网络安全协议及分析
概述

密码与网络安全系　刘虹

2025年春季学期

课程体系

本章学习目标

- 网络协议存在的安全缺陷
- 网络安全协议的定义及主要组件
- 网络安全协议的安全需求

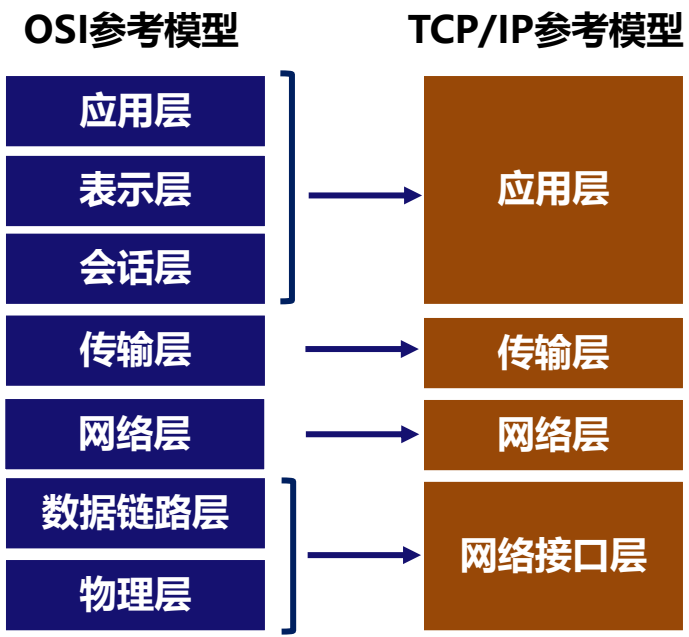
提纲

概述

- 传输控制协议/因特网互联协议

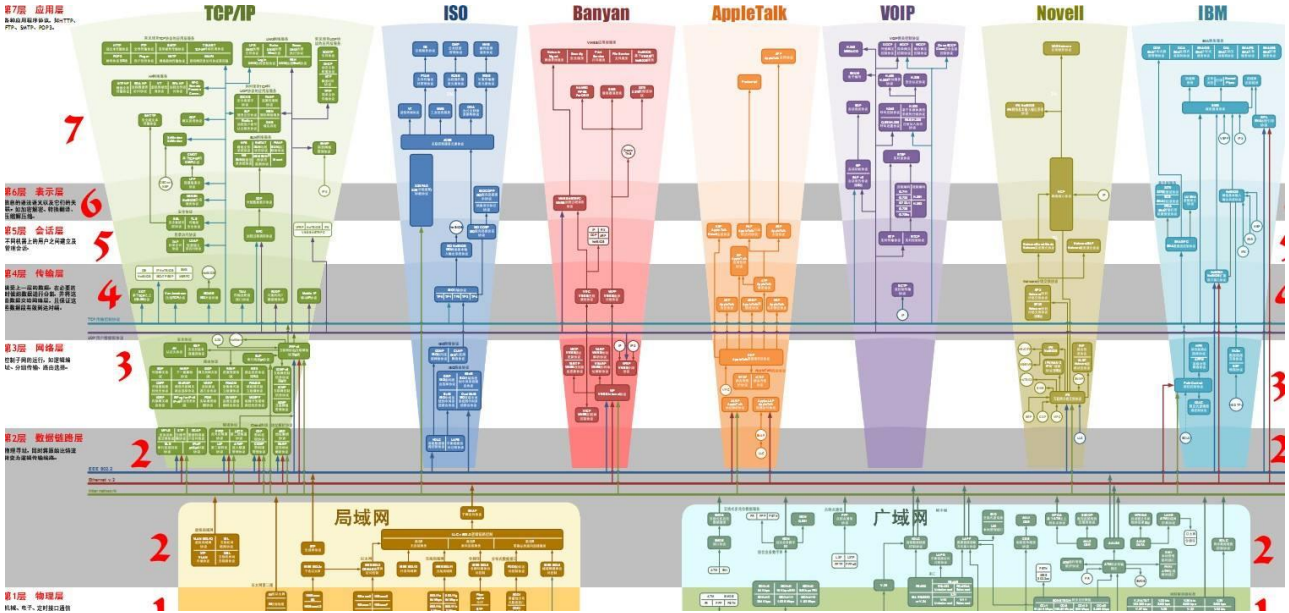
(Transmission Control Protocol / Internet Protocol，TCP/IP)

