Week 4
Cryptography Overview

Study Areas

- Cryptography
  - From Latin: “secret writing”
  - The study of creating ciphers
- Cryptanalysis
  - The study of breaking ciphers
- Cryptology
  - The encompassing study of cryptography and cryptanalysis

Related Techniques

- Encryption/decryption
- Message digests (digital hash)
- Digital signatures/verification
- Digital certificates
- Key management
- Authentication
- Many more

Cryptographic Services

- Confidentiality
- Integrity
- Authentication
- Nonrepudiation
  - It provides the inability of a user to deny previous activities (e.g., sending a message).

- Examples?
  - Please try to find an example of each service above.

Cryptographic Systems

- Secret key (symmetric) cryptography
  - Conventional
  - Single key
- Public key (asymmetric) cryptography
  - Two keys
  - Introduced in the late 1970s
- Why are they called symmetric or asymmetric?
  - Check the number of keys required in each cryptographic system