Key Management

Dr. B C Dhara
Department of Information Technology
Jadavpur University

Objectives

- Explain the need for a key-distribution center (KDC)
- Show how a KDC can create a session key
- Show how two parties can use a symmetric-key agreement protocol to create a session key
- Describe Kerberos as a KDC and an authentication protocol
- Explain the need for certification authorities for public keys
- Introduce the idea of Public-Key Infrastructure (PKI) and its duties

Introduction

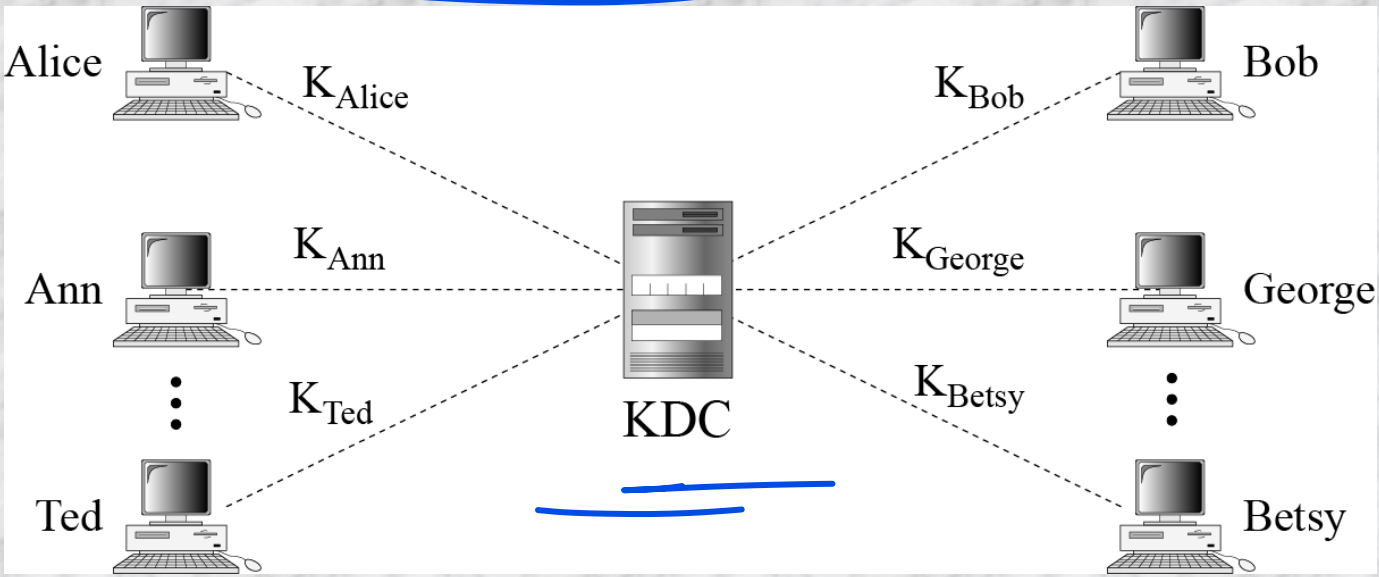
- We have studied symmetric-key and asymmetric-key cryptosystem
  - How the secret keys in symmetric-key cryptography, public keys in asymmetric-key cryptography are distributed and maintained

SYMMETRIC-KEY DISTRIBUTION

- *Symmetric-key cryptography is more efficient than asymmetric-key cryptography for enciphering large messages*
- *Symmetric-key cryptography, however, needs a shared secret key between two parties*
- *The distribution of keys is another problem*

Key-Distribution Center: KDC

- A practical solution to distribute the keys is the use of a trusted third party, referred as **key-distribution centre** (KDC)

