Admin:

- Pset #1 posted; due Mon 2/23
- See TAs if you don't have pset group
- Recitation #1 this week (Fri 2/13 11am 4-270)

Reminder:

- See "The Imitation Game" Thu 7pm
  (see link to Piazza to sign up...)
- DSP07 4pm "Secure Computation"

Today:

- [ ] Finish LO1 material
- [ ] "Growth of Cryptography" talk (Killian award lecture)
Some principles:

- be sceptical & paranoid
- don’t aim for perfection
  (“there are no secure systems, only degrees of insecurity…”)
- tradeoff cost/security
  (“to halve the risk, double the cost…” - Adi Shamir)
- be prepared for loss
- “KISS” (“keep it simple, stupid!”)
- ease of use is important
- separation of privilege - require 2 people to perform action
- defense in depth (layered defense)
- complete mediation (all requests checked for authorization)
- least privilege (don’t give some more permissions than they need)
- education
- transparency (no security through obscurity)
- sharing information about vulnerabilities & defenses