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

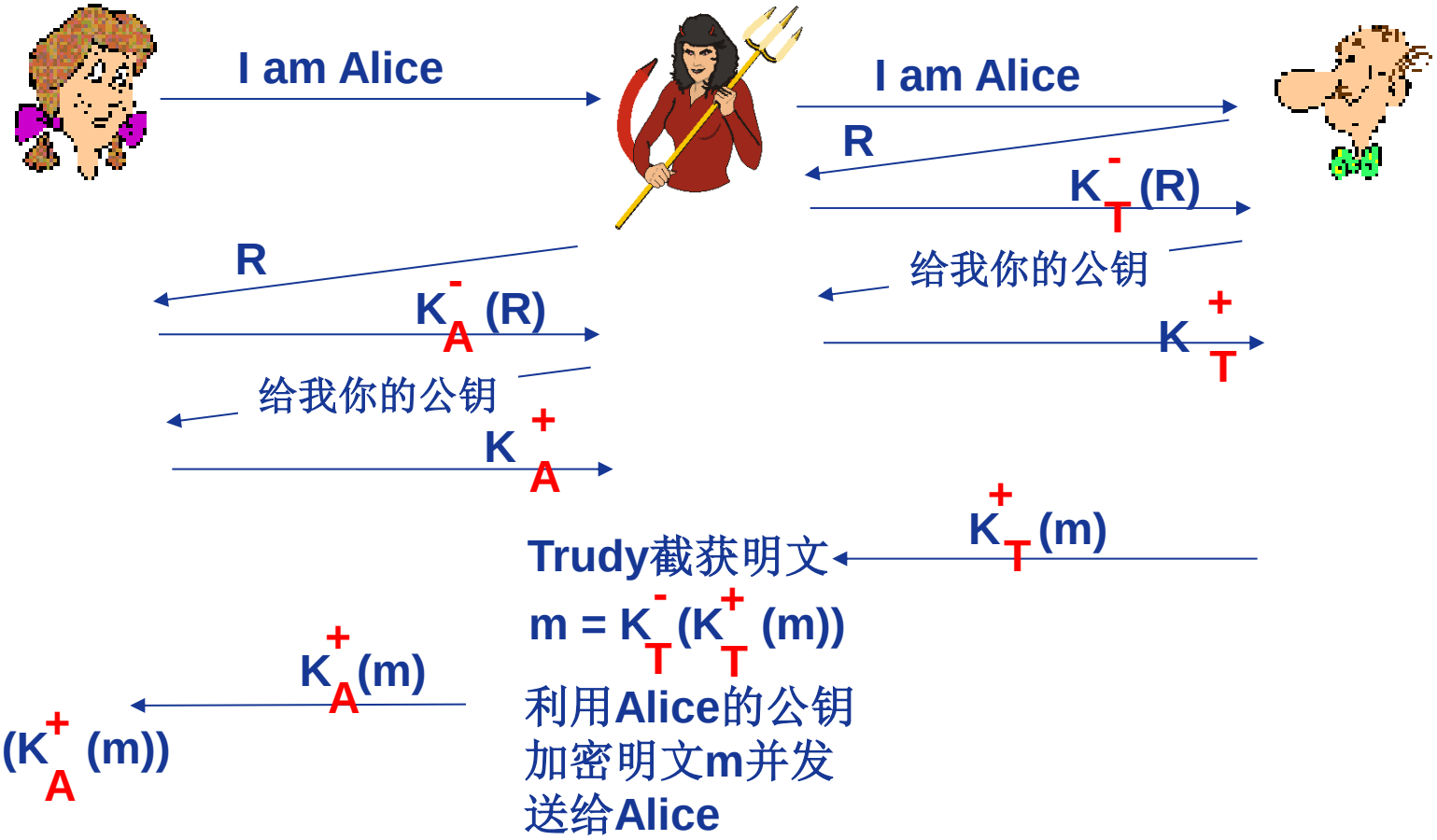
主讲人：李全龙

本讲主题

认证中心(CA)

回顾身份认证协议：ap5.0

中间人攻击(man in the middle attack): Trudy向Bob假扮Alice，向Alice假扮Bob。



比萨恶作剧

- Trudy针对Bob实施“比萨恶作剧”
  - Trudy创建邮件订单:
    Dear Pizza Store, Please deliver to me four pepperoni pizzas. Thank you, Bob
  - Trudy利用她的私钥签名订单
  - Trudy向比萨店发送订单
  - Trudy向比萨店发送她的公钥，但她声称这是Bob的公钥
  - 比萨店核实签名；然后向Bob递送4个腊肠比萨
  - Bob根本就不喜欢腊肠

