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

报文完整性

报文完整性？

- 报文/消息完整性(message integrity)，也称为报文/消息认证（或报文鉴别），目标：
  - 证明报文确实来自声称的发送方
  - 验证报文在传输过程中没有被篡改
  - 预防报文的时间、顺序被篡改
  - 预防报文持有期被修改
  - 预防抵赖
    - 发送方否认
    - 接收方否认

密码散列函数

密码散列函数(Cryptographic Hash Function)：H(m)

- 散列算法公开
- H(m)能够快速计算
- 对任意长度报文进行多对一映射，均产生定长输出
- 对于任意报文无法预知其散列值
- 不同报文不能产生相同的散列值
- 单向性：无法根据散列值倒推出报文
  - 对于给定散列值h，无法计算找到满足h = H(m)的报文m
- 抗弱碰撞性(Weak Collision Resistence-WCR)
  - 对于给定报文x，计算上不可能找到y且y≠x，使得H(x)=H(y)
- 抗强碰撞性(Strong Collision Resistence-SCR)
  - 在计算上，不可能找到任意两个不同报文x和y(x≠y)，使得H(x)=H(y)

Internet校验和是优秀的密码散列函数吗？

Internet校验和(checksum)具备散列函数的某些属性：

- ✓ 多对一映射
- ✓ 对于任意报文，产生固定长度的散列值(16-bit校验和)

但是，对于给定的报文及其散列值，很容易找到另一个具有相同散列值的不同报文！

message	ASCII format
I O U 1	49 4F 55 31
0 0 . 9	30 30 2E 39
9 B 0 B	39 42 D2 42
	B2 C1 D2 AC

message	ASCII format
I O U 9	49 4F 55 39
0 0 . 1	30 30 2E 31
9 B 0 B	39 42 D2 42
	B2 C1 D2 AC

不同报文却
得到完全相同的
散列值!

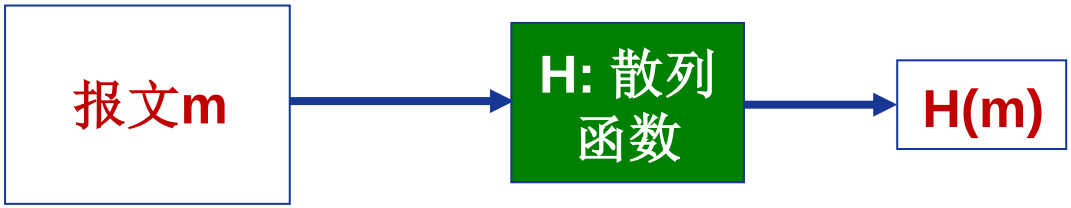
散列函数算法

- MD5：被广泛应用的散列函数(RFC 1321)
  - 通过4个步骤，对任意长度的报文输入，计算输出128位的散列值
  - MD5不是足够安全
    - 1996年，Dobbertin找到了两个不同的512-bit块，在MD5计算下产生了相同的散列值
- SHA-1(Secure Hash Algorithm)：另一个正在使用的散列算法
  - US标准 [NIST, FIPS PUB 180-1]
  - SHA-1要求输入消息长度<2^{64}
  - SHA-1的散列值为160位
  - 速度慢于MD5，安全性优于MD5

报文摘要(Message digests)

