UNIVERSITY of WISCONSIN-MADISON
Computer Sciences Department

CS 537
Introduction to Operating Systems

Andrea C. Arpaci-Dusseau
Remzi H. Arpaci-Dusseau

# Encryption

## Questions answered in this lecture:

- How does encryption provide privacy?
- How does encryption provide authentication?
- What is public key encryption?
- What is symmetric key encryption?

# Motivation

Scenario: Communicate between two endpoints over unprotected channel (e.g., network)

- Others can eavesdrop on channel
- Others can inject messages on channel

Goals

- Provide secure communication
  - No one can understand message contents
- Provide authentication
  - Establish identify of sender
  - Ensure that message contents are not altered

# Encryption Mechanism

Convert data to form that does not make sense to others

Terminology

- Clear text (plain text): Initial readable text that needs protection
- Cipher text: Encrypted version of clear text

Steps

- Sender: Encrypt clear text to cipher text
  - Apply function with encryption key to clear text
- Cipher text can be stored in readable file or transmitted over unprotected channels
- Receiver: Decrypt cipher text to clear text
  - Apply function with decryption key to cipher text

Based on factoring very large numbers (product of two primes)