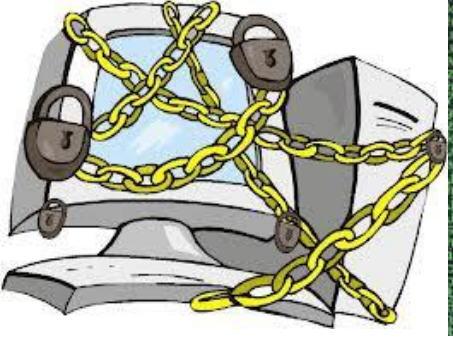


信息系统安全

数据安全保护

完整性与不可否认性保护

陈春华 博士

chunhuachen@scut.edu.cn

2018 春季

华南理工大学 软件学院

大纲

- 完整性保护
  - 消息认证
  - 消息认证码 (MAC)
  - Hash函数
  - 其他
- 不可否认性保护
  - 数字签名
  - 公证机制
  - 数字证书与公钥基础设施

数据完整性保护的概念

- 包括针对如下3种攻击所采取的措施
  - 内容篡改(content modification)，包括对报文内容的插入，删除，改变等
  - 序列篡改(sequence modification)，包括对报文序列的插入，删除，错序等
  - 时间篡改(timing modification)，对报文进行延迟或者回放
- 即完整性包括内容完整性，序列完整性和时间完整性

消息认证的概念 message authentication

- 又称报文鉴别，是用于验证所收到的消息确实来自真正的发送方，并未受到内容篡改，序列篡改和时间篡改攻击；包括
  - **内容认证，是消息认证的核心**
  - 序列认证，通常通过报文序号，接收方检查序号来鉴别报文序列是否遭受攻击
  - 时间认证，又称数据实时性保护，通常可以采用时间戳或者**询问-应答机制**进行确认

消息认证-鉴别码

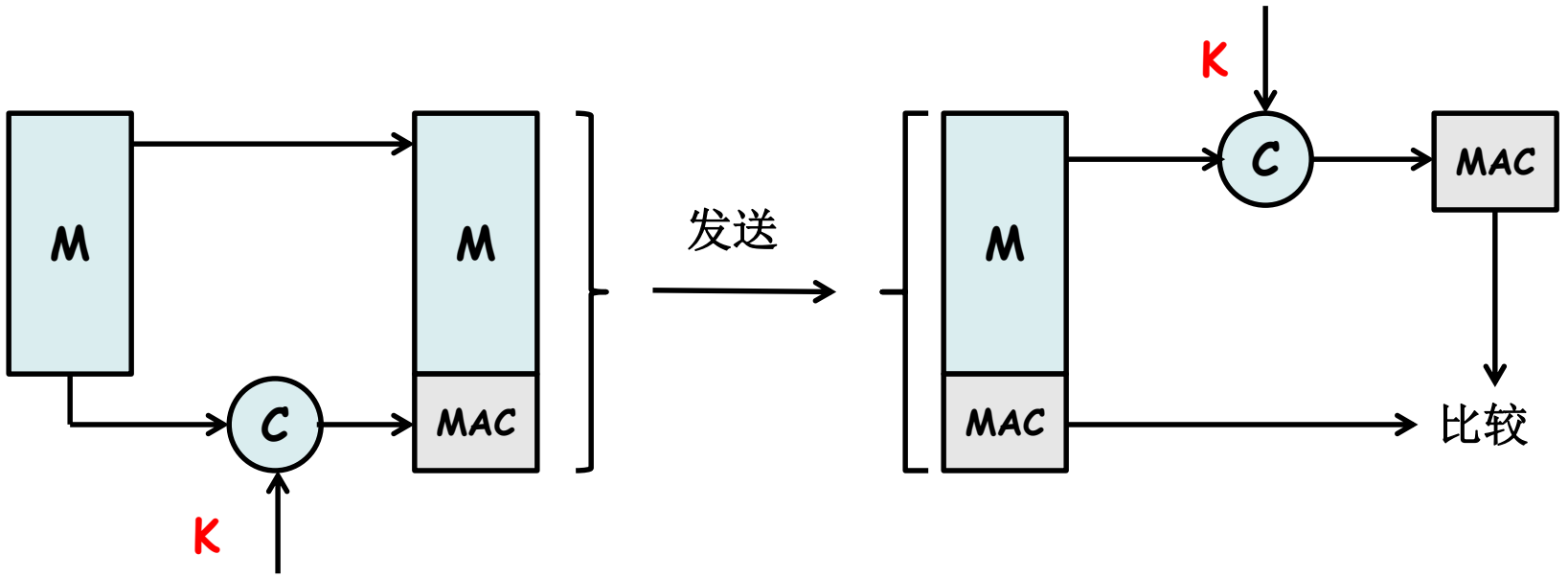
- 从功能上可分为两个层次：
  - 底层是认证函数
  - 上层是认证协议
- 认证函数的功能是能够由报文产生具有唯一性的**鉴别码**

