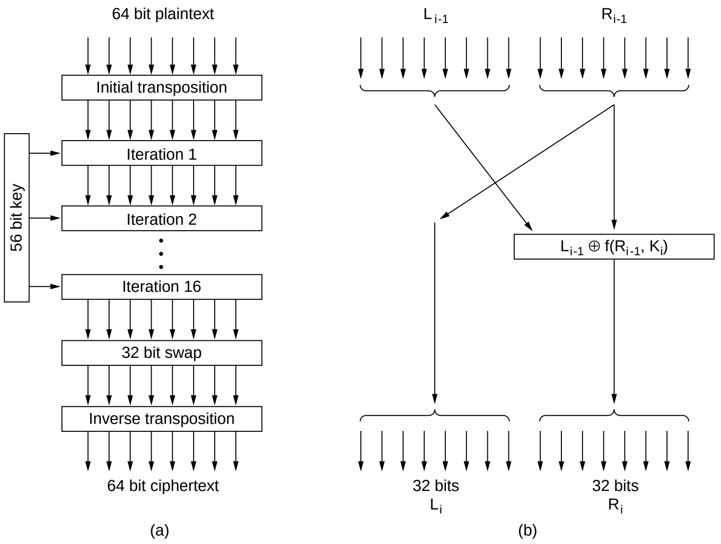
Announcements

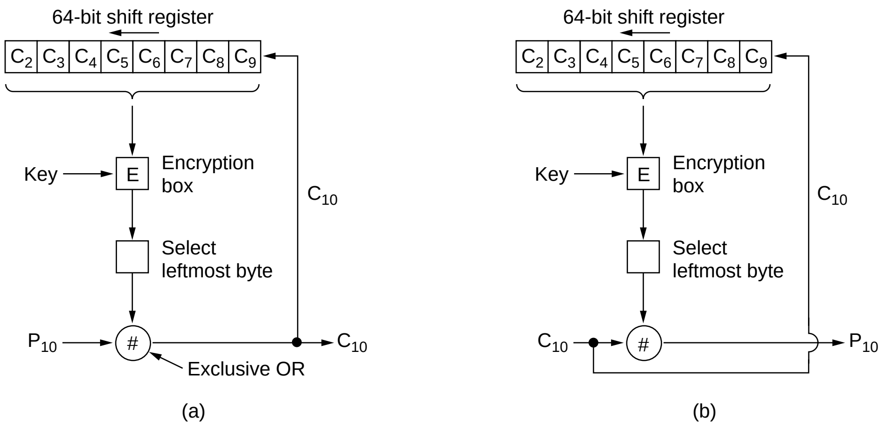
- Reading
  - Today: 7.1
- No Office Hours on Wed
  - will have office hours on Thursday 10:45 to 11:45

copyright 1997 Jeffrey K. Hollingsworth

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.

