

## Outline for May 27, 2022

**Reading:** *text*, §54, 55

**Assignments:** Lab Exercise 2, due June 2

---

1. Announcements
2. Network Security
  - (a) Cryptographic considerations
  - (b) Firewalls
3. Cryptography
  - (a) Symmetric cryptography
    - i. Transposition cipher
    - ii. Substitution cipher
    - iii. Product cipher
    - iv. AES
  - (b) Public key cryptography
    - i. Requirements for public (encryption) and private (decryption) keys
    - ii. RSA
    - iii. Provides confidentiality, integrity, authentication, non-repudiation
    - iv. Cryptographic hashes and digital signatures
4. Malware
  - (a) Trojan horses
  - (b) Computer viruses
  - (c) Computer worms
  - (d) Bacterium, rabbits
  - (e) Logic bombs