. Be sure to define all predicates, constants, and variables.
   i) Not all birds can fly.
   ii) Every child is younger than its mother.

3) Prove by induction the following statement: **[10 Points]**

($n^3 + 2n$) is *divisible by* 3, *where n is a natural number.*

4) Exercise on Lattice **[10 + 20 Points]**

(a) Prove that the set of all subsets of a given set *S* (called the *power set* of S) forms a lattice under the relation "subset" ($\subseteq$).

(b) Consider set of digits $D = \{1, 2, 3\}$. Let *S* be set of all numbers containing two digits from *D*; i.e., each element $a \in S$ can be written as $a = a_1a_2$ where $a_1, a_2 \in D$ (i.e., they are elements of *D*). For instance $a = a_1a_2 = 12$ is an element of *S*, as $a_1 = 1$ and $a_2 = 2$. Let relation $\lesssim$ be the "*dominance*" relation on *S*. For every $a, b \in S$ we say *a* is *dominated* by *b* (written as $a \lesssim b$) if and only if $a_1 \leq b_1$ and $a_2 \leq b_2$. (here $\leq$ is the "*less than or equal to*" relation on natural numbers 1, 2, and 3, i.e., $1 \leq 2$, $2 \leq 3$, $1 \leq 1$, etc.)

1. Does relation $\lesssim$ generate a *partial order* or a *total order* on the elements of *D*? Draw the *Hasse* diagram for the order it generates.
2. Answer the following and justify it.
   a. Does *S* and $\lesssim$ form a lattice?
   b. Now remove elements 21 and 22 from set *S*, i.e. Does the resulting new set *S* and $\lesssim$ form a lattice?