  - TCP：解决可靠传输问题
  - IP：解决异构网络互联问题



协议安全缺陷

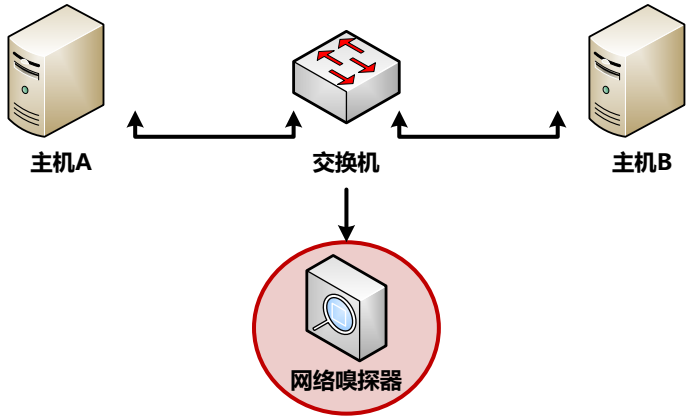
- 网络协议是网络通信的基础，规定了通信报文的格式、处理方式和交互时序，每一项内容都会影响通信的安全性。
  - 信息泄露
  - 信息篡改
  - 身份伪装
  - 行为否认



协议安全缺陷

信息泄露

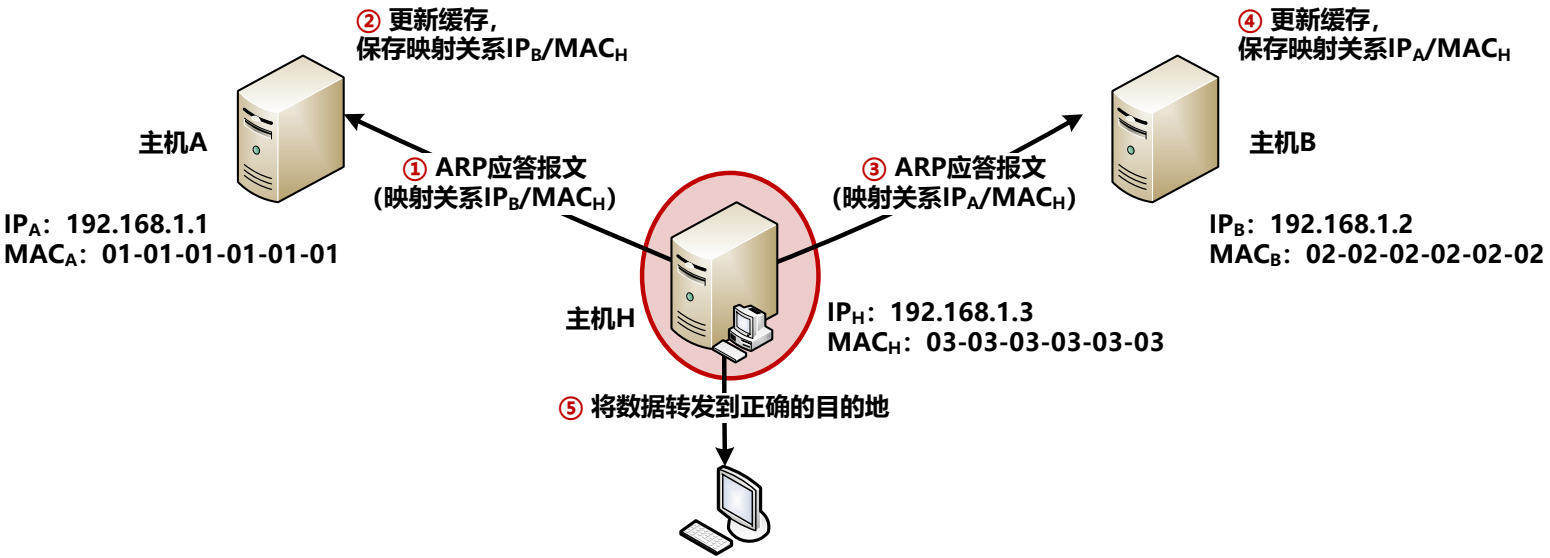
- 嗅探
  - **共享式**网络架构：所有数据以广播方式发送，将网卡工作模式设置为“**混杂**”就可以嗅探网段内所有的通信数据。
  - **交换式**网络架构：交换机具有“**记忆**”功能，通过将每个端口ID与该端口所连设备的“物理地址”进行绑定，并依据帧首部的“**目标地址**”将数据直接发送到相应端口。



