What me worry?

An introduction to cryptography

---

**CS349 Cryptography**

Department of Computer Science
Wellesley College

---

**Cryptology**

- This course is about secrets.
- Making secrets (**cryptography**), and breaking them (**cryptanalysis**).
- But, who are we keeping secrets from?
The woods are full of noises

You can get further with a kind word and a gun than you can with a kind word alone.

Willy Sutton, bank robber


Confidentiality and beyond

- Historically, the focus cryptology has been on the use of conventional encryption to provide confidentiality.
- More recently, we have seen cryptology used to address a number of other considerations.
Security services

**Confidentiality**
Protection of data from unauthorized disclosure.

**Authentication**
Assurance that the origin of a communication is correctly identified.

**Integrity**
Only authorized entities are able to modify resources.

**Nonrepudiation**
Protection against denial by one of the parties.

**Access control**
Prevention of unauthorized use of a resource.

Thwarting the snooper

- If encryption is to be used to counter attacks on confidentiality, we need to decide what to encrypt and where the encryption function should be located.
- In other words, we need to understand where we are vulnerable.
Points of vulnerability

A good place to start

John the Ripper

- People are usually the weakest link.
- Access to etc/passwd is a giant security hole that existed in the CS Department for many years.
- Social engineering is often easier still.
Broadcast networks and wiring closets

Switched LANs may require access to the wiring closet.

Workstations on the same link can sniff with impunity.

Telnet application over TCP

Host A

User types 'c'

Host ACKs receipt of echo'd 'c'

Time

Seq=45, ACK=43, Data='c'

Seq=43, ACK=40

Host B

Host ACKs receipt of 'c'

Echoes back 'c'

Time
Sniffing a password

The great outdoors

Communications to the outside world are especially vulnerable
**Datagram networks**

A datagram network sends a packet by stamping it with the address of the destination and dropping it into the network.

Traffic analysis

- Sometimes it is enough just to know that the communication is taking place.
- Traffic analysis may be used to
  - Identify communication partners;
  - frequency of communication;
  - message pattern;
  - length, or quantity;
  - correlate traffic with events.
Model of conventional cryptosystem

Fundamentals of conventional ciphers

Substitution

The pigpen cipher was used by the Society of Freemasons and Confederate soldiers during the civil war.

Transposition

Spartans spirally wrapped a strip of parchment around a tapered rod called a scytale before writing on it.
Traditional symmetric-key encryption has a big problem

The protagonists

Alice  Bob
plaintext  encryption  ciphertext  decryption  plaintext

Carol
Diffie-Hellman-Merkle key exchange

1. Alice chooses a number
   \( A = 3 \)
   and keeps it a secret
2. Alice calculates \( 7^A \mod 11 \)
   \( 7^3 = 343 = 2 \mod 11 \)
3. Alice sends 2 to Bob
   Bob sends 4 to Alice

Carol listens intently

4. Alice takes Bob's result,
   and works out \( 4^A \mod 11 \)
   \( 4^3 = 64 = 9 \mod 11 \)
   Bob takes Alice's result,
   and works out \( 2^B \mod 11 \)
   \( 2^6 = 64 = 9 \mod 11 \)

Splitting up a secret

- There are many occasions when it is necessary to divide a key into puzzle parts.
- This is a good way to force people to cooperate.
- Nuclear weapon systems require two people to turn different keys simultaneously.