Introduction to Cryptography CS 355

Lecture 1

Overview of the Course

See the Course Homepage

- http://www.cs.purdue.edu/homes/ninghui/courses/Fall05/index.html

CS 355 (Introduction to Cryptography)
or
CS426 (Computer Security)

CS 426: Taught by Dr. Keith Frikken

- Basic introduction to computer security
- Not an in-depth course of cryptographic protocols or secure system design –- it is more high level
- Primary difference to 355: less mathematically focused and more systems focused

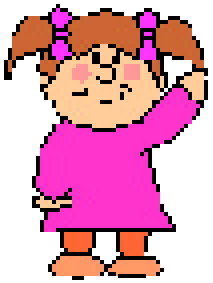
Topics in CS426 include

- Security Policies
- Basic Cryptography
- Database Security
- Identity Management
- Malicious Logic
- Legal and Ethical Issues
- Time Permitting:
  - Program Security
  - Network Security

Going Back to 355

Let’s Make the Introductions

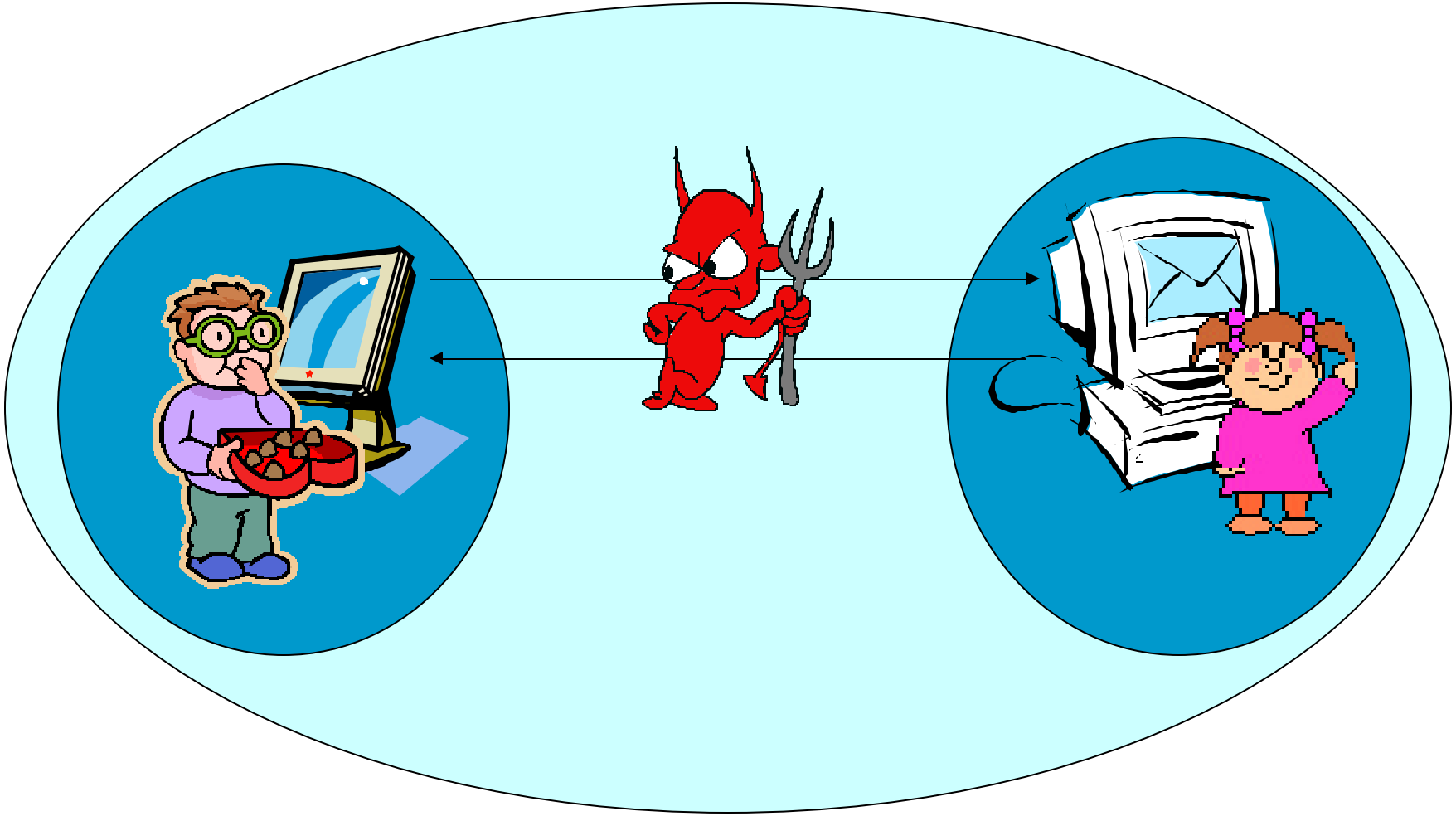
- Alice



- Bob

- Eve

Secure Communication



Goals of Cryptography

- The most basic problem: ensure security of communication over insecure medium
- Security goals:
  - privacy (secrecy, confidentiality)
    - only the intended recipient can see the communication
  - authenticity (integrity)
    - the communication is generated by the alleged sender

Approaches to Secure Communication

- Steganography
  - “covered writing”
  - hides the existence of a message
- Cryptography
  - “hidden writing”
  - hide the meaning of a message

Basic Terminology in Cryptography

- plaintexts,
- ciphertexts,
- keys
- encryption
- decryption
- cryptography
- cryptanalysis
- cryptology

Phases in Cryptography's development

- Cryptography is driven by computing and communication technology
- First stage, paper and ink based scheme
- Second stage, use cryptographic engine
- Third stage, modern cryptography
  - relying on mathematics and computers
  - information-theoretic security
