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

数字签名

数字签名

Q:如何解决下列与报文完整性相关的问题？

- 否认：发送方不承认自己发送过某一报文
- 伪造：接收方自己伪造一份报文，并声称来自发送方
- 冒充：某个用户冒充另一个用户接收或发送报文
- 篡改：接收方对收到的信息进行篡改

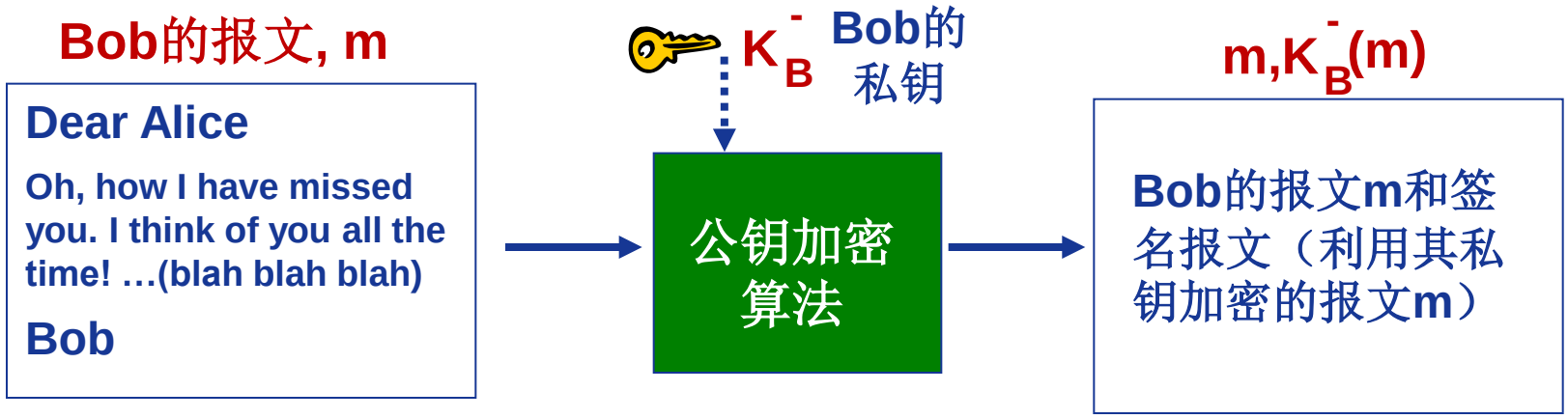
A:数字签名(Digital signatures)！

- 数字签名技术是实现安全电子交易的核心技术之一
- 可验证性(verifiable)
- 不可伪造性(unforgeable)
- 不可抵赖性(non-repudiation)

数字签名

对报文m的简单数字签名:

- 报文加密技术是数字签名的基础
- Bob通过利用其私钥 K_B^- 对m进行加密，创建签名报文，$K_B^-(m)$



数字签名

- 假设Alice收到报文m以及签名$K_B^-(m)$
- Alice利用Bob的公钥K_B^+ 解密$K_B^-(m)$，并检验$K_B^+(K_B^-(m)) = m$ 来证实报文m是Bob签名的。
- 如果$K_B^+(K_B^-(m)) = m$ 成立，则签名m的一定是Bob的私钥
- 于是：

Alice可以证实:

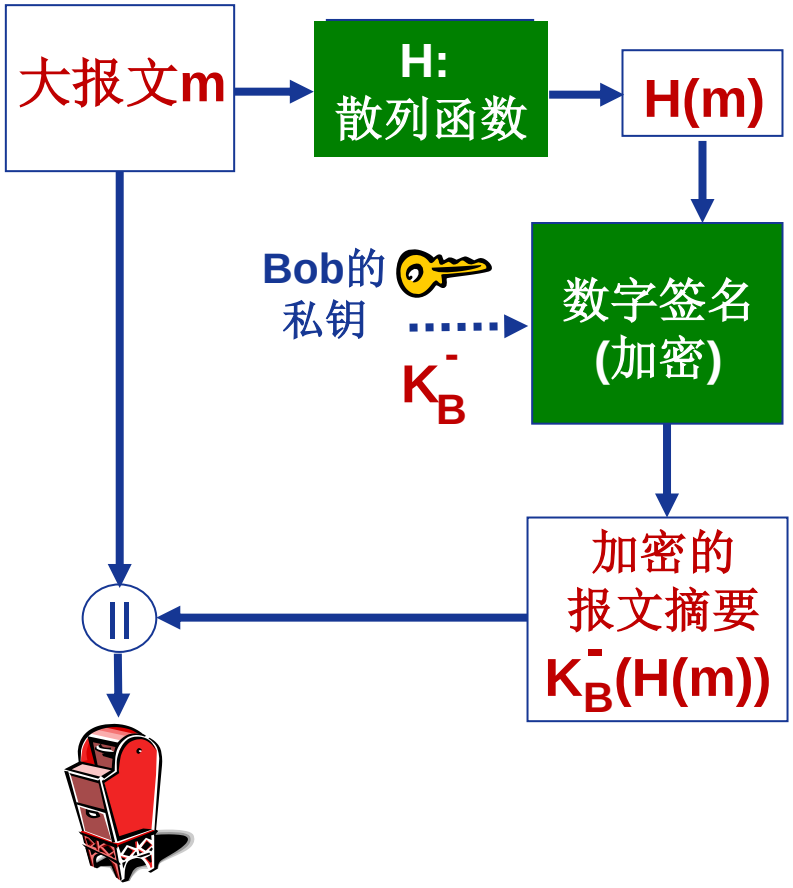
- ✓ Bob签名了m
- ✓ 没有其他人签名m的可能
- ✓ Bob签名的是m而不是其他报文m'

不可抵赖(non-repudiation):

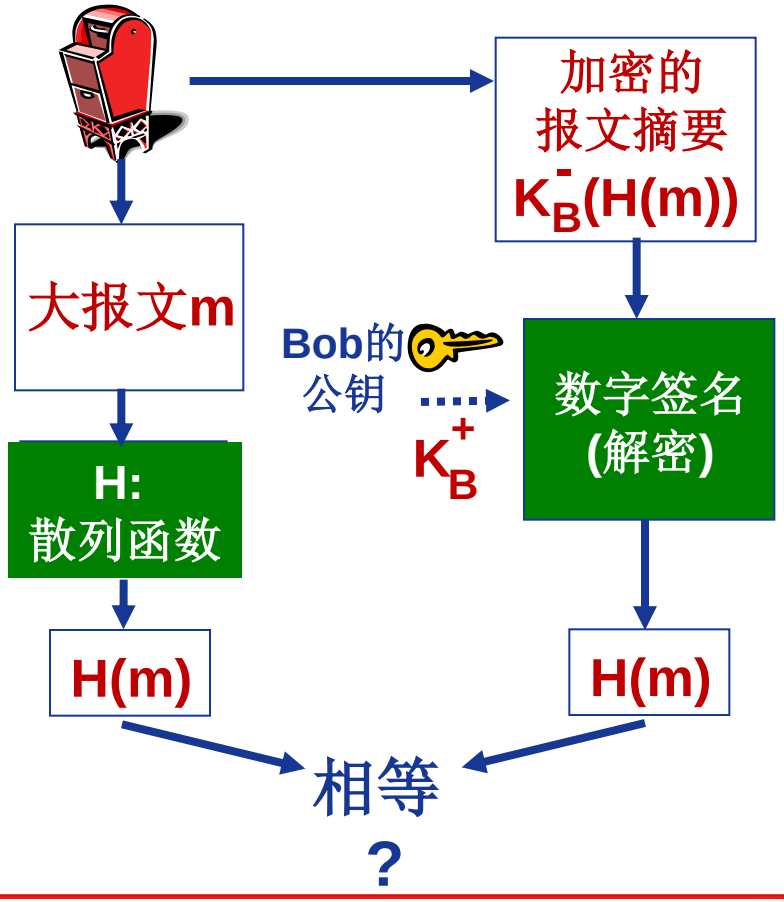
- ✓ Alice可以持有m和签名$K_B^-(m)$，必要时可以提交给法院证明是Bob签名的m

签名报文摘要

Bob发送数字签名的报文:



Alice核实签名以及数字签名报文的完整性:



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！