消息认证-鉴别码

- 完整性保护的基本原理
  - 利用认证函数生成基于报文的鉴别码*A*
  - 将报文(是否保密，取决应用需求)+鉴别码*A*发送接收方
  - 接收方由报文生成鉴别码B，由于鉴别码的唯一性，如果*A*=B，说明报文没有收到针对内容完整性的攻击

认证函数：生成鉴别码的方法

- 基于MAC (Message Authentication Code, 消息认证码)的方法，使用一个由密钥控制的鉴别码生成函数基于报文的固定长的鉴别码



MAC函数

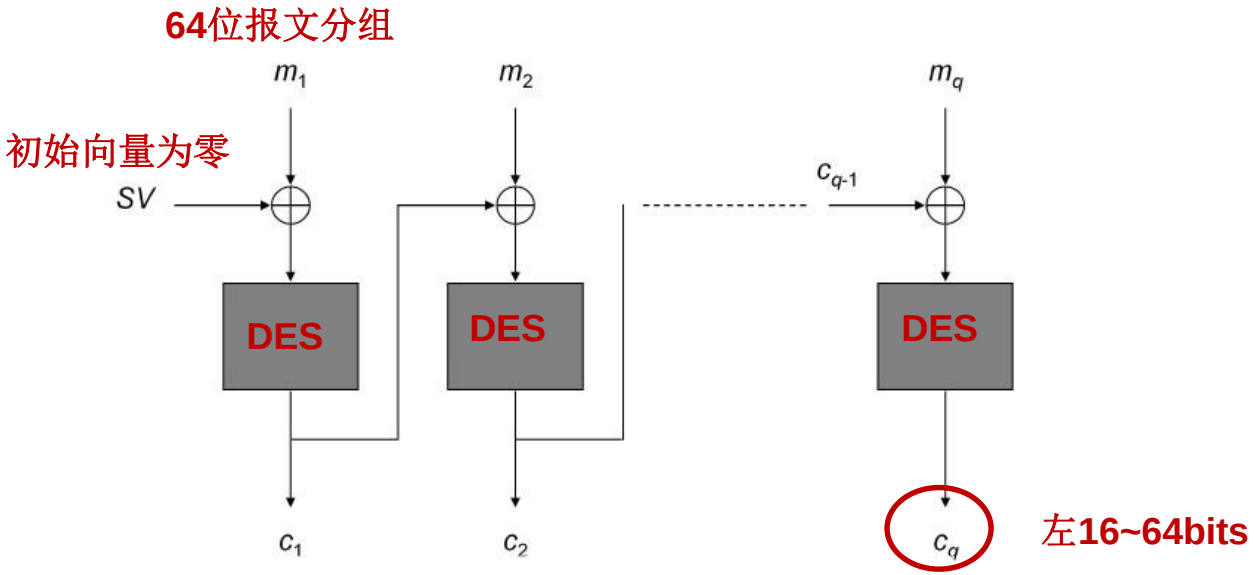
- 与加密函数类似，均需要通信双方共享密钥，但是有本质的区别
  - 加密算法要求可逆性，MAC算法不要求可逆性
  - 加密函数明文长度与密文长度一般相同，是一对一的函数；而MAC中，消息可以任意长，生成的鉴别码程度固定；存在M != M*，但是它们的MAC相等(多对一)!!
  - MAC函数比加密函数更不容易被攻破

安全MAC函数具备的性质

- 已知M和MAC，要找到满足MAC* = MAC的另一个M*，在计算上是不可能的；
- MAC是均匀分布的：对随机选择的M和M*，使得MAC* = MAC的概率是2^{-n}，n为MAC长度；
- 若M*是M的一个已知变换，则使得MAC* = MAC的概率是概率是2^{-n}；
- MAC函数所需密钥的长度必须足够抵抗穷举密钥攻击；
- 如果明文也需要机密性保护，必须使用另外一个密钥，不可同时使用MAC密钥作为加密密钥。