  - computational security

Example Usages of Cryptography

- In History
- In current life

Secret-key Cryptography vs. Public-key Cryptography

- Secret-key cryptography (a.k.a. symmetric cryptography)
  - encryption & decryption use the same key
  - key must be kept secret
  - key distribution is very difficult
- Public-key cryptography (a.k.a. asymmetric cryptography)
  - encryption key different from decryption key
  - cannot derive decryption key from encryption key

A Sample List of Other Goals in Modern Cryptography

- Pseudo-random number generation
- Non-repudiation: Digital signatures
- Zero-knowledge proof
- Commitment schemes
- E-voting
- Secret sharing

What Cryptography is About?

- Constructing and analyzing protocols which enables parties to achieve objectives, overcoming the influence of adversaries.
  - a protocol (or a scheme) is a suite of algorithms that tell each party what to do

- How to devise and analyze protocols
  - understand the threats posed by the adversaries and the goals

The Rules of the Game

1. Overcome the adversary only by means of protocols
2. Protocol designs are made public, only keys are secret
   - security by obscurity does not work

What is This Course About?

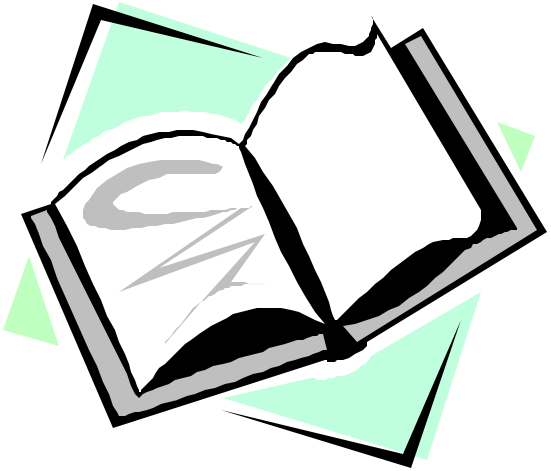
- Mostly mathematical
  - understand the fundamentals of protocol design
  - understand the mathematics underlying the cryptographic algorithms & protocols

Backgrounds Necessary for the Course

- Probability theory
  - a brief overview will be given to refresh your memory
- Data structures and basic analysis of algorithms

Recommended Reading for This Lecture

- Trappe & Washington
  - Chapter 1



Coming Attractions …

- Shift cipher
- Substitution cipher

- Recommended reading for next lecture:
  - The Code Book: Chapter 1