协议安全缺陷

信息泄露

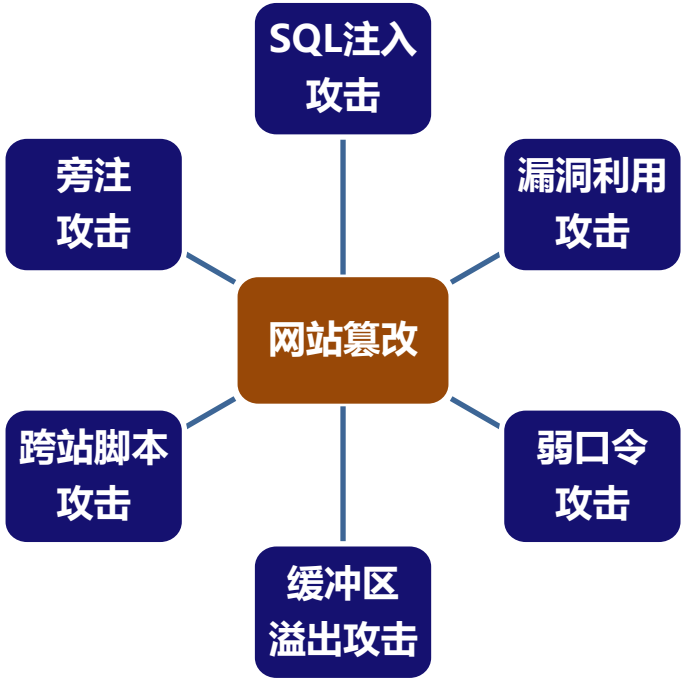
- ARP欺骗（Address Resolution Protocol，ARP），是攻击者在交换式网络环境下实施嗅探的基础。



协议安全缺陷

信息篡改

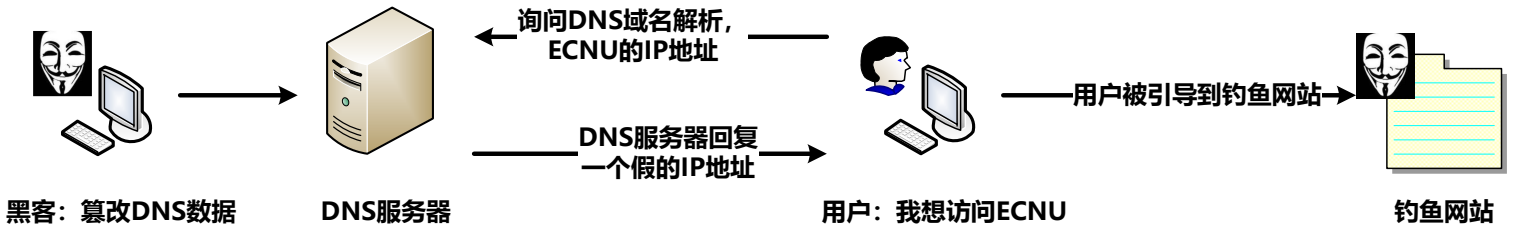
- 在截获的数据中插入**恶意代码**，以实现木马植入和病毒传播的目的。
- 超文本标记语言（Hyper Text Markup Language，HTML）源文件放在HTTP报文的数据区，这种攻击的实质是报文在传递过程中被恶意更改。



协议安全缺陷

身份伪装

- ARP欺骗：网络接口层
- IP欺骗：IP层
- 域名服务器（Domain Name System，DNS）欺骗：应用层
- 路由信息协议（Routing Information Protocol，RIP）欺骗：网络层