公钥问题？

公钥问题:

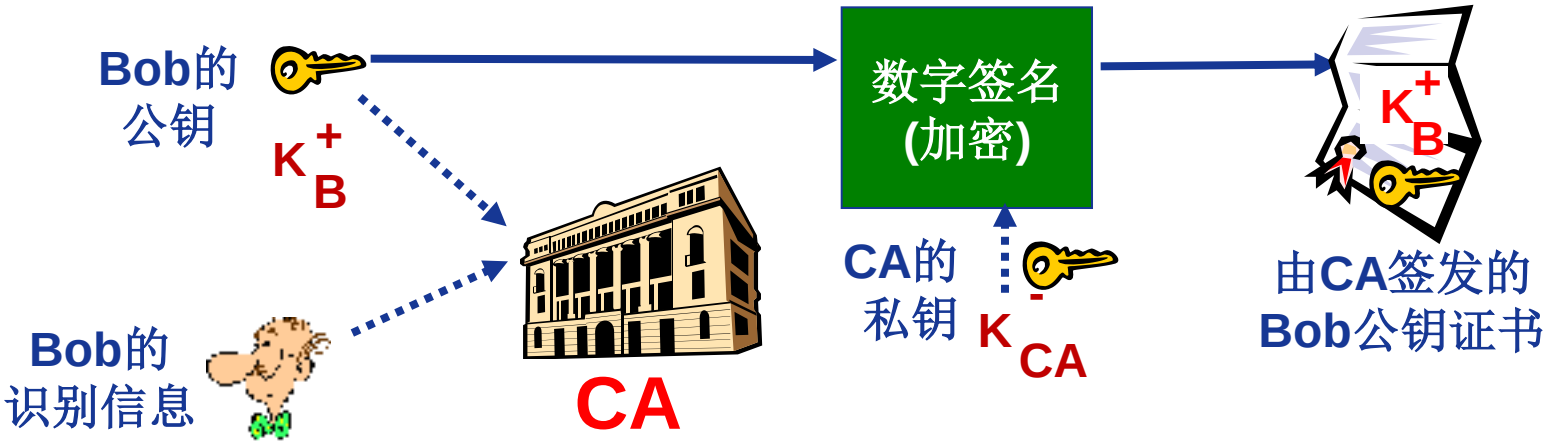
- 当Alice获得了Bob的公钥 (通过web网站、e-mail、磁盘等)，她怎么确认这真的是Bob的公钥而不是Trudy的?

解决方案:

- 可信任的认证中心(Certification Authority-CA)

