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

安全电子邮件基本原理

电子邮件安全威胁

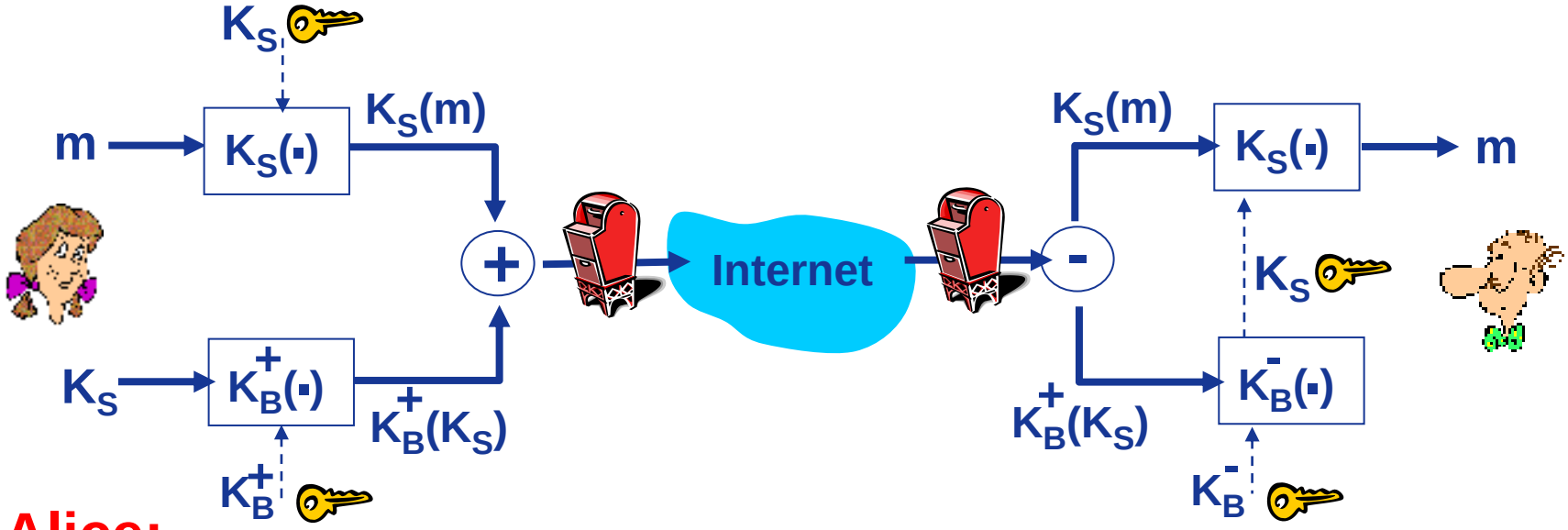
- 垃圾邮件
  - 增加网络负荷，占用服务器空间
- 诈骗邮件
  - 能迅速让大量受害者上当
- 邮件炸弹
  - 短时间内向同一邮箱发送大量电子邮件
- 通过电子邮件/附件传播网络蠕虫/病毒
- 电子邮件欺骗、钓鱼式攻击

电子邮件安全需求

- 机密性
  - 只有真正的接收方才能阅读邮件
- 完整性
  - 电子邮件在传输过程中不被修改
- 身份认证性
  - 电子邮件的发送者不被假冒
- 抗抵赖性
  - 发信人无法否认发过电子邮件

安全电子邮件基本原理

- 邮件具有单向性和非实时性
  - 不能通过建立隧道来保证安全，只能对邮件本身加密
- Alice期望向Bob发送机密邮件m



Alice:

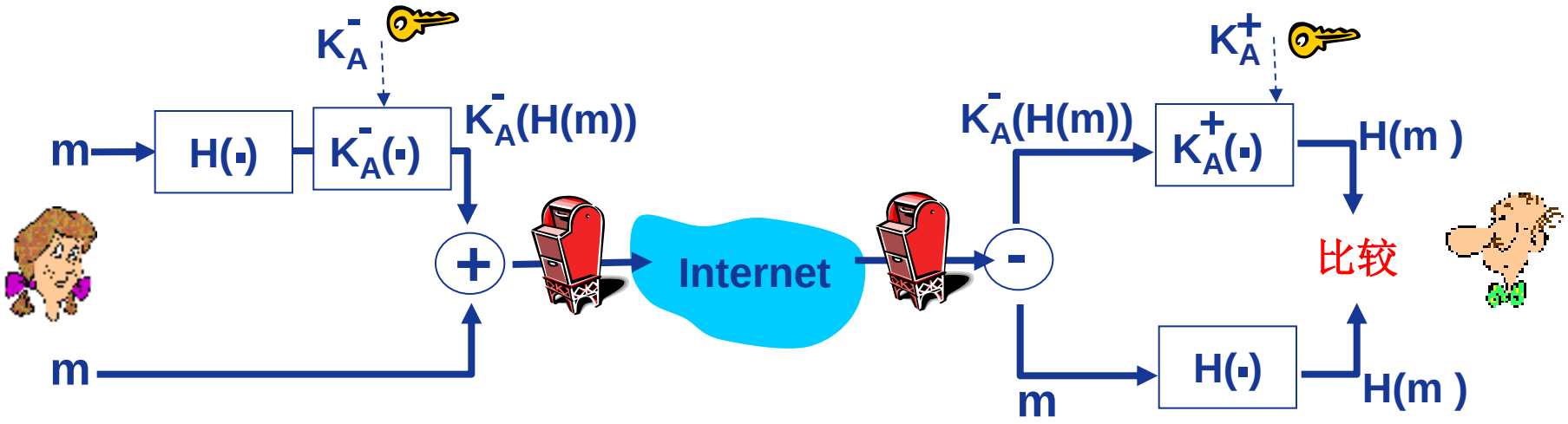
- 生成随机对称密钥, K_S
- 利用K_S加密报文 (为了效率)
- 同时，利用Bob的公钥加密K_S
- 将$K_S(m)$和$K_B^+(K_S)$发送给Bob