协议安全缺陷

- **行为否认**
  - 数据发送方否认自己已发送数据，或者接收方否认自己已收到数据

- **举例**
  - IP协议、用户数据报协议（User Datagram Protocol，UDP）、TCP、HTTP等常用的协议都没有提供防止行为否认的功能。
  - 日志审计：源IP、目标IP、源端口和目的端口此类协议特征信息

网络安全需求

- 信息保障技术框架（Information Assurance Technical Framework，IATF）定义网络安全需求：
  - 机密性：不被泄露
  - 完整性：不被篡改
  - 可用性
  - 来源真实性
  - 不可否认性

网络安全需求

- 基于“密码学”的安全机制具有通用性，兼顾安全性和高效性
  - HTTPS（Hyper Text Transfer Protocol Secure）
  - 安全套接层：Secure Sockets Layer，SSL
  - 传输层安全：Transport Layer Security，TLS

HTTPS = HTTP + TLS/SSL

- HTTPS需要到CA申请证书
- HTTP是明文传输； HTTPS基于SSL加密传输协议
- HTTP端口80，HTTPS端口443

提纲

一、网络安全协议的引入

二、网络安全协议的定义

三、网络安全协议组件

四、网络安全协议设计要素

二 网络安全协议定义

- 网络安全协议：基于密码学的通信协议
  - 网络安全协议以密码学为基础：
    - 算法+密钥
  - 网络安全协议也是通信协议：
    - 语法规定协议报文的格式
    - 语义规定对报文的处理方法
    - 时序则规定通信双方交换报文的顺序
- 设计理念
  - 灵活性、兼容性、互操作性

二 网络安全协议定义

- 密码学中的人物“历险记”
  - Alice 爱丽丝　　协议中第一个参与者。
  - Bob 鲍伯　　协议中第二个参与者，Alice希望把一条消息传送给Bob。
  - Carol 卡罗尔　　协议中第三个参与者。
  - Dave 戴夫　　协议中第四个参与者。
  - Eve 伊夫　　偷听者（Eavesdropper），但行为通常是被动的。
  - Isaac 艾萨克　　互联网服务提供者（ISP）。
  - Ivan 伊凡　　发行人，用于商业密码学。
  - Justin 贾斯汀　　司法机关（Justice）。
  - Mallory 马洛里　　恶意攻击者(Malicious Attacker)。
  - Matilda 马提尔达　　商人(Merchant)，用于电子商务。

二 网络安全协议定义

- 密码学中的人物“历险记”
  - Oscar 奥斯卡　　敌人，等同马洛里。
  - Peggy 佩吉　　证明者（Prover）。
  - Victor 维克托　　验证者（Verifier），与证明者证实某事件是否实际进行。
  - Plod 普特　　执法官员。
  - Steve 史蒂夫　　隐写术者（Steganography）。
  - Trent 特伦特　　可信赖的仲裁人（Trusted Arbitrator），中立的第三者。
  - Trudy 特鲁迪　　侵入者（Intruder），等同马洛里。
  - Walter 沃特　　看守人（Warden），根据协议保护爱丽丝和鲍伯。
  - Zoe 佐伊　　协议中最后一位参与者。

