

# Cryptography Overview

John Mitchell

# Announcement: Homework 1

- ◆ Posted on web
  - Five problems
- ◆ Due April 29

# Cryptography

## ◆ Is

- A tremendous tool
- The basis for many security mechanisms

## ◆ Is not

- The solution to all security problems
- Reliable unless implemented properly
- Reliable unless used properly
- Something you should try to invent yourself unless
  - ♦ you spend a lot of time becoming an expert
  - ♦ you subject your design to outside review