UNIVERSITY OF OREGON

CIS 433/533 - Computer and Network Security

Public Key Crypto/ Cryptographic Protocols

Professor Kevin Butler
Winter 2010

Key Distribution/Agreement

UNIVERSITY OF OREGON

- Key Distribution is the process where we assign and transfer keys to a participant
  - Out of band (e.g., passwords, simple)
  - During authentication (e.g., Kerberos)
  - As part of communication (e.g., skip-encryption)

- Key Agreement is the process whereby two parties negotiate a key
  - 2 or more participants
- Typically, key distribution/agreement this occurs in conjunction with or after authentication.
  - However, many applications can pre-load keys

Key Distribution

UNIVERSITY OF OREGON

- Say we used pairwise key distribution/agreement in this class (strictly symmetric cryptography)

- **Q: how many key negotiations would there be?**

- 36481 ASes in the Internet: how many negotiations for secure routing solutions?