Instructor: Adam O'Neill
adamo@cs.umass.edu

if (tex.outputmode or tex.pdfoutput or 0) ¿ 0 then tex.print('““pdftrue') end

HOW TO CALCULATE RUNNING-TIMES

The main point. We will count running-times *symbolically for oracle queries, cryptographic, and arbitrary functions; and otherwise, asymptotically, converting concrete numbers into variables.* Note common operations like XOR, string comparison, bit-wise complement, *etc.* are linear-time operations, so can be hidden under the same asymptotic term. So, for example, if a PRF-adversary calls oracle Fn twice and then computes AES twice, xor'ing the outputs and comparing the result to some fixed string, we would calculate running-time as: "2 Fn queries + $2 \cdot T_{\mathsf{AES}} + O(\ell)$, where for AES $\ell = 128$." In particular, the $O(\ell)$ term comes from the constant number of xor and string comparisons.

Further examples. Let's give more examples of how to calculate running-time of the adversaries in the homework under these guidelines. In the homework 2 solutions, Part B, the running-time of the given adversary would be "2 Fn queries + $2^{130} \cdot T_{\mathsf{AES}} + O(\ell)$ where $\ell = 128$ for AES." As above, the $O(\ell)$ term comes from the constant number of xor and bit-wise complement computations.

Number-theoretic algorithms. *In the number-theoretic setting we can use asymptotics naturally because numbers can vary in bit-length.* You are expected to know the running-time of the basic algorithms discussed in class (there is a table in the slides giving these). The only one whose running-time derivation is not explained is $\mathsf{EXT\text{-}GCD}$, so just remember that it's quadratic-time; and you should understand that $\mathsf{MOD\text{-}INV}$ calls $\mathsf{EXT\text{-}GCD}$ so its running-time is also quadratic-time. You should also understand that exponentiation in a group $G = \langle g \rangle$ exponentiating g to the power m uses $O(|m|)$ g-operations by the square-and-multiply algorithm; when $G = \mathbb{Z}_p^*$ the g-operation is multiplication modulo p which is quadratic time. Thus is $|m|$ is on the order of $|p|$ as it is commonly for discrete-log-based schemes, exponentiation in $\mathbb{Z}_p^*$ is *cubic-time.*