copyright 1997 Jeffrey K. Hollingsworth

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

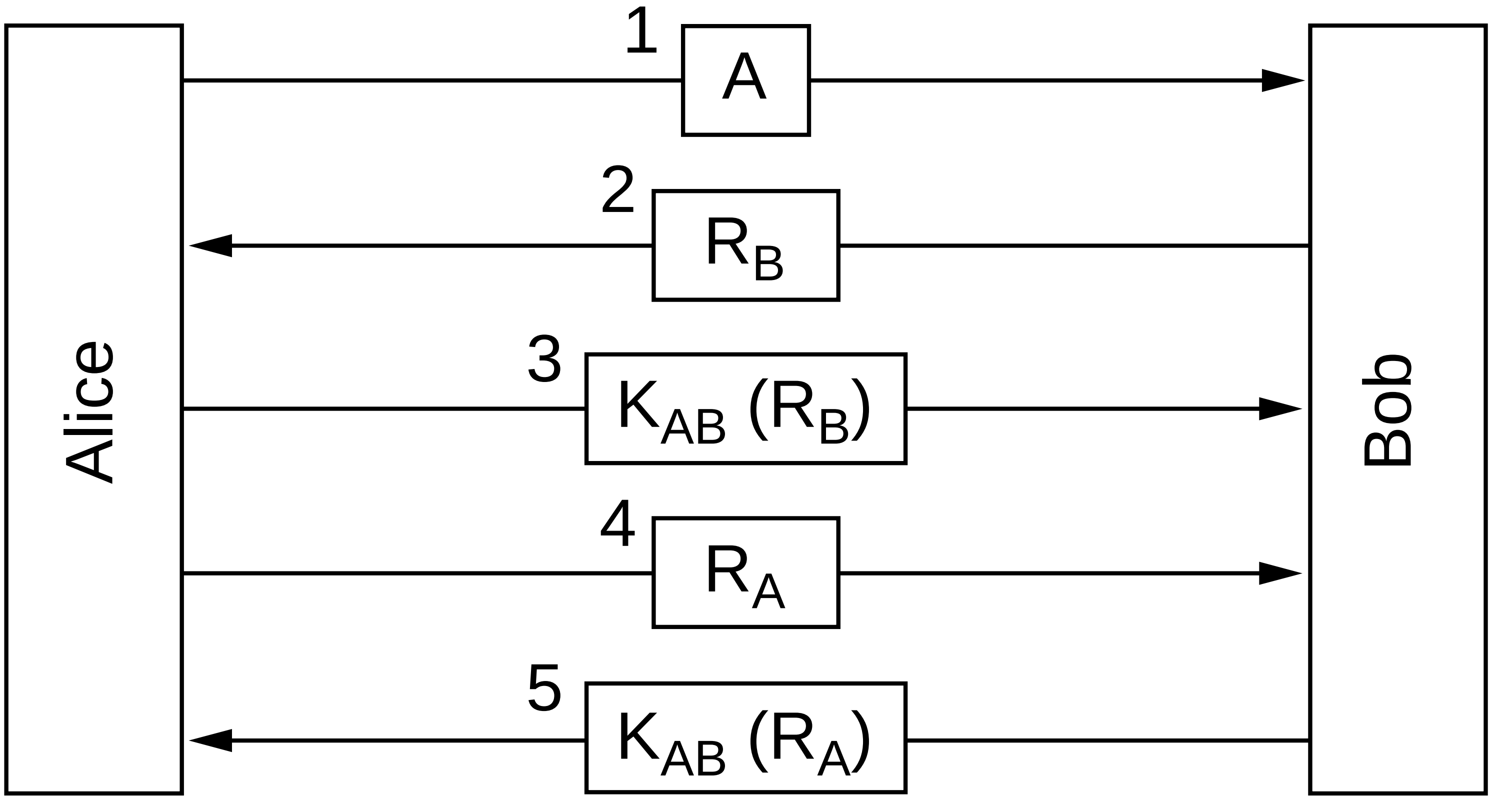
copyright 1997 Jeffrey K. Hollingsworth

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

copyright 1997 Jeffrey K. Hollingsworth