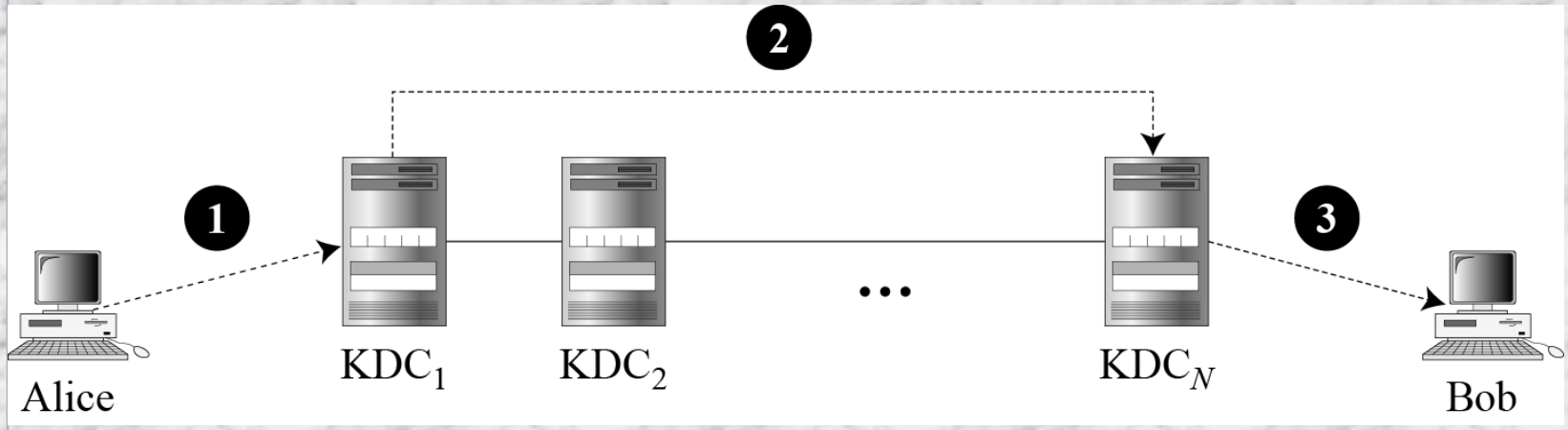


How session key is created?

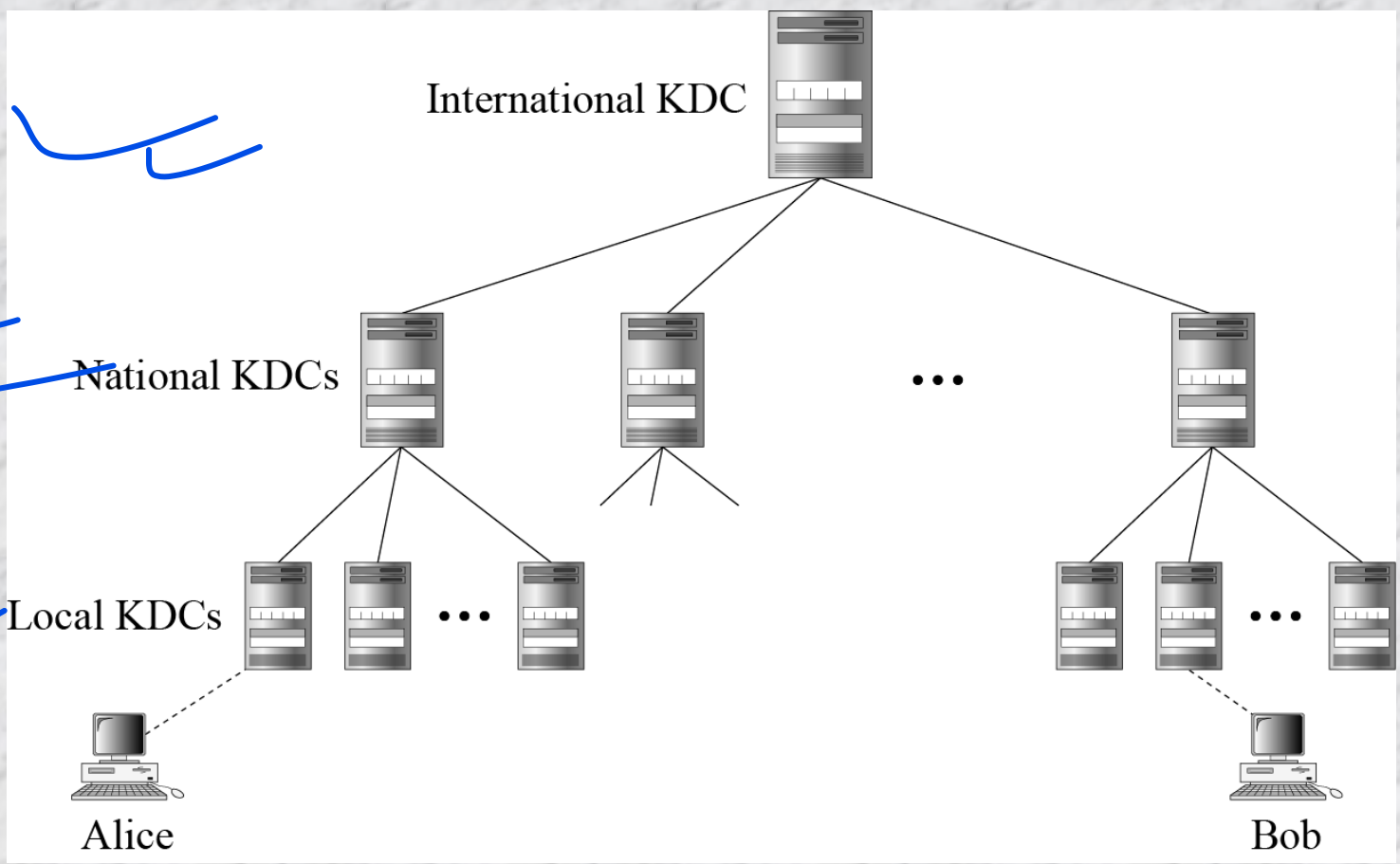
- A secret key is established between KDC and each member
- How two parties can send a confidential message between them?
  - Sender (X) sends a request to the KDC for a session key between him and Y
  - KDC informs Y about the X's request
  - If Y agrees, a session key is created between X and Y
  - This session is used to authenticate X and Y to the KDC and prevent third party from impersonating

