哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

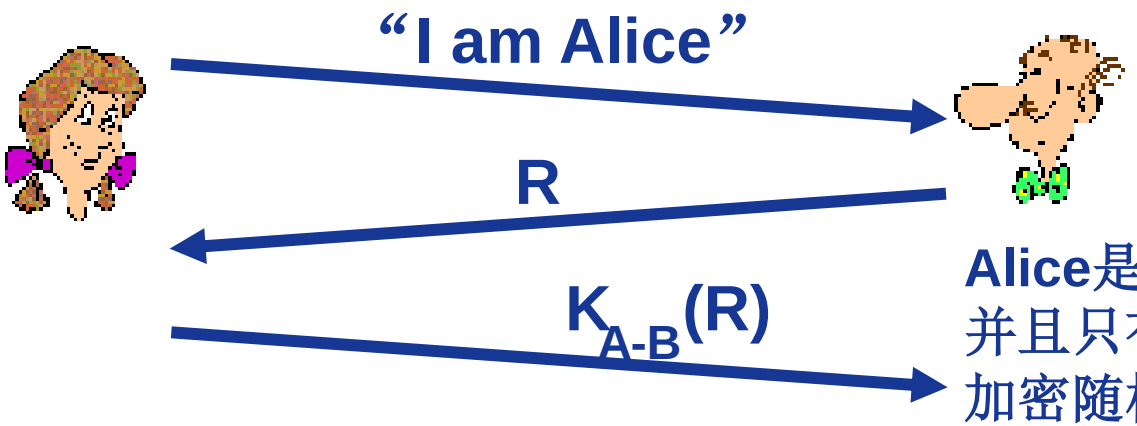
密钥分发中心(KDC)

回顾身份认证协议：ap4.0

目标：避免回放攻击

一次性随机数(nonce)：一个生命期内只用一次的数R

ap4.0：为了证明是“真实的”Alice，Bob向Alice发送一个随机数R，Alice必须返回R，并利用共享密钥进行加密



如何共享对称密钥？

对称密钥问题？

对称密钥问题:

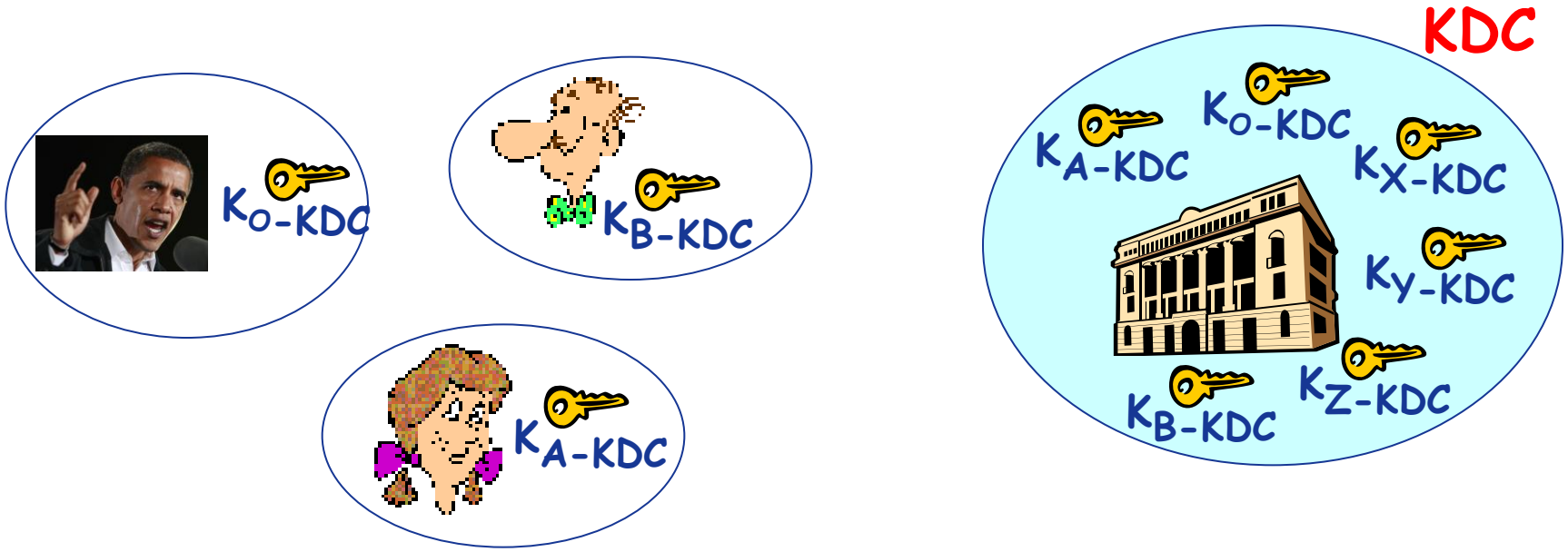
- 两个实体在网上如何建立共享秘密密钥？

解决方案:

- 可信任的密钥分发中心(Key Distribution Center-KDC)作为实体间的中介(intermediary)

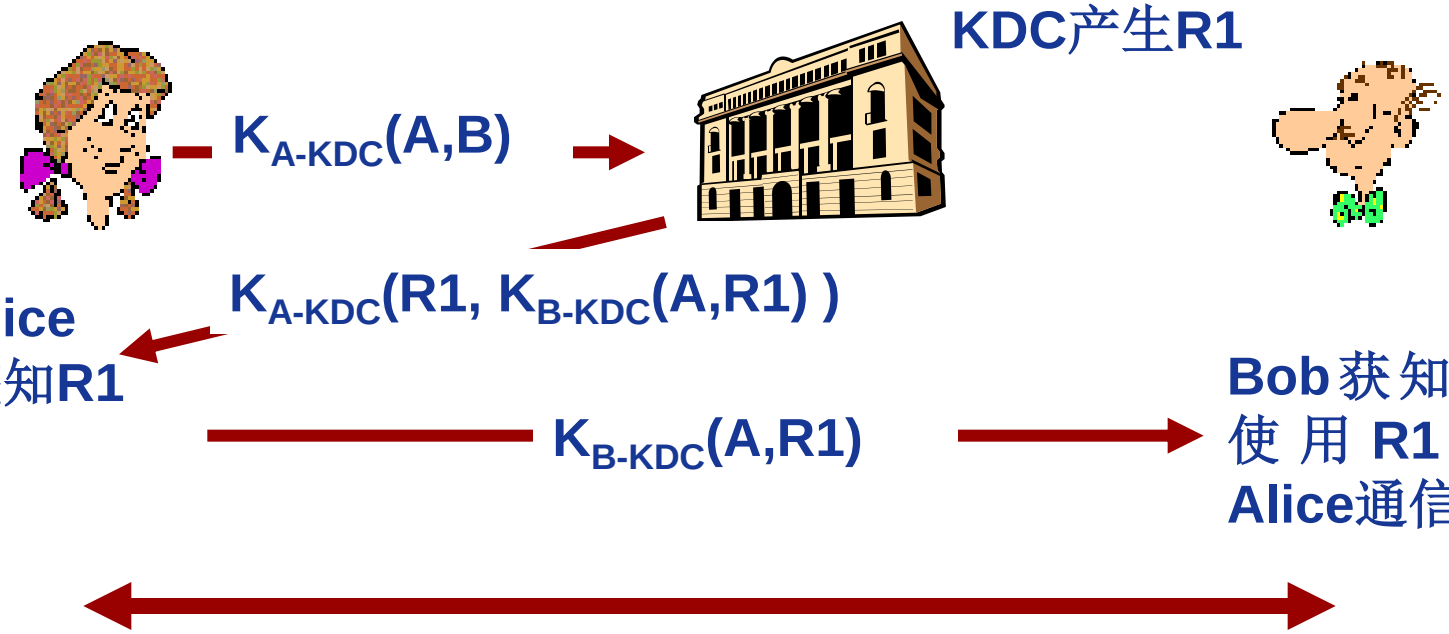
密钥分发中心(KDC)

- Alice与Bob需要共享对称密钥.
- KDC：一个服务器
  - 每个注册用户(很多用户)共享其与KDC的秘密密钥
- Alice和Bob只知道自己与KDC之间的对称密钥，用于分别与KDC进行秘密通信.



密钥分发中心(KDC)

Q: KDC如何支持Bob和Alice确定用于彼此通信的共享对称密钥呢？



哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！