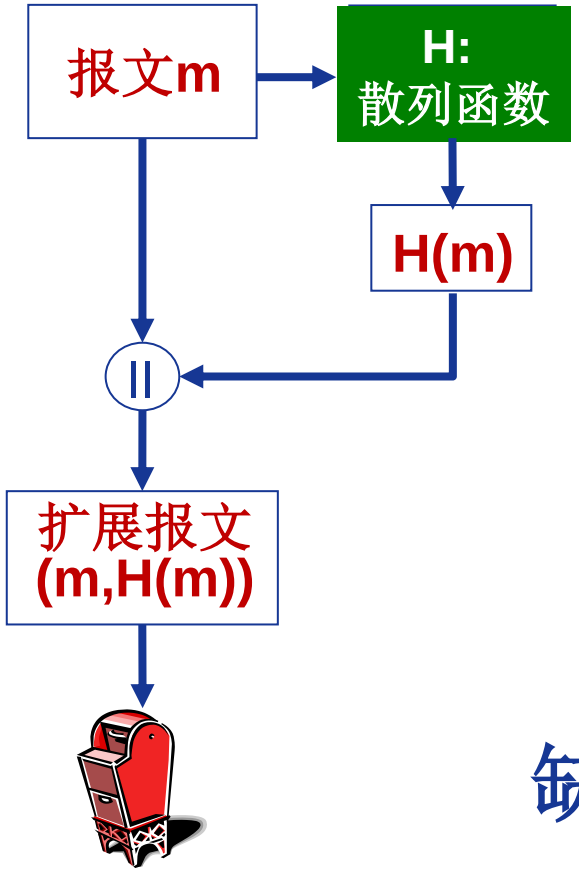
对报文m应用散列函数H，得到一个固定长度的散列码，称为报文摘要(message digest)，记为H(m)

- ✓ 可以作为报文m的数字指纹(fingerprint)。

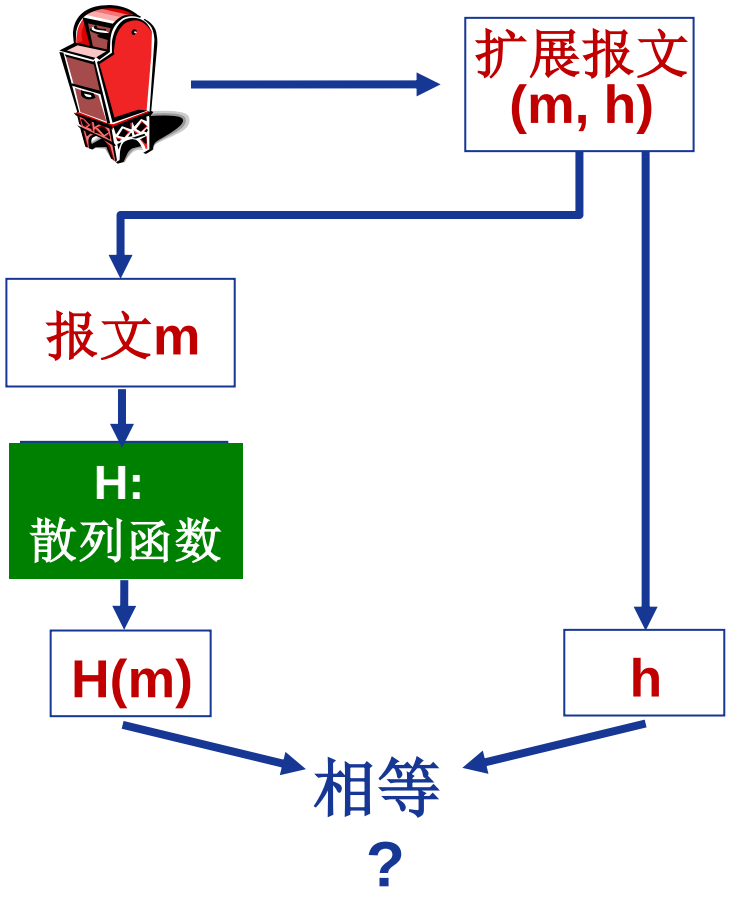


报文认证

简单方案：报文+报文摘要→扩展报文(m, H(m))