Flat Multiple KDCs

- When number of people increases, a bottleneck situation may arises
  - We need multiple KDCs
  - Divide the world into domains



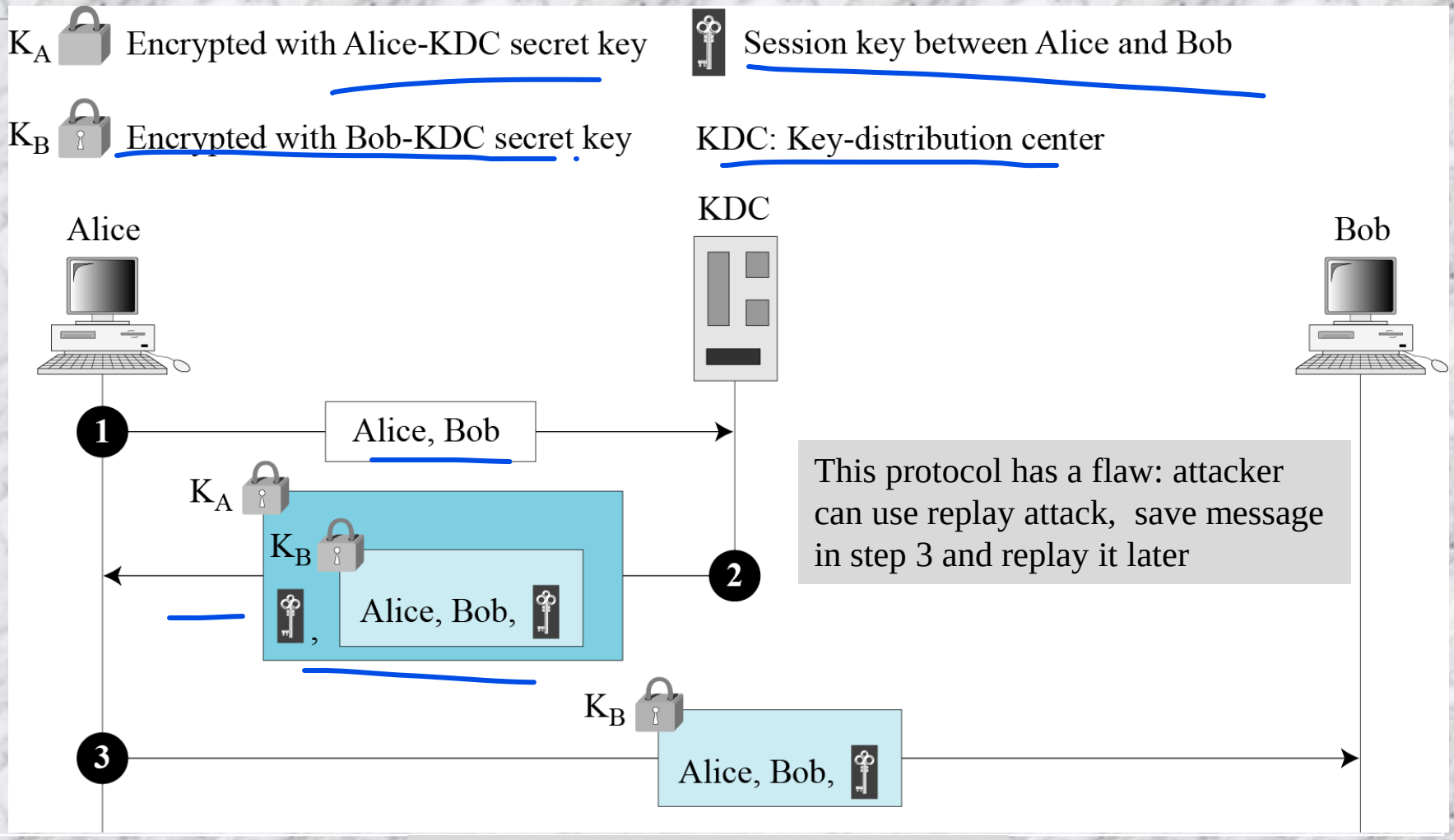
Hierarchical Multiple KDCs



Session Keys

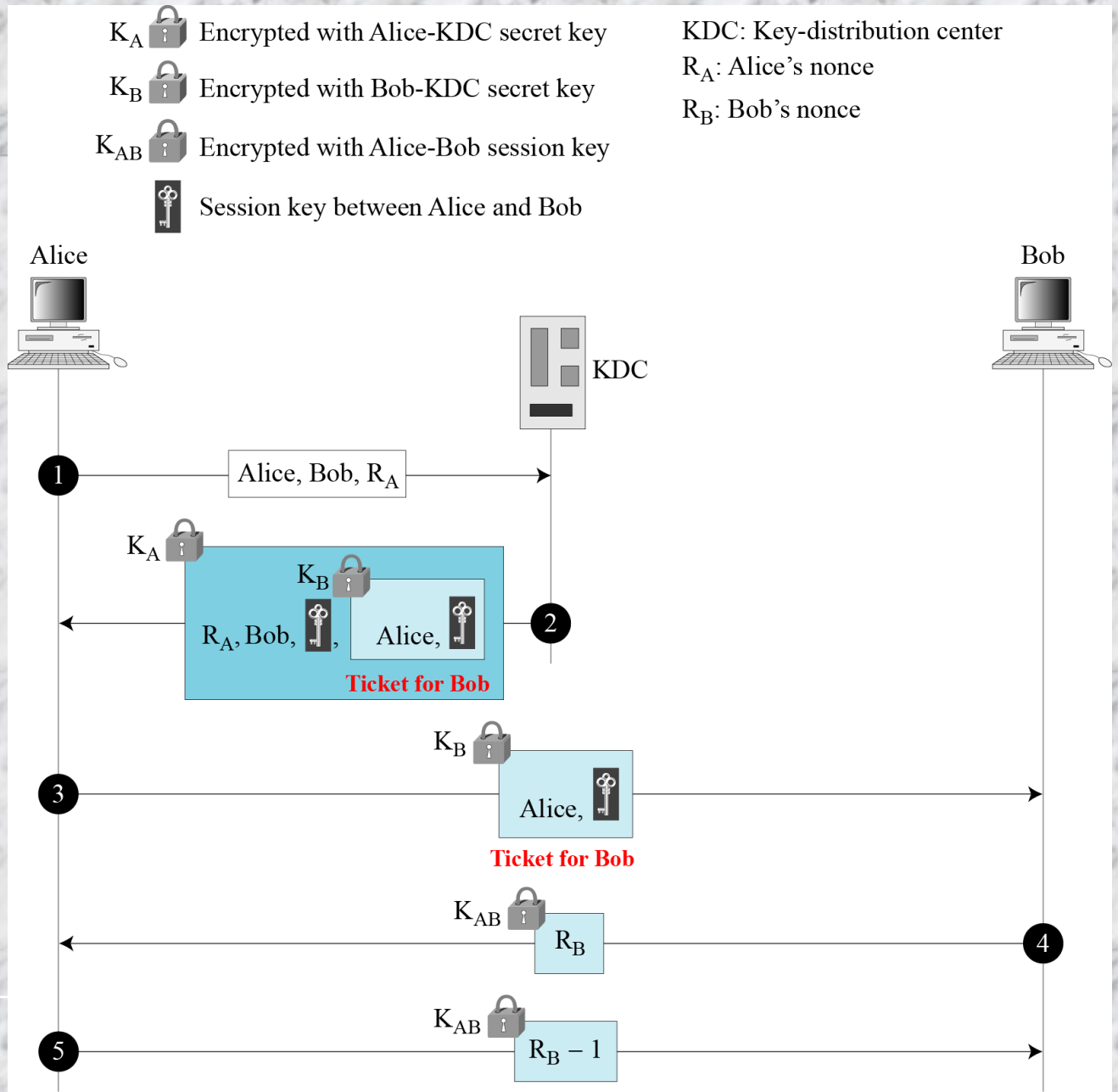
- *A KDC creates a secret key for each member*
- *This secret key can be used only between the member and the KDC, not between two members*
  - *A session key is created , using their secret keys (between member and KDC)*
  - *Members are authenticated by the secret key*
  - *After communication is terminated, the session key is no longer useful*
    - *A session symmetric key between two parties is used only once*