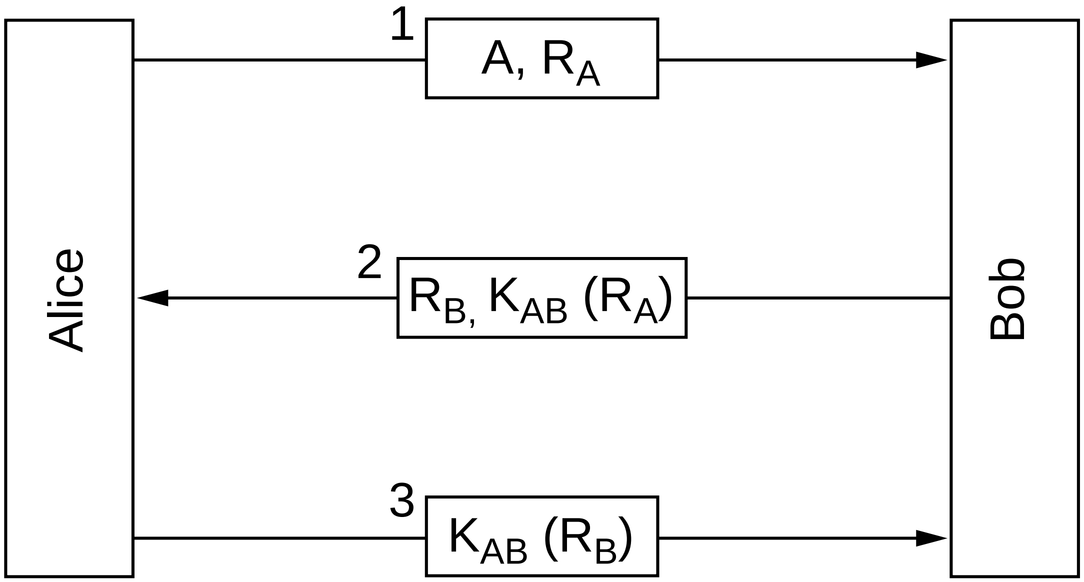
Authentication Example



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

copyright 1997 Jeffrey K. Hollingsworth

Simplified Protocol



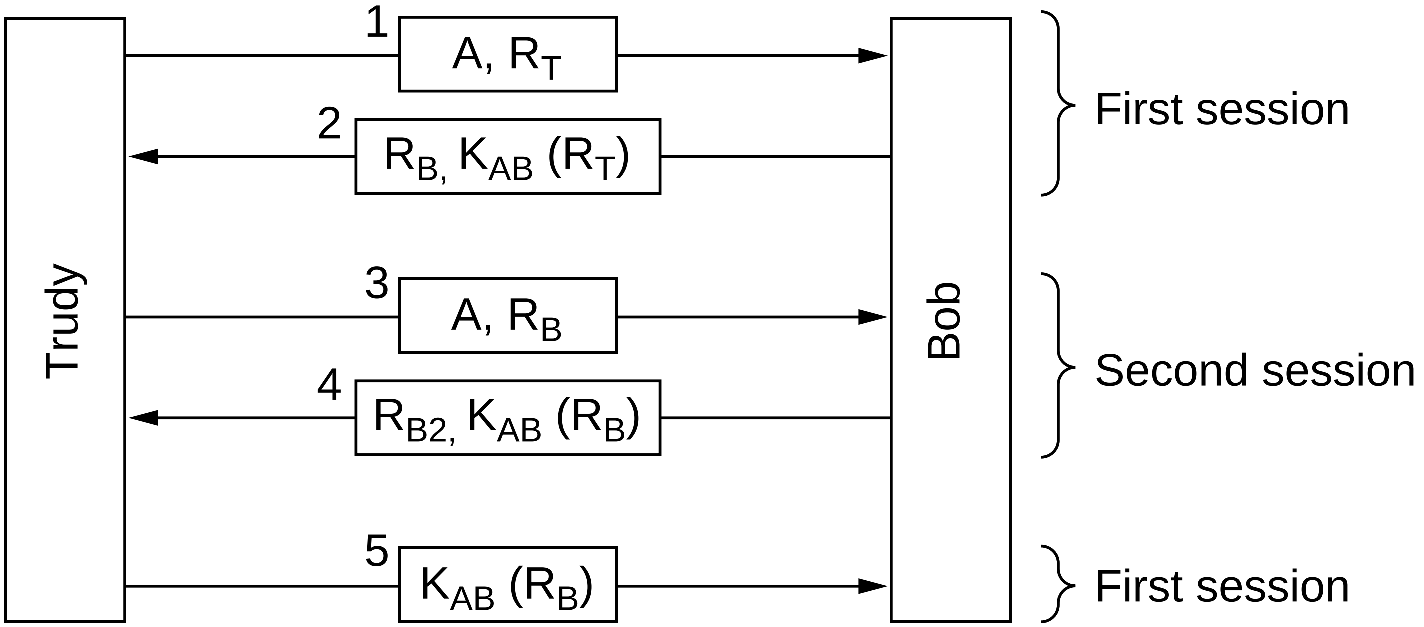
From: *Computer Networks*, 3rd Ed. by Andrew S. Tanenbaum, (c)1996 Prentice Hall.

