# Problem Set 1 Solutions

ECS 227 — Phil Rogaway — Spring 2005

**Your Name Here!**

April 4, 2005

## Problem 1

Here you'll put your solution to problem 1. A most *excellent* solution to problem 1. Make all of your solutions excellent and you will make me happy. Don't you want me to be happy?

## Problem 2

To turn this file into a *dvi* file type `latex sample.tex`. The resulting `sample.dvi` can be looked at using a previewer such as *xdvi* (on UNIX) or *yap* (on Windows), and it can be printed out from those programs. To create a *pdf* file you can say `pdflatex sample.tex`.

When working under Windows I use *MiKTeX*, a free distribution of LaTeX and associated programs. You can download it from various web sites; just google *miktex*. After downloading *MiKTeX* you can put its directory of executables in your path and use a command prompt (DOS window) to do things, editing your tex-files with a Windows-based version of *vi* or *emacs*. Alternatively, get your LaTeX distribution under *cygwin*.

## Problem 3

One of the most important aspects of LaTeX is its math mode. Mathematical symbols should look like $a$ or $X_5$ or $Ctr^i$; never write something like x in ordinary text mode—it looks terrible.

## Problem 4

To produce an offset formula you can write things like

$$\begin{aligned} \mathbf{Adv}^{\mathrm{prp}}_{E}(A) &= \Pr[K \xleftarrow{\$} \mathcal{K} : \ A^{E_K} \Rightarrow 1] - \Pr[\pi \xleftarrow{\$} \mathrm{Perm}[n] : \ A^{\pi} \Rightarrow 1] \\ &\leq 1 \end{aligned}$$

## Problem 5

I won't suggest that becoming good with LaTeX is easy; it isn't. But essentially all computer science researchers use this program nowadays—and lots of other scientists and non-scientists do, too. If you are in or bound for graduate school in computer science (or math or physics or $\cdots$), you'll eventually want to learn how to use this program well. (In addition, you'll eventually need to learn

some drawing tool, such as *xfig/jfig*, whose output can be combined with that from LaTeX.) There are numerous good books on LaTeX. The most "standard" one is *LaTeX: A Document Preparation System* (2nd edition), by Leslie Lamport.