

# Computer Security

## Key Management

# Key Management

- cryptography is used in real systems
- That means the keys exist in real systems
- Some questions
  - How many are there?
  - Who creates them?
  - Where are they stored?
  - etc

# Key Management

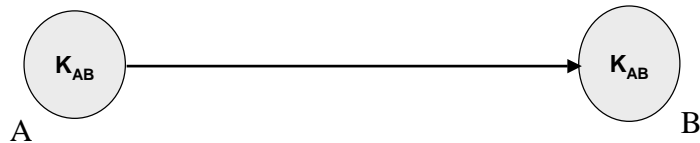
- We'll look at key management in a number of parts of this course
- For now a brief introduction will do

# How Many Keys Are There?

- For basic symmetric cryptography there need only be one
  - The shared secret key
- For basic asymmetric cryptography there needs to be four
  - Private and public key for each participant

## Who Knows The Key

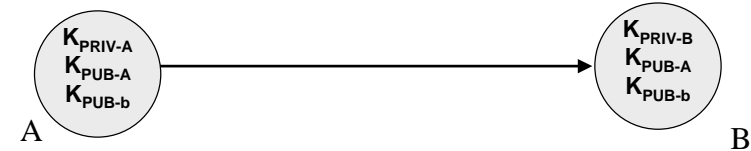
- For symmetric cryptography both participants know the key



5

## For asymmetric cryptography

- Each secret key is known only by its owner
- The public keys are known by everybody



6

## Session keys vs. Long Term Keys

- The above assumes a minimal number of keys
- If one key is used too much and/or for too long it is more vulnerable
- So use more keys for less time each
  - Session keys
  - Replacement keys

7

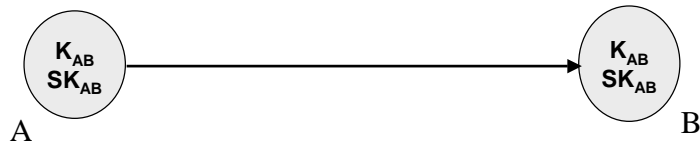
## Session Key

- Used for a “session”
- Once the long term secret(s) is (are) used for authentication a session key generated
- Discarded once communication completed

8

## Who Knows What Keys?

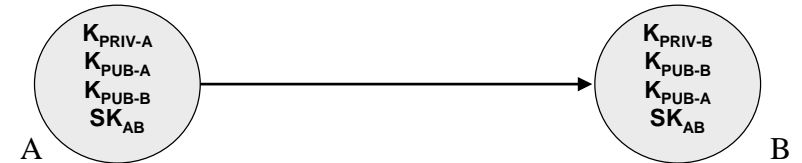
- For symmetric cryptography with session key  $SK_{AB}$



9

## Who Knows What Keys?

- For asymmetric cryptography with session key  $SK_{AB}$
- Note the session key is a *symmetric* key



10

## Replacement Keys

- Once a key (either session or long term) has been used for a while it may be wise to replace it
- Need to tell everyone who knows the key what the new one is - *securely*

11

## Who Creates the Keys?

- For a symmetric key (long term or session)
  - One participant?
  - Both?
  - A trusted third party?
- For an asymmetric key pair
  - The owner?
  - A trusted third party?

12

## How are they Distributed

- For a session (or component) key it can be distributed protected by a long term secret
- For long term keys there is no other key to protect their distribution in the system
- Must be distributed off-line or by special mechanism

13

## Where are stored

- the keys need to be protected
- Have to store them in the user's storage space
- How are they protected?
- Often by passwords
- Which are cryptographically much less secure
- Hmmmm.....

14

## Summary

- Remember who knows what keys and how many
- The difference between long term and session key
- Key distribution
- Key protection
- We'll look at a lot of this in more detail as we go through the course

15