Computer and Network Security: Long-term Key Distribution

Kameswari Chebrolu

Basic Idea

- Use Long-term key to authenticate
- In the process establish a short-term session key
- Use session key for confidentiality and integrity

Outline

- **Long-term Key Management**
  - **Shared and Public key systems**
- Authentication Protocol
  - One way, two-way and mediated authentication
  - Short-term/session key establishment
  - Confidentiality/Integrity of data

Question?

“Can two parties agree on a shared key over an insecure channel without any prior communication?”

Ans:

1. Passive Eavesdropping: Yes
2. Modify Messages: No

Diffie-Hellman Key Exchange Protocol

- Public-key algorithm **based** on modular exponentiation
- **Used** for sharing keys in symmetric cryptography
- Based on the hardness of solving discrete logarithm
  - Given $X = g^x \bmod p$; difficult to recover x

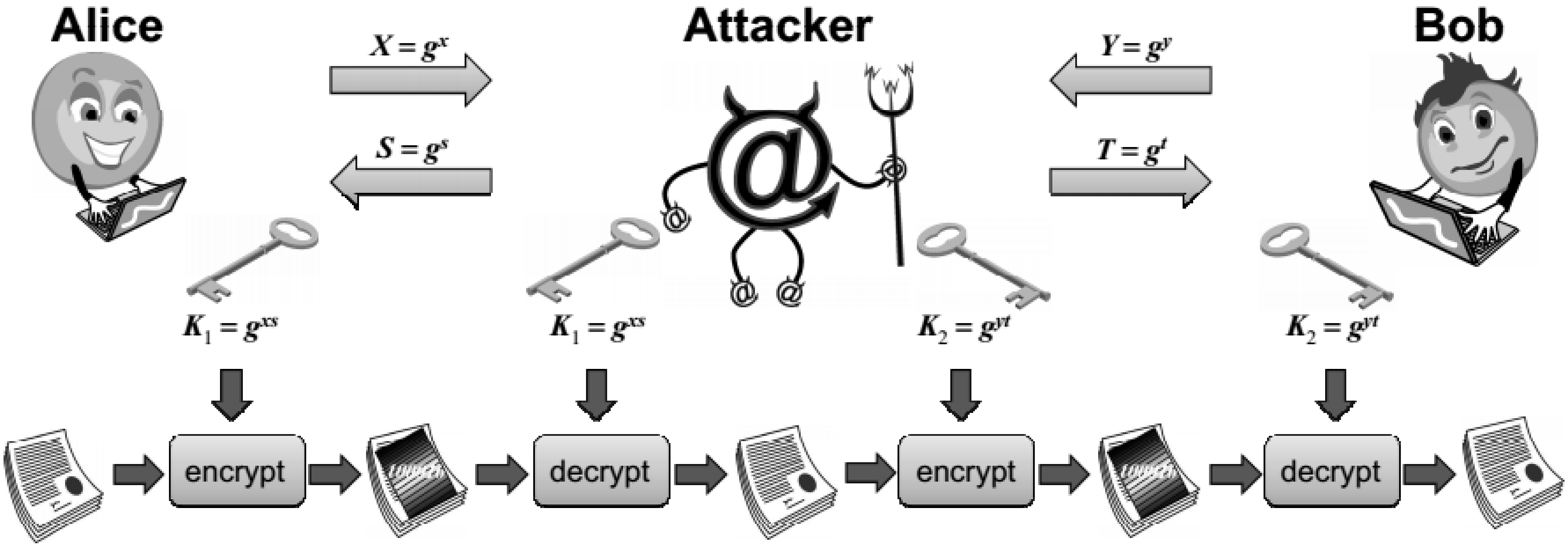
Operation

- Prime p ; g (=primitive root modulo p)
  - Both p and g are public (can be used by all users in the system)
- A → B : X = g^x mod p ; B → A: Y = g^y mod p
  - x,y: random positive #
  - X,Y not secret but x is A's secret, y is B's secret
- A calculates $K_1 = Y^x \, mod \, p$
- B calculates $K_2 = X^y \, mod \, p$
- Shared Secret Key K = g^{xy} mod p = K1 = K2

Weaknesses

- p has to be large
- x and y: random number generator values cannot be predicted
- Does not provide authentication; subject to MITM (man-in-the-middle) attack