A Simple Protocol Using a KDC



First approach using KDC

Needham-Schroeder Protocol



KERBEROS

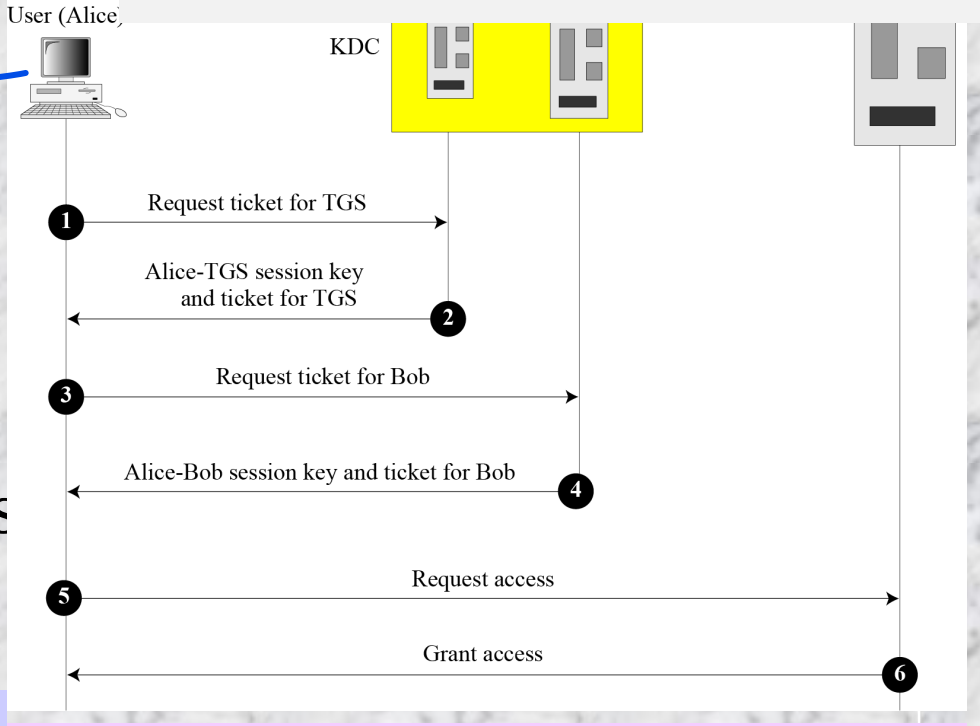
- *Kerberos is an authentication protocol, and at the same time a KDC, that has become very popular*
- *Several systems, including Windows 2000, use Kerberos. Originally designed at MIT, it has gone through several versions*

Kerberos (contd..

- Three types of servers:
  - Authentication server (AS)
  - Ticket-granting server (TGS)
  - Data (or real) server, to provide services to others

*Authentication Server (AS)" each user registers with AS and granted **user id and password***

In response of request from user: issue session key between user-TGS and ticket for TGS , to access TGS



Ticket-Granting Server (TGS): issues a ticket for the real server (Bob).