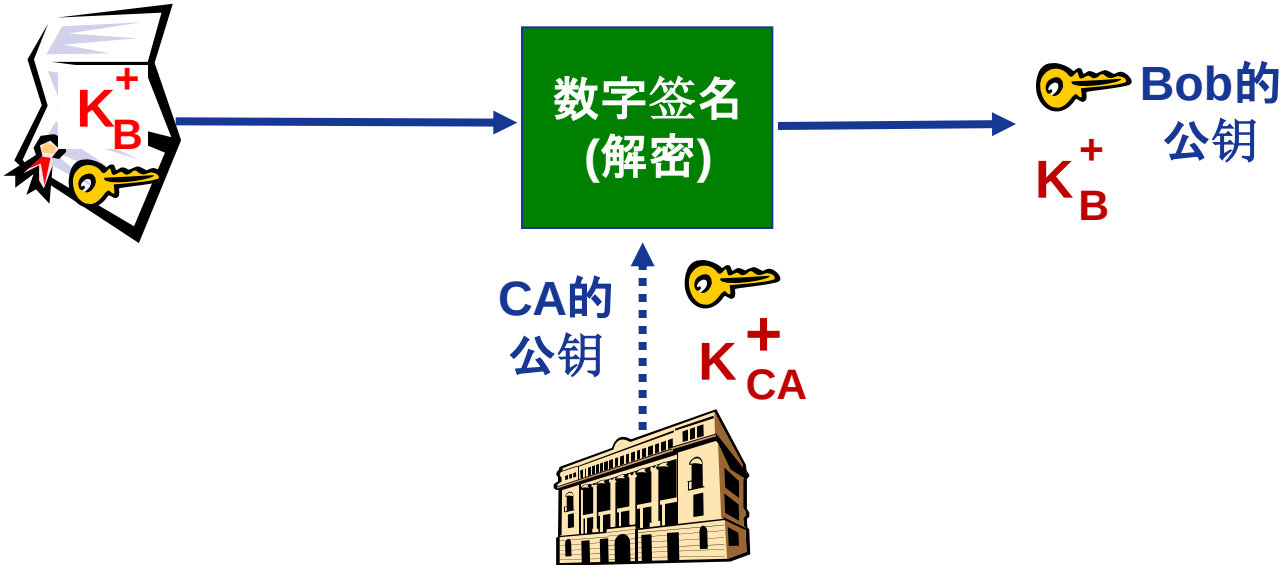
认证中心

- 认证中心(CA): 实现特定实体E与其公钥的绑定
- 每个E(如人、路由器等)在CA上注册其公钥.
  - E向CA提供“身份证明”.
  - CA创建绑定E及其公钥的证书(certificate).
  - 证书包含由CA签名的E的公钥 – CA声明：“这是E的公钥”



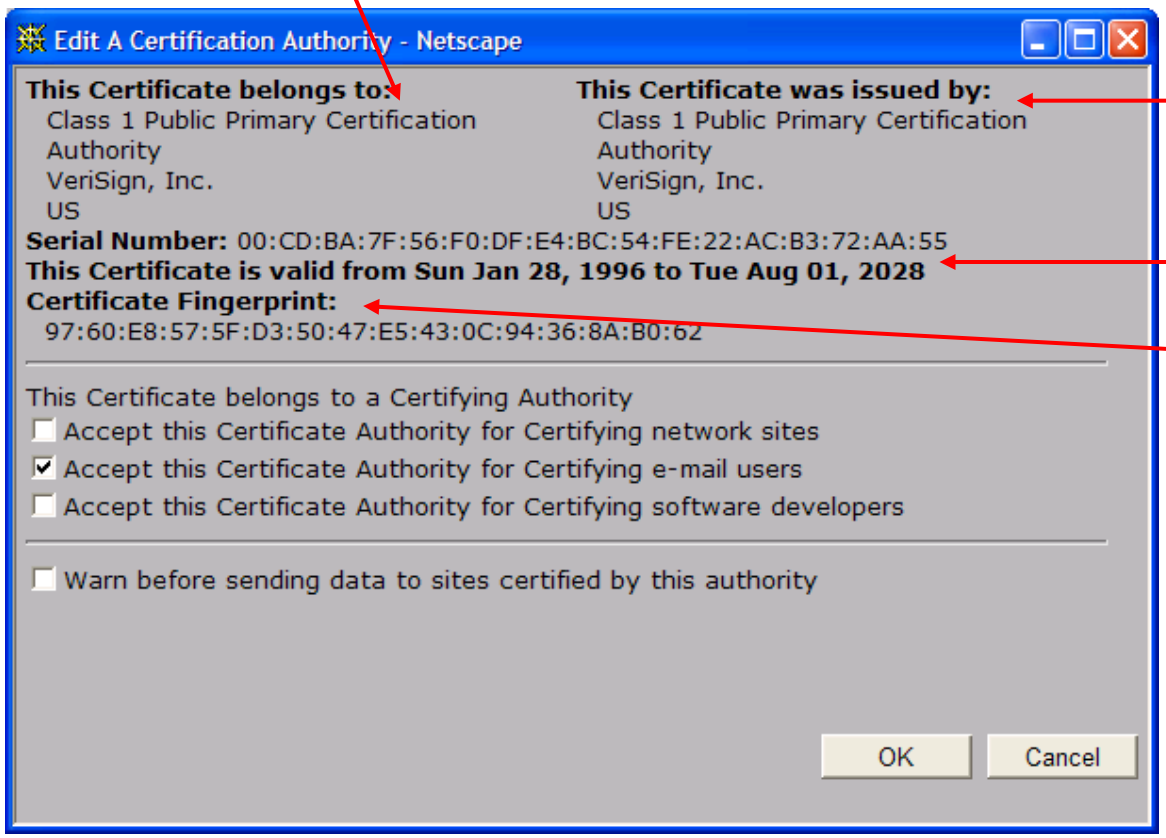
认证中心

- 当Alice想要Bob的公钥时:
  - 首先或取Bob的公钥证书(从Bob或者其他地方).
  - 应用CA的公钥，解密证书中签名的公钥，获得Bob公钥



公钥证书主要内容

- 序列号(唯一发行号)
- 证书持有者信息，包括算法和密钥值(未显示)



- 证书发行者信息
- 有效期
- 发行者数字签名

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！