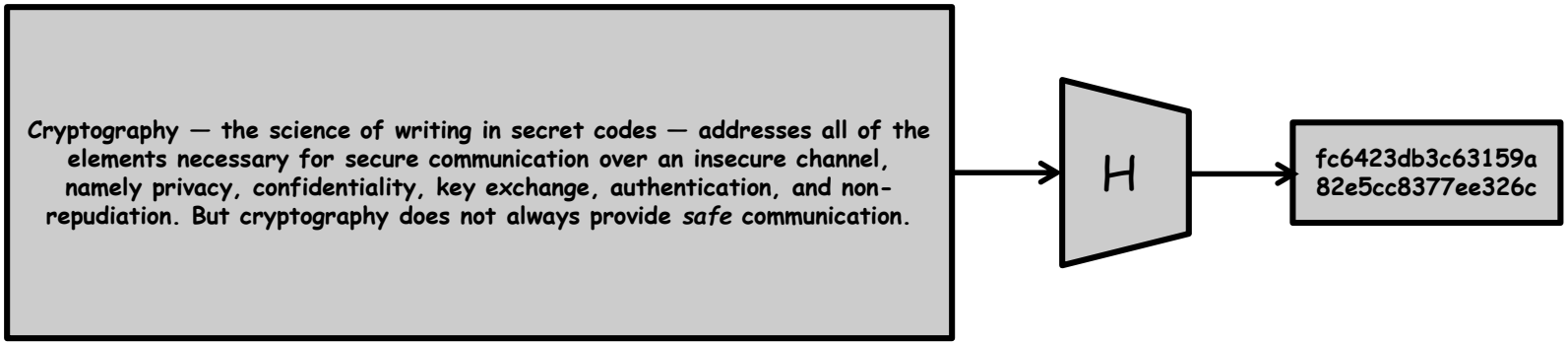
CBC-MAC

- ANSI标准，又称数据认证算法
- 建立在DES基础上，基于分组密码，并按照CBC模式操作的MAC构造方法之一
- 简单描述:



哈希函数

- 将任意长的输入消息串通过哈希算法(H)变换成为固定长度的输出串，该输出串就是哈希值，又称为数据指纹



hash函数具备的性质

- 为了满足消息认证的安全性：
  - H可以应用于任意长度的输入数据块，产生固定长度的哈希值 (效率考虑)
  - 给定M，计算h=H(M)很容易; 给定h,找到一个M,使得h=H(M)在计算上是不可能的，即单向性
  - 对于给定的M及其哈希值h, 要找到另外一个M*!=M, 使得H(M*)=H(M)在计算上是不可能的，即弱抗**碰撞(collision)性** (防止替代性报文，伪造)
- 其他应用可能需要更高的安全性：
  - 找到任何M!=M*且H(M)=H(M*)在计算上是不可能的，即强抗碰撞性 **(抗生日攻击，复杂度2^{80})**

实际应用中的hash函数

- 1991年，Ronald L. Riverst, MD5算法
  - 不以任何假设和密码体制为基础，是一个直接构造出来的算法；
  - 哈希值长度：128-bits
  - 主要应用在：防篡改鉴别(软件下载)和加密(口令保存)
  - Crypto'04, 山东大学数学系-王小云教授公开找到MD5产生碰撞的方法(复杂度 2^{40})

实际应用中的hash函数

- 1995年，SHA (Secure Hash Algorithm) 安全哈希算法，包括SHA-1, SHA-224和SHA-256等
  - 基于MD4构造，哈希值长度：160-bits上
  - 主要应用在：数字签名标准算法(DSS)中
  - Crypto'04, 山东大学数学系-王小云教授公开找到SHA-0产生碰撞的方法 (复杂度2^{40})
  - SHA-1比MD5的抗穷举攻击能力强，执行速度相对较慢

算法	哈希值长度 bit	最大报文长度	分组处理长度 bit
MD5	128	无限制	512
SHA-1	160	$2^{64}-1$	512

认证函数：生成鉴别码的方法

- 基于报文（消息）摘要(Message Digest, MD)的方法，将报文使用单向杂凑(hash，称哈希或者散列)函数变换称为具有固定长度的鉴别码。
- Hash函数不使用密钥，通常配合其他安全机制使用。

实验@为报文生成哈希摘要

- 时间，待安排

不信任：否认与抵赖

- 在通信过程中，有时会发生一方对另一方进行如下的欺骗行为：
  - 否认：发送方否认自己发送过某个报文，或者接收方接收一个报文后，否定接受过；
  - 冒充：发送方冒充第三方给接收方发送报文；
  - 伪造：某一方自己伪造一份报文，却声称来自对方；
  - 篡改：接收方接收到一份报文后，却说这是对方发过来的报文原样。
- 在通信双方尚未建立起信任关系且存在利益冲突情况下，单纯的消息认证无法有效解决上述问题；为此，可采用数字签名技术。

