Lecture 1 Outline

Reading: text, §1

Assignments due: Homework #1, due April 13, 2001 at 11:55pm

1. Greetings and felicitations!
   a. About the class
   b. Prof. Rogaway is teaching ECS 189A, Cryptography, this term (MWF 2:00pm–3:00pm in 146 Robbins)

2. Basic components of computer security
   a. Confidentiality
   b. Integrity
   c. Availability

3. Classes of threats
   a. Disclosure
   b. Deception
   c. Disruption
   d. Usurpation

4. Policy vs. mechanism
   a. Policy
   b. Mechanism

5. Goals of security
   a. Prevention
   b. Detection
   c. Recovery

6. Trust and Assumptions