Introduction
Ahmet Burak Can
Hacettepe University
abc@hacettepe.edu.tr

Books
• Textbook:
• Supplementary books:
  ◦ Handbook of Applied Cryptography. A. Menezes, P. van Oorschot and S. Vanstone. CRC Press

Outline of the Course
• Basic ciphers
• Block ciphers, Encryption modes and Stream ciphers
• Hash functions, message digests, HMAC
• Number Theory, Public Key Cryptography, RSA
• Digital certificates and signatures, X509
• Authentication: Two–Three factor authentication, Biometrics, Smart Cards
• Security Handshake
• Real-time Communication Security, SSL/TLS, IPSEC
• Kerberos

Outline of the Course
• Threshold cryptography
• Operating System Security
• Malicious Software: Trojans, logic bombs, viruses, worms, botnets, rootkits, trapdoors and cover channels
• Program Security
• Firewalls, VPNs, Intrusion detection systems
• HTTP and Web Application Security, XSS
• Wireless Security: WEP and WPA

3.11.2016
Information Security

- Computer Security:
  - Ensure security of data kept on the computer
- Network Security:
  - Ensure security of communication over insecure medium
- Approaches to Secure Communication
  - Steganography
    - hides the existence of a message
  - Cryptography
    - hide the meaning of a message

Basic Security Goals

- Privacy (secrecy, confidentiality)
- Authenticity (integrity)
- Authorization
- Availability
- Non-repudiation
- Auditing

Least significant bit values of pixels can be used to hide a secret message

- Below images seem to be same but right picture store 5 Shakespeare games.

Steganography Sample

Hamlet, Macbeth, Julius Caesar
Merchant of Venice, King Lear
Privacy (secrecy, confidentiality)

- Only the intended recipient can see the contents of the communication.
- SSL https protocols can protect privacy of communication.
- Some applications have encrypted communication capabilities to protect privacy, such as Skype, WhatsApp.

Authenticity (integrity)

- The communication is generated by the alleged sender.
- Are you sure that you are communicating with the right person?

Authorization

- Limit the resources that a user can access.
- In the real world, we use locks, fences etc.
Authorization

- If authorization mechanisms are not properly defined, resources cannot be protected.

Availability

- Make the services available 99.999...% of time

Authorization

- In the digital world, we use password, smartcard, USB tokens, fingerprints, etc. for authentication.

- Sometimes multiples of them 😊

Availability

- Internet worms can cause billions of dollar damage, such as Slammer, Nimda, Code Red worms.
- Availability is requirement for Internet companies!
Non-repudiation

- No party can refuse the validity of its actions.
- In the real world, we use wet signatures, authorization offices (noter):
  ![Signature]
- In the digital world, similar signature techniques can be used:

Auditing

- Take a log of everything done in the system
- Then use it for further analysis