

## HW #1: Warm up!

### CS 392/681: Computer Security Fall 2006

**[100pts] DUE 09/14/2005**

#### **Objective**

The goal of this homework is for me to get a feel of how literate (or illiterate ☺) you are in the area of computer security, and what your background is like. This will help me know the class better and adopt my lectures accordingly.

#### **Problem 1**

- [10pts] List and explain in detail **two** problems related to computer security that you know of or that you encounter in your day-to-day life. Illustrate the problems with examples.
- [10pts] Do you know of any solutions that have been adopted to tackle these problems? If so, explain in detail these solutions.
- [5pts] Are these solutions satisfactory? Explain why or why not.
- [5pts] If the solutions are not satisfactory, do you think they can be improved? If so, explain how.

#### **Problem 2**

1. [10pts] While logging yourself in using a pair of username and password, say, at a web mailing service, you might have noticed that you are often timed-out after 3 failed attempts? What do you think this might protect against?
2. [10pts] If I give you my cell phone number, a four digit number  $S$  and tell you who my service provider is, would you be able to tell if  $S$  corresponds to the last four digits of my social security number (SSN)? Would you be able to crack the last four digits of my SSN? [You can use your cell phone number and info about your service provider to figure out the answer]

#### **Problem 3**

1. [10pts] What are prime and composite numbers? Is 1 a prime? What about 2? What about 111111111111? What about 2984612412461246912643274000528745923462392634918292100009525860457457431332492325235230?
2. [10pts] What is the greatest common divisor (gcd) (I assume the meaning is self-explanatory!) of

- a. 18 and 24?
  - b. 18 and 19?
3. [10pts] Find a natural number  $x$  such that  $9x \bmod 7 = 3$ ? (“ $x \bmod y$ ” denotes the remainder obtained when natural number  $x$  is divided by a natural number  $y$ ; e.g.,  $18 \bmod 5$  is 3)
4. [20 pts] I have a secret 10-bit long password  $K$ . If I disclose a value  $K_0$  such that  $K_0 = f(K)$  for a *public non-invertible* function  $f$  that takes an arbitrary long number and outputs a fixed length (say 1000-bit long) number. Is it possible (given a reasonably powerful computer) for you to determine  $K$ , if you are given  $K_0, f()$  and the length of  $K$ ? If so, how many calls to  $f()$  do you need to make in the worst case? What about if  $K$  is 40-bit long? What if it is 80-bit long?

### Instructions

- I need a first hand input from you (even if it is a plain “I do not know”) – do not refer to or borrow material from other sources.