Computer Security

- One of the fastest growing areas in Computer Science
- Enormous budget for research on security (DARPA)
- Fundamental for electronic commerce

Computer Security

- Security covers a wide range of issues
  - Local access: e.g., OS and database access
  - Distributed access: e.g., cryptography, firewalls
  - Hardware: transmission line protection, “vaults”
  - Software: algorithms
- Focus in Webware: distributed access (network security) and software solutions
Network Security: Four areas
(see Tanenbaum)

• Secrecy
  – Keep the information out of the hands of unauthorized users (e.g., credit card numbers)

• Authentication
  – Know whom we are talking to, especially when sharing sensitive information

Network Security: Four Areas
(see Tanenbaum)

• Nonrepudiation
  – Ensure commitment to a transaction - similar to a signature. Typical example: X sold you gold at $y/ounce and gold has since doubled! X denies the transaction took place.

• Integrity Control
  – Ensure integrity of the information sent, that is, that nobody tampered with it in transit or made up a false message.
Secrecy: Cryptography

- Cryptography: art of devising ciphers
- Cipher: mathematical formula
- Key: parameter of the cipher

Cryptography

- Traditional cryptography:
  - Symmetric Ciphers. Use private key or secret key ciphers.
- Modern cryptography:
  - Asymmetric ciphers (one-way). Use public key ciphers.
- Hybrid cryptography: People agree on secret key (e.g., using asymmetric cipher or another method), and use symmetric cipher from then on. Can be more efficient.