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

copyright 1997 Jeffrey K. Hollingsworth

Attacking the Simplified Protocol

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



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

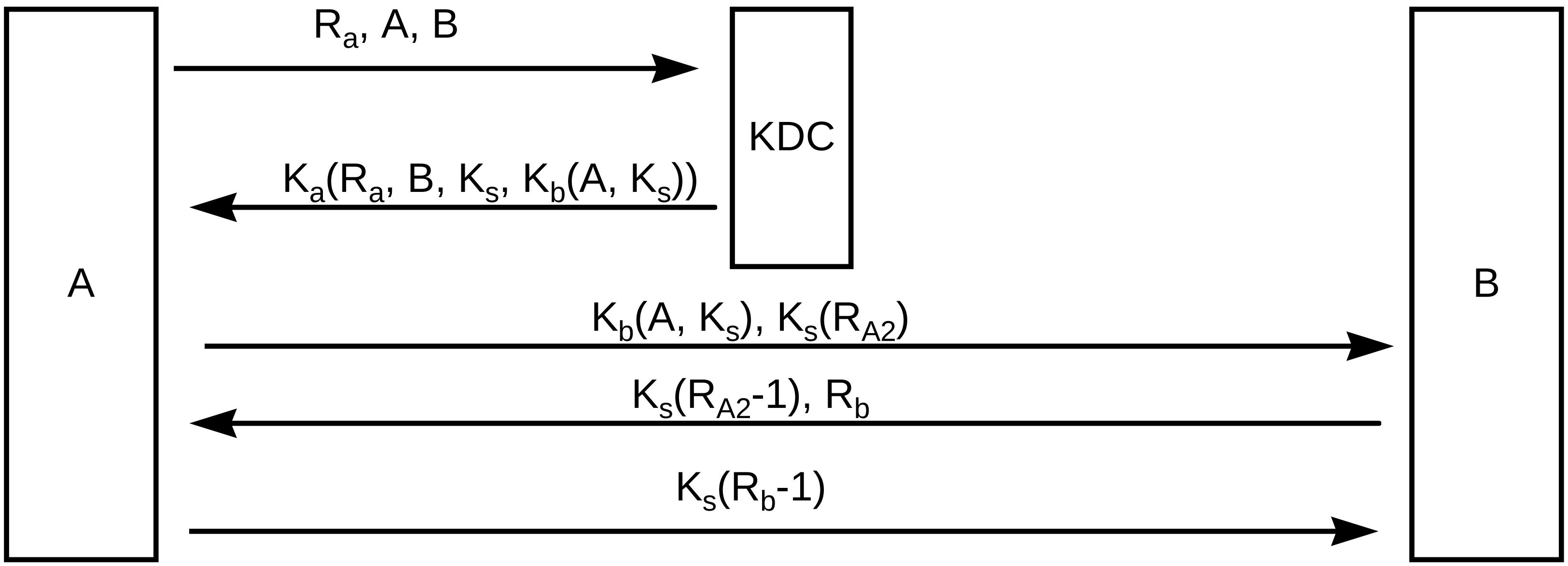
copyright 1997 Jeffrey K. Hollingsworth

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

copyright 1997 Jeffrey K. Hollingsworth

Needham-Schroeder Authentication


R_a, A, B
KDC
$K_a(R_a, B, K_s, K_b(A, K_s))$
A
B
$K_b(A, K_s), K_s(R_{A2})$
$K_s(R_{A2}\text{-}1), R_b$
$K_s(R_b\text{-}1)$

- 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

copyright 1997 Jeffrey K. Hollingsworth