数字签名

- 数字签名:“附加在数据单元上的一些数据，或是对数据单元所做的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如，接收者）进行伪造”。

  --ISO 7492-2标准

- 数据签名是实现数据的不可否认性保护的安全机制。

数据签名技术要求

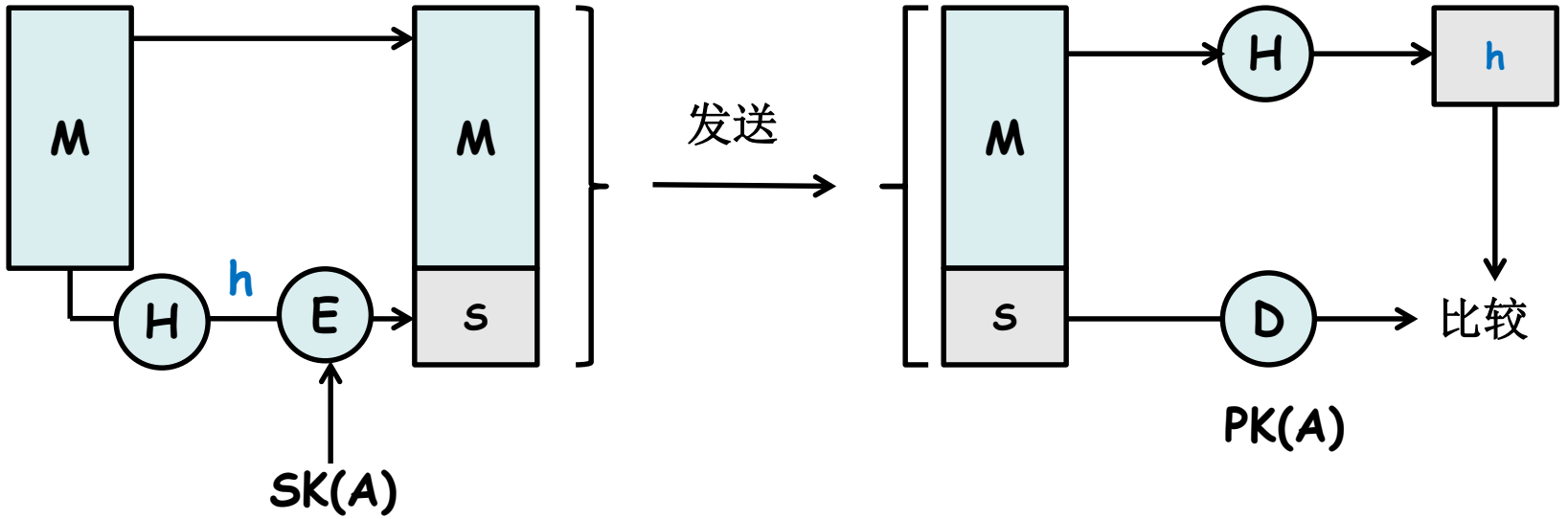
- 签名的生产，识别和验证应比较容易
- 签名能够用于证实被签名报文内容的真实性
- 签名的结果必须是与签名的报文相关的二进制串
- 签名能够验证签名者的身份以及签名的时间
- 用已知的签名构造一个新的报文或者由已知的报文产生一个假冒的签名，在计算上都是不可行的
- 签名可以由第三方验证，以解决双方在通信中的争议
- …… ……

直接数字签名

- 签名过程只有发送方和接收方参与
- 实施这种方法的前提是接收方可以通过某种方式验证发送方提交的凭证/签名，也可以在发送争议时将凭证交第三方仲裁。
- 使用对称加密构造，仅抵抗冒充，无法抵抗否认，篡改和伪造。
  - 为什么？

直接数字签名

- 使用非对称加密构造，A用私钥将报文加密，将其发送给B后，B用A的公钥将密文解密。
- 公钥算法效率慢，上述过程通过先将报文M通过一个单向哈希函数生成定长鉴别码，将消息认证与签名结合进行。



直接数字签名

- 这个过程中，A不可能冒充第三方，也无法否认自己的发送，B也无法篡改和伪造。
  - B可以否认接受吗？

- 有仲裁的数字签名，涉及第三方的参与，可提供更全的完整性与不可否认性保护。

数字签名算法

- RSA签名算法
- DSA (Digital Signature Algorithm, 数字签名算法)是美国国家标准委员会公布的数字签名标准

实验@使用RSA进行加密与签名

- 时间，待安排

如何管理公私钥？

- 公钥基础设施(PKI)，后续课程

Further Reading: