CS3235 tutorial questions for the days of (Mon Nov 1-Fri Nov 5, 2004) (Not sure what week...)

October 29, 2004

1. (Textbook, p42: Q1) An essential component of the RSA cryptographic scheme is raising a large number x to a large power y (modulo some other number n). We could do this by just multiplying x by itself $y - 1$ times, but this is not fast. Find a faster method for calculating x^y.

(a) Estimate the time complexity of both methods using big $\mathcal{O}$ notation.

(b) Given that a multiplication takes 1mS, and assuming that all other operations are instantaneous, estimate the time to calculate x^y using each method, where y is a randomly generated 100 digit number.

2. What is the precise relation between compressibility and relative entropy of a source?

3. A common technique for inhibiting password guessing is to disable an account after three consecutive failed login attempts. You could argue that this is an example of fail-safe defaults, because by blocking access to an account under attack, the system is defaulting to a known, safe state.
Argue this both ways - that is, find arguments both for and against this position.

4. In class Hugh demonstrated how a buffer overflow attack can be made against a web server running on a LINUX system. Assume that Harry-the-hacker has found a similar vulnerability on a web server on WinXP, and because of the ease of that attack, Harry concludes that WinXP is an operating system with very poor security. Is this a reasonable conclusion? Why or why not?