Bob:

- 利用他的私钥解密$K_B^+(K_S)$，获得K_S
- 利用K_S解密$K_S(m)$恢复m

安全电子邮件基本原理

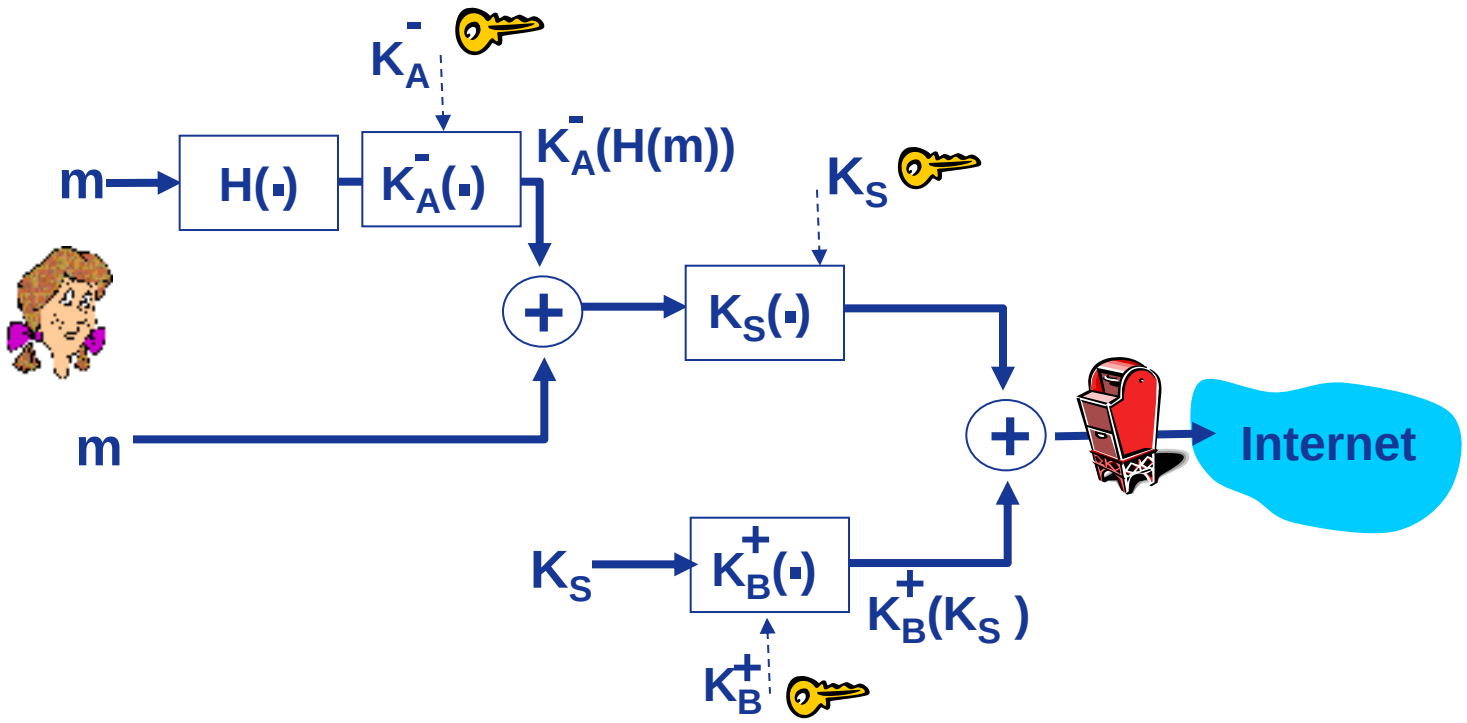
- Alice期望提供发送者认证与报文完整性



- Alice对报文进行数字签名
- 发送报文（明文）和数字签名

安全电子邮件基本原理

- Alice期望提供保密、发送者认证与报文完整性



Alice使用3个密钥: 她自己的私钥、Bob的公钥和新生成的对称密钥

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！