# Foundations of Network and Computer Security

John Black

CSCI 6268/TLEN 5831, Fall 2004

# Introduction

- UC Davis
  - PhD in 2000
  - Cryptography
  - Interested in broader security as well
- UNR two years
- CU Boulder two years
- Computer and Communications Security Center
- My teaching style and personality

# This Class

http://www.cs.colorado.edu/~jrblack/class/csci6268/f04/

- Use above for all materials
  - Available from my home page
  - Available from WebCT as well

- This is a CAETE course
  - About 4 distance-learning students
    - Any live students today?
  - Lectures from WebCT, I think
  - Lectures on VHS in library in Math bldg

# Logistics

- TR, ECCS 1B12, 9:30am – 10:45am
- Final, Monday Dec. 13th, 10:30am – 1pm

- Office Hours
  - ECOT 627, W 4-4:50pm; R 9:00-10:00am
  - More as needed
  - **jrblack@cs.colorado.edu** (better than dropping by without an appt)

# Grading

- See course info sheet
  - Let's go over it now
- Course Topics
  - Why no book?
  - Cryptography and Network Security
    - Quite a blend of math, hacking, and thinking

# Topics

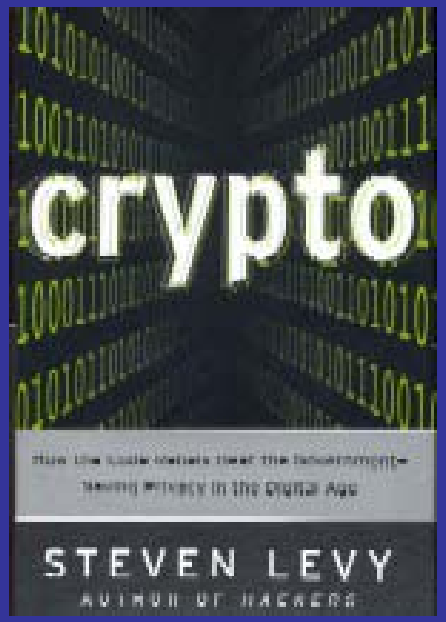
- Policy, Law, History
  - Today
- Cryptography (can't help it)
  - Not how to make it, but how to *use* it
- Hacking
  - Buffer overruns, WEP attack, TCP session hijacking, DDoS, prevention
  - Some hands-on, but depends on distance students

# Class Format

- Informal
  - Small class
  - Ask questions
  - Class participation counts for 5% of grade
  - (Not sure what to do with distance folks for this yet.)

# History

- Early days of Cryptography
- Lucifer and DES
- Export restrictions
  - 40 bit keys!
- Public Key Cryptography
  - MI6 had it first?!
- Differential cryptanalysis
  - NSA knew first



# Who is the NSA?

- National Security Agency
  - Huge
  - Fort Meade, MD
  - More mathematicians than anywhere
  - Classified budget

# Laws

- DMCA
  - Felten RIAA/SDMI case most famous
    - 2001 SDMI challenge
  - Many believe it's the right idea, but a bad law
  - All reverse-engineering is sketchy
- CALEA (1994)
  - Communications Assistance for Law Enforcement Act
  - Recently ruling says VoIP must provide compliance
    - Still in the courts
- Patriot Act

# Case Study

- Accountant for crime ring
  - Used PGP
    - Pretty Good Privacy
    - Phil Zimmerman
  - Feds seized computer
    - Couldn’t read files!
  - Subpoena for keylogger
  - Worked like a charm!

# Policy

- Government has attempted to control encryption before
  - Skipjack
  - Key Escrow
  - Clipper Chip
- Ultimately failed due to massive protest from “privacy advocates”
  - Electronic Frontier Foundation (John Gilmore)