Midterm #1

MON, 3/1

exam: 1:25 – 2:15 PM

upload work by 2:45 PM
PDF

format

- check it out ! — link in email
- show-your-work problems — ~ 3
- short answer problems — ~ 10

use calculator / Sage to compute things like powers

practice

- review HW
- practice problems + solutions

tools

- calculators allowed — but: show work
- notes allowed — but: watch time

Questions ?

not on the exam historical ciphers, credit cards, CSS

- review of number theory
  congruences, modular inverses (Euclid !),
  phi function, little Fermat + Euler,
  numbers in different bases
- binary exponentiation
- one-time pad
- stream ciphers + PRGs
  LCG
  LFSR, period
- Chinese remainder theorem
  solving quadratic equations
  number of solutions
  quadratic residues
- Blum-Blum-Shub
- primes + primality testing
  Fermat + Miller-Rabin, liars
  PNT