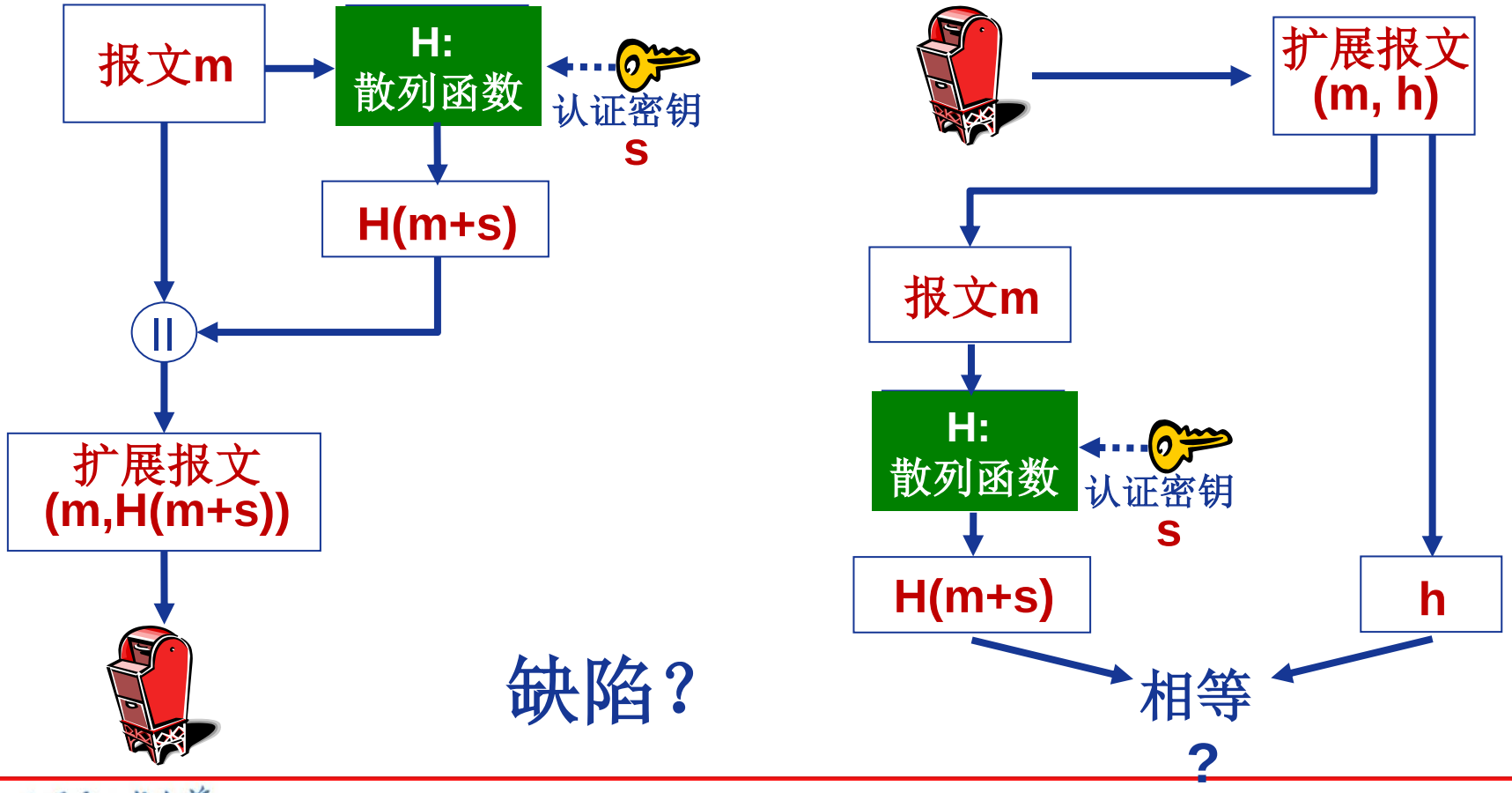
缺陷？



报文认证

报文认证码MAC(Message Authentication Code)：

报文m+认证密钥s+密码散列函数H→扩展报文(m, H(m+s))



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！