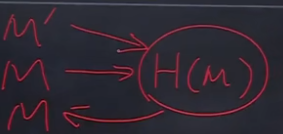
消息完整性与数字签名

1. 消息完整性检测方法

密码散列函数

1. 特性：
   1. 定长输出
   2. 单向性（无法根据散列值逆推报文）
   3. 抗碰撞性（无法找到具有相同散列值的两个报文）



1. 典型散列函数
   1. MDS：128位散列值
   2. SHA-1：160位散列值
2. 报文认证

报文认证是使消息的接收者能够检验收到的消息是否是真实的认证方法。来源真实、未被篡改

1. 报文摘要（数字指纹）：利用哈希算法，算成一个比较短的固定的值
2. 报文认证方法
   1. 简单报文验证：仅使用报文摘要，无论验证来源真实性
   2. 报文认证码：使用共享认证密钥，但无法防止接收方篡改
3. 数字签名

身份认证、数据完整性、不可否认性

1. 简单数字签名：直接对报文签名（公钥算法，产生的数据量太大）
2. 签名报文摘要（U盾）

