Logistics

- Final Exam: Monday, 3/19 3:00pm – 6:00pm in Franz Hall 1260
  - Roughly 20% before midterm, 80% after midterm
  - Closed book & notes, allow up to 2 double-sided cheat sheets

- *Please complete course evaluation on MyUCLA, thanks!*
Wireless security threats

- Eavesdropping
- Impersonation
- Hijacking/MITM Attack (Man-in-the-middle attacks)
- DoS (Denial of Service)
Symmetric key v.s. public key cryptography

- Symmetric key crypto: DES, AES
- Public key crypto:
  - Diffie-Hellman, RSA
  - CA (certificate authority)
More things to know

• How to achieve:
  • Encryption
  • Authentication
  • Digital signature
  • Message integrity
• SSL, IPSec, VPN, Firewall …
Study guide & sample final solutions