Real Server: provides services for the user

SYMMETRIC-KEY AGREEMENT

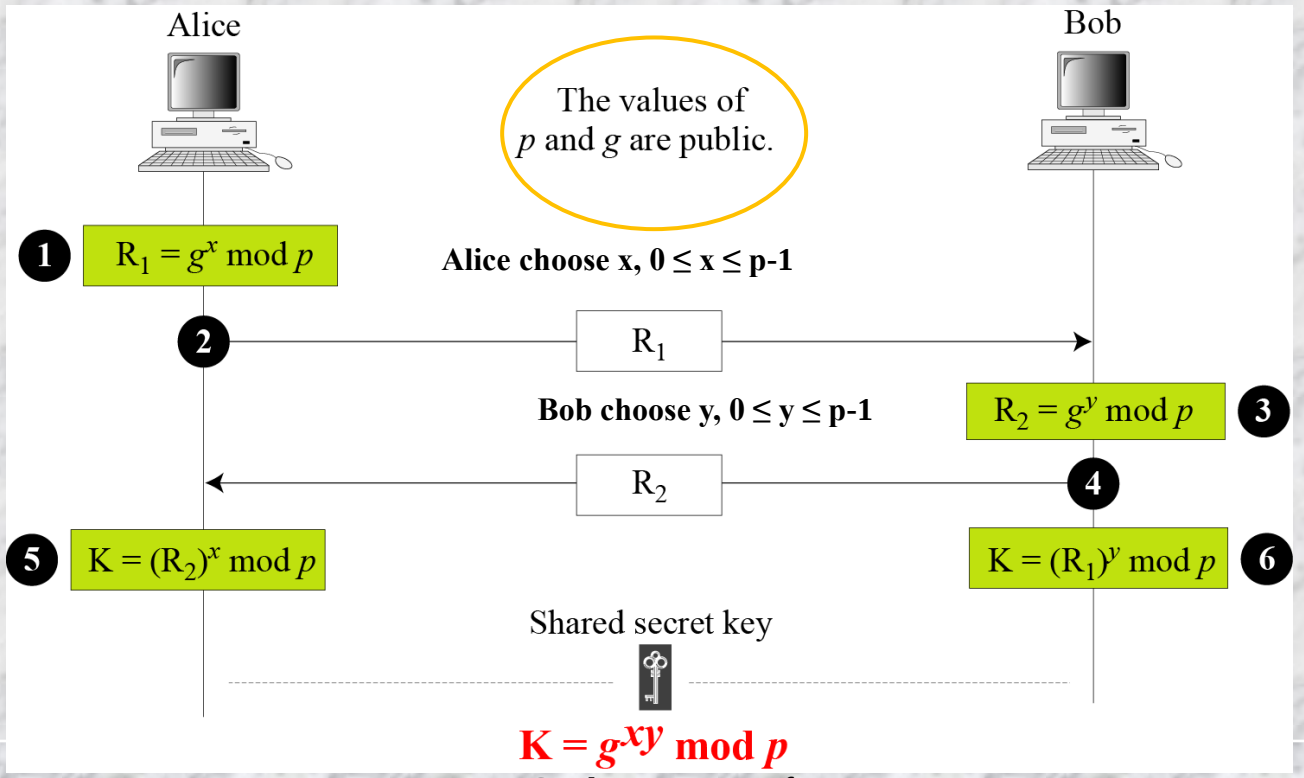
- *When two parties create a session key between themselves without using a KDC. This method of session-key creation is referred to as the symmetric-key agreement*

