Announcements

- **Reading**
  - Today: 7.1

- **No Office Hours on Wed**
  - will have office hours on Thursday 10:45 to 11:45
DES

- Block cipher: uses 56 bit keys, 64 bits of data
- Uses 16 stages of substitution
- Variations
  - cipher block chaining: xor output of block n with into block n+1
  - cipher feedback mode: use 64bit shift register
    - can produce one byte at a time

From: *Computer Networks*, 3rd Ed. by Andrew S. Tanenbaum, (c)1996 Prentice Hall.
Public Key Encryption

- Split into public and private keys
  - public key used to encrypt messages
    - publish this key widely
  - private key used to decrypt messages
    - keep this key a secret

- RSA
  - algorithm for computing public/private key pairs
  - based on problems involved in factoring large primes
  - for an n bit message $P$, $C = (P^e \mod n)$, and $P = (C^d \mod n)$

- Other Public Key Algorithms
  - knapsack
    - given a large collection of objects with different weights
    - public key is the total weight of a subset of the objects
    - private key is the list of objects
Authentication

- Identify the parties that wish to communicate
- Create a session key
  - a random string
  - used only for one session
- Authentication based on Shared Keys
  - each party already shares a private key
    - exchanged via an out of band transmission
  - challenge-response
    - send a random string
    - response is the encryption of the random string with the shared key
Authentication Example

From: Computer Networks, 3rd Ed. by Andrew S. Tanenbaum, (c)1996 Prentice Hall.
Simplified Protocol

- Only requires three messages
- But it is subject to a “man in the middle attack”

From: Computer Networks, 3rd Ed. by Andrew S. Tanenbaum, (c)1996 Prentice Hall.
Attacking the Simplified Protocol

- T can get B to respond to its own challenge
- T opens a second session with B
  - it issues B’s session 1 challenge back to B in session 2
Key Distribution Center

- **Problem with Private Key Authentication**
  - Need to establish key
  - for n people need $n^2$ keys
  - keys must be established via **out-of-band** communication

- **Solution: Key Distribution Center (KDC)**
  - trusted party used to assist in authentication
  - each party establishes a private key with the center

- **have KDC trans-code a message with a session key**
  - A sends to KDC $<A, K_A(B, K_s)>$
  - KDC sends to B $<K_b(A, K_s)>$
  - open to replay attack
    - T logs KDC to B message **and** all traffic using $K_s$
Needham-Schroeder Authentication

- $R_A$, $R_{A2}$ and $R_B$ random strings
  - used to prevent replay attacks
- If $T$ ever gets $K_s$ can establish contact with $B$
  - can prevent this with a slight variation of the algorithm
- Used in Kerberos Authentication System