Man-in-the-Middle Attack



No key exchange protocol exists if attacker can modify messages

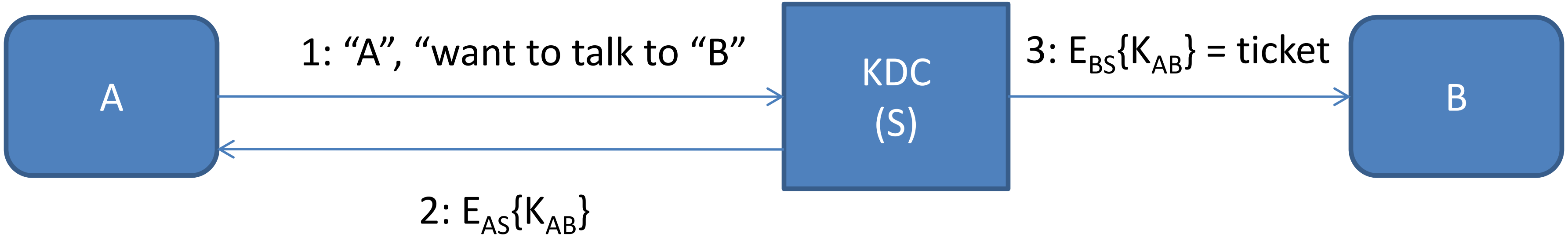
Distribution of Symmetric Keys

Challenges:

- N nodes implies N (N-1)/2 symmetric keys
  - N is large → Large number of keys
- Add new node, need to generate N new keys
- How to secretly get these keys into the nodes?
- Offline mode: meet secretly face-to-face and configure
  - Not practical in most settings
- Public key **distribution** preferred to symmetric key

Key Distribution Center (KDC)

- A trusted entity that shares a key with every node
  - Number of keys: N
  - Key setup out of band
  - Easy node addition; easy key revocation



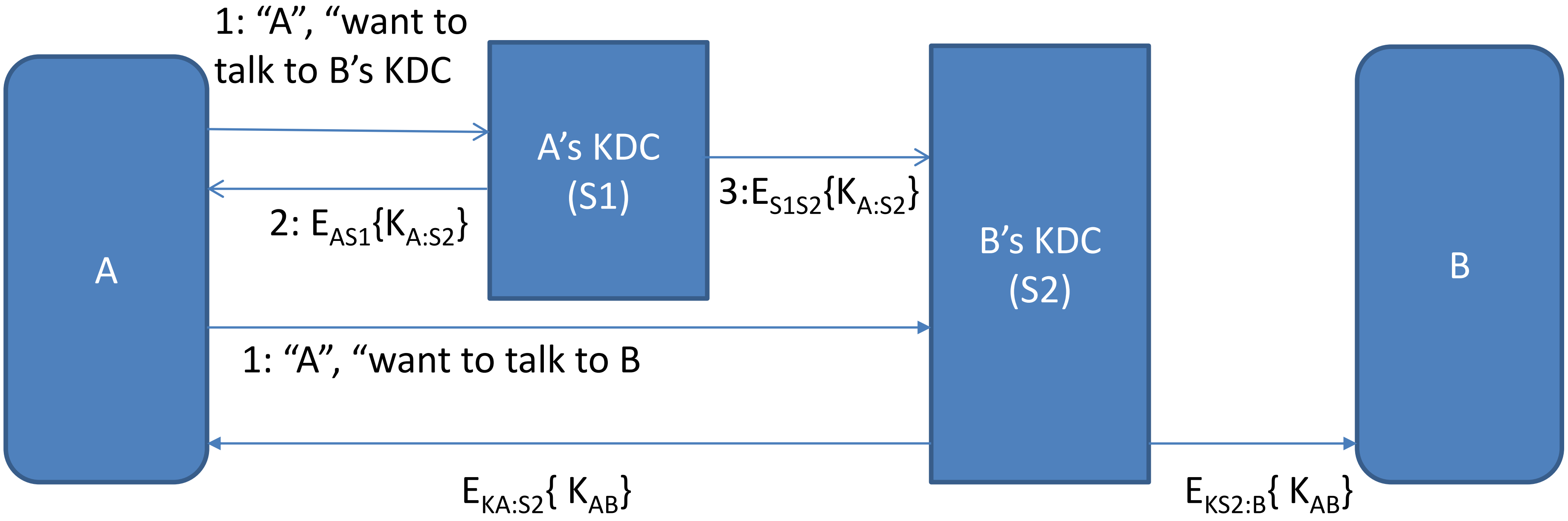
(a)

Ticket allows A to communicate with B

Disadvantages

- KDC can impersonate anyone
- Single point of failure
- Performance bottleneck

Multiple KDCs



Hierarchy (Tree)

- Mesh is impractical
- Tree (maybe with a few additional links)
- A can negotiate a chain of KDC’s to get to B’s KDC
  - B given choice to choose the chain