Problem Set 1 Solutions

ECS 227 (Fall 2003)

Phillip Rogaway

October 14, 2003

Problem 1

Here goes a solution to problem 1. A most *excellent* solution. 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 tool like `xdvi` (on UNIX) or `yap` (on Windows). When working under Windows I use `MiKTeX` (a distribution of LaTeX and associated programs). You can download it for free from any of numerous web sites.

Problem 3

One of the most important things you need to learn is to use is to use math mode. Mathematical symbols should look like a or X_5 or Ctr^n; never write x in ordinary text mode, it looks terrible.

Problem 4

To produce an offset formula you can write things like

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

Problem 5

I won't suggest that becoming good with LaTeX is easy; it isn't. But essentially all computer scientists use this program nowadays—and lots of other scientists and non-scientists do, too. You'll eventually want to learn how to use this program reasonably well—and you'll eventually want 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.