Admin:

Pset #1 posted today, due Mon 2/26

Pset groups being created by TAs & emailed today.

Recitations in 54-100

Today:

☐ "Growth of Cryptography"

(Rivest Killian lecture - see slide)

☐ Principles of Security

(copied pg 2 here, also pg 8 of LO1 notes)
Some principles & maxims:

- Think adversarially
- Be sceptical & paranoid
- Don’t aim for perfection
  ("There are no secure systems, only degrees of insecurity," Shamir)
- Tradeoff: cost/security
  ("To halve the risk, double the cost," Shamir)
- Tradeoff: ease-of-use/security
- Attacker has to find only one vulnerability,
  Defender has to protect or monitor them all
- “Assume that your system has been breached”
  (Deterrence/recovery may be more important than prevention)
- Defense in depth (layered defense) ≠ Be prepared for less.
- “Don’t underestimate the time & effort an adversary will spend trying to break your system” (Morris Sr.)
- Use “separation of privilege” — require a people to perform sensitive action
- Use “least privilege” — don’t give someone more permissions than they need
- Complete mediation — all requests checked for authorization
- Transparency — no security through obscurity
- Importance of education & training
- Sharing info about vulnerabilities can help
- Computers & software are toys — if you play roughly with them, they will break
- Adversaries to worry about:
  - Insiders
  - NSA
  - Chinese