Diffie-Hellman Key Agreement

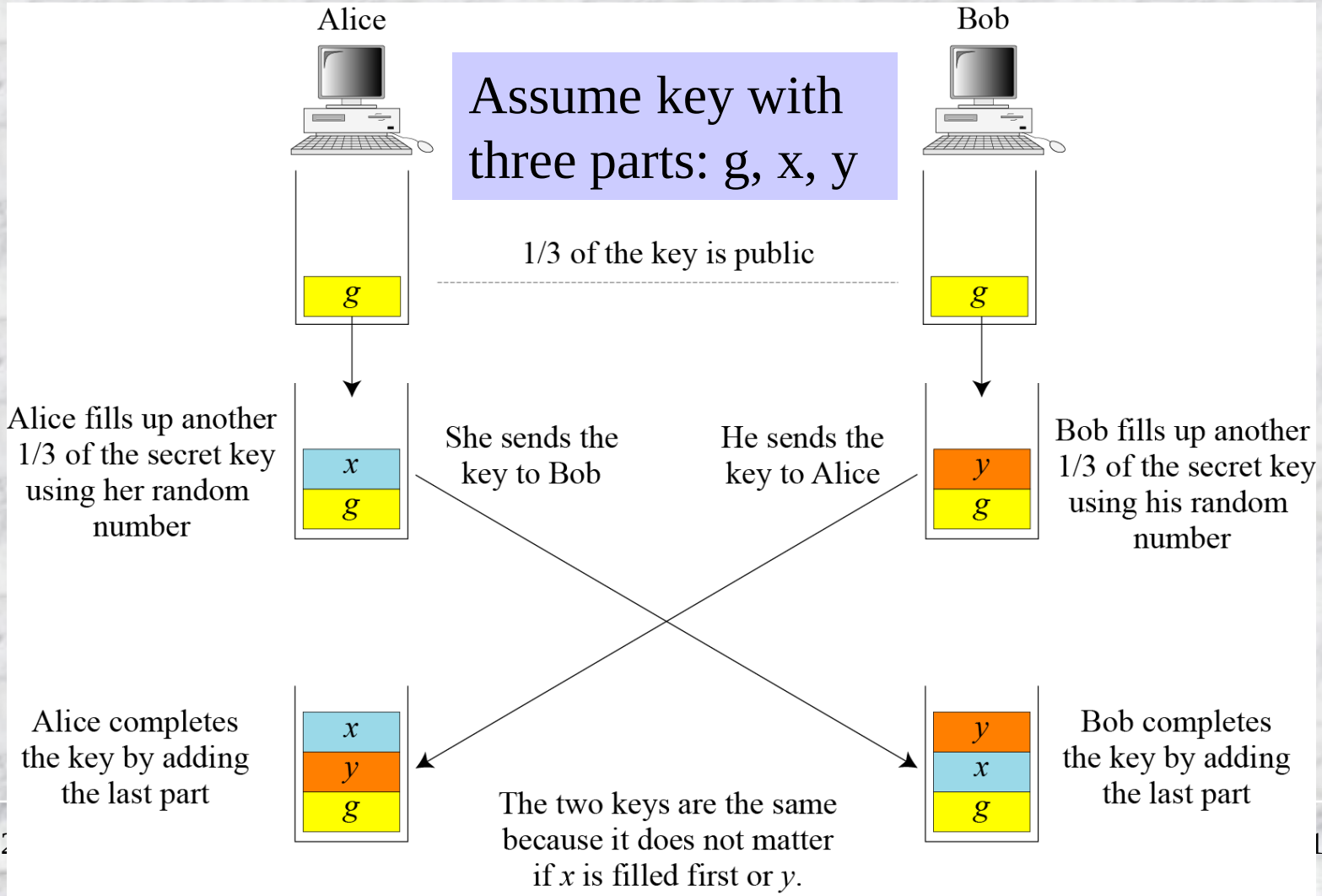
Station-to-Station Key Agreement

Diffie-Hellman Key Agreement

Two parties choose two number p and g: p is large prime number (with 300 digits), g is a generator of the group $(Z_p^*, \times)$



Analysis of Diffie-Hellman



Security of Diffie-Hellman

- *This key exchange is susceptible to two attacks:*
  - *Discrete logarithm attack*
  - *Man-in-the-middle attack*

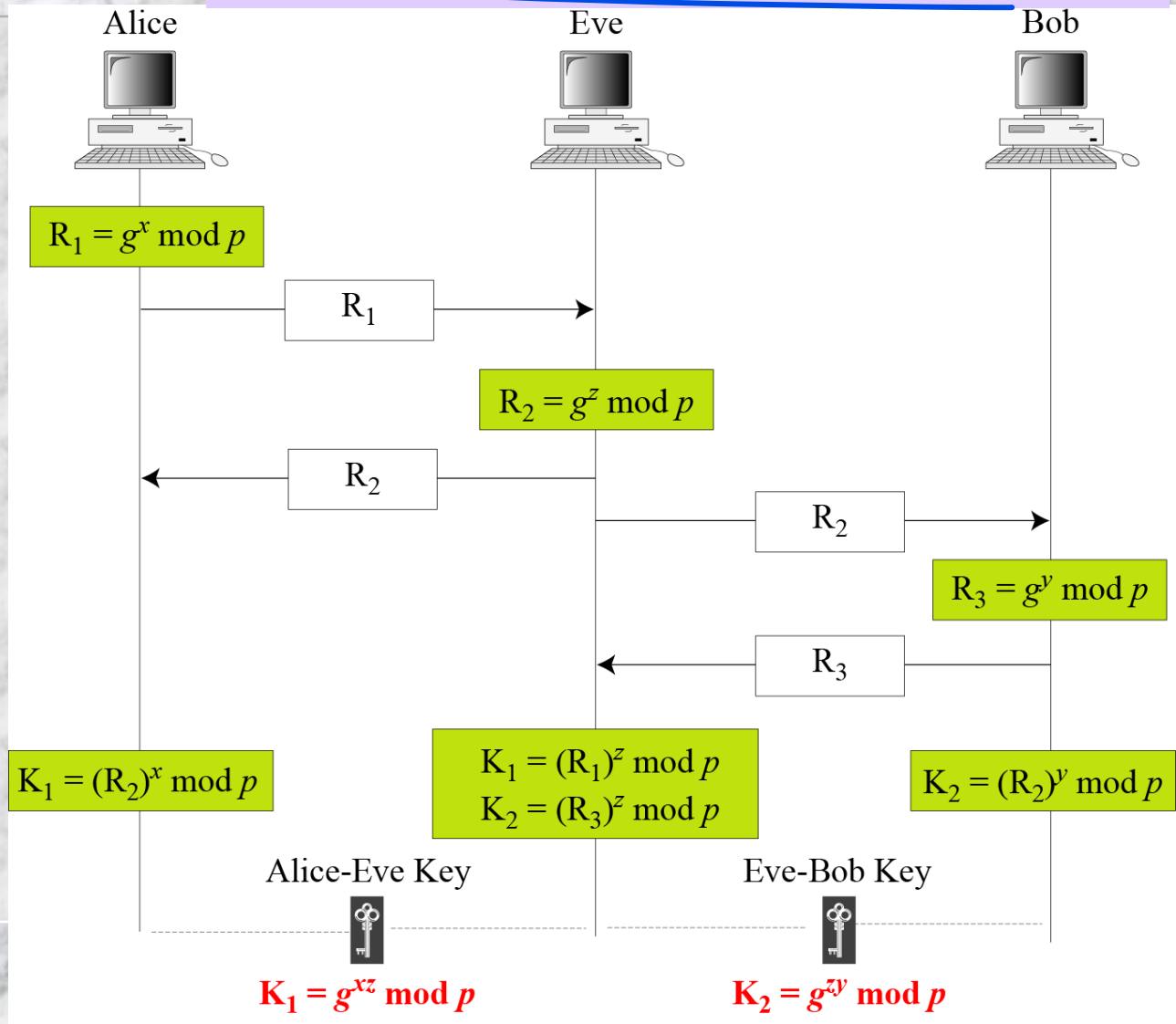
Discrete Logarithm Attack

- A third party can intercepts: R_1 and R_2
  - If can find x from $R_1=g^x \bmod p$ or
  - y from $R_2 = g^y \bmod p$
  - The key $K= g^{xy} \bmod p$ is no more secure
- To make Diffie-Hellman secure from discrete logarithm attack:

The prime p must be very large (more than 300 decimal digits)
Generator must be chosen from the group $(Z_p^*, \times)$
Destroy x and y after the symmetric key is calculated
Different x and y must be used at different time instance

Man-in-the-middle Attack

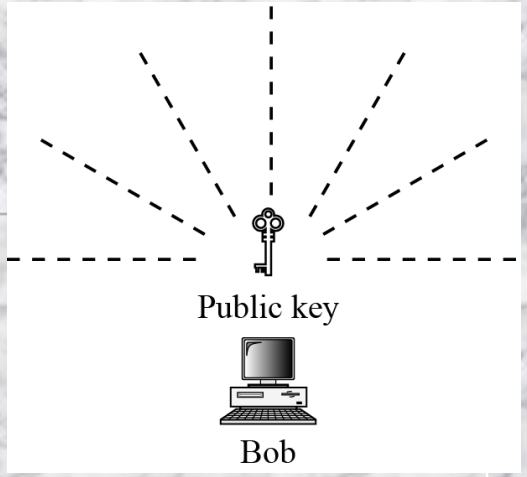
Attacker does not have to find x and y
Attacker creates two keys:
one between himself and Alice and
other one between himself and Bob



PUBLIC-KEY DISTRIBUTION

- In asymmetric-key cryptography, people do not need to know a symmetric shared key; everyone shields a private key and advertises a public key.
- How the public key can be distributed?
  - Public Announcement
  - Trusted Center
  - Controlled Trusted Center
  - Certification Authority
  - X.509
  - Public-Key Infrastructures (PKI)

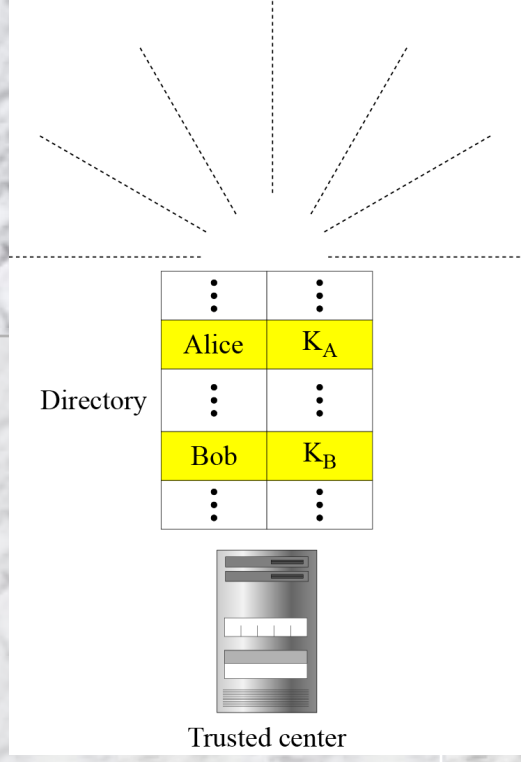
Public Announcement



- Announce public keys publicly
  - Put public key on website
  - Announce in a local/national newspaper
  - This approach is not secure, it is subject to forgery
    - Eve could make such a public announcement (before step from Bob, damage could be done)
    - If Alice directly requests Bob
      - Eve can intercept Bob's response and substitute her own public key

Trusted Center

- There is a directory of public keys
  - Which is dynamically updated
- Each user has to register in the center
  - Gets an identity
- Each user fix a private key and public key
  - Keep the private key and public key is stored into the directory
- The directory can be publicly advertise by the trusted center



Controlled Trusted Center

- Higher level of security can be achieved if additional controls added on the distribution of the public key
- Announcement of public-key includes a timestamp and a signature of authority
  - Prevents interception and modification of the response