提纲

一、网络安全协议的引入

二、网络安全协议的定义

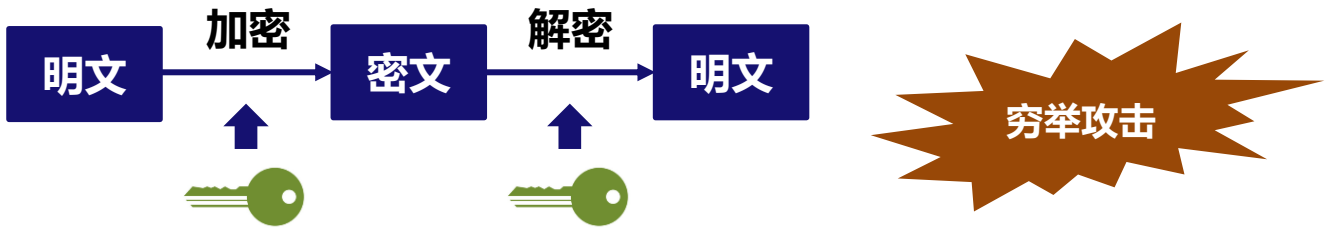
三、网络安全协议组件

四、网络安全协议设计要素

网络安全协议组件

加密与解密

- 将数据在密钥的作用下转换为密文，是增加“**数据不规则性**”的过程。



- 在未知密钥的情况下，攻击者可以对密文进行“**穷举攻击**”破解以还原明文。当密钥的范围足够大时，便无法完全遍历所有可能的密钥。

三 网络安全协议组件

- 加密与解密
  - 对称密码算法：AES、3DES、SM4等

  - 公钥密码算法：RSA、DSA、ECC、SM2等

Bob的公钥　　Bob的私钥

三 网络安全协议组件

消息摘要

- 一段数据的摘要（Digest）是表征该数据特征的字符串，获取数据摘要的功能通常由散列（Hash）函数完成，例如MD5、SHA-1/2/256/512。
- 散列函数是一种“压缩映射”过程，实现将任意长度的数据，转化为固定长度的散列值，数学表达式为：

$$h=H(M)$$

例如，TCP/IP协议族中的报文包含“校验和”，将任意报文长度转化为2B

- 摘要是验证数据完整性的基础

三 网络安全协议组件

消息摘要

- 映射分布均匀性和差分分布均匀性
  - **雪崩效应**：输入中一个比特的变化，散列结果中将有一半以上的比特改变
- 单向性：$M=H^{-1}(M)$不可行
- 抗冲突性：$H(M)\neq H(M')$
  - 弱抗冲突性
  - 强抗冲突性

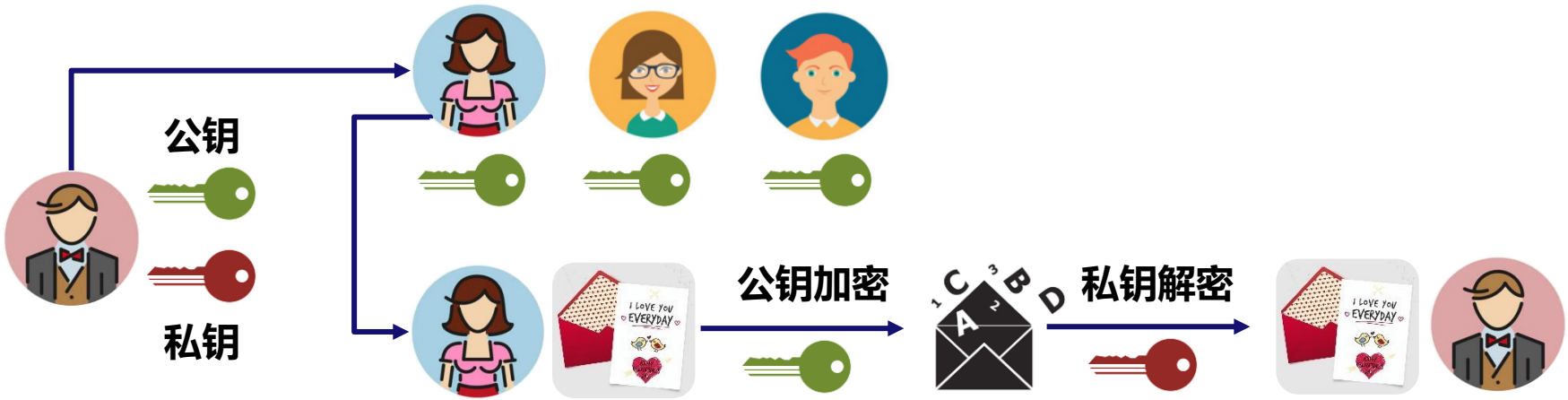
单向性和抗冲突性似乎形成了一对矛盾
任何抵御冲突发生的消息摘要的强度只有摘要值长度的一半

网络安全协议组件

- 消息验证码
  - Message Authentication Code（MAC）：密钥+Hash函数。
  - 与完整性校验值（Integrate Check Value，ICV）的含义相同，是基于密钥和消息摘要所获得的一个值，可用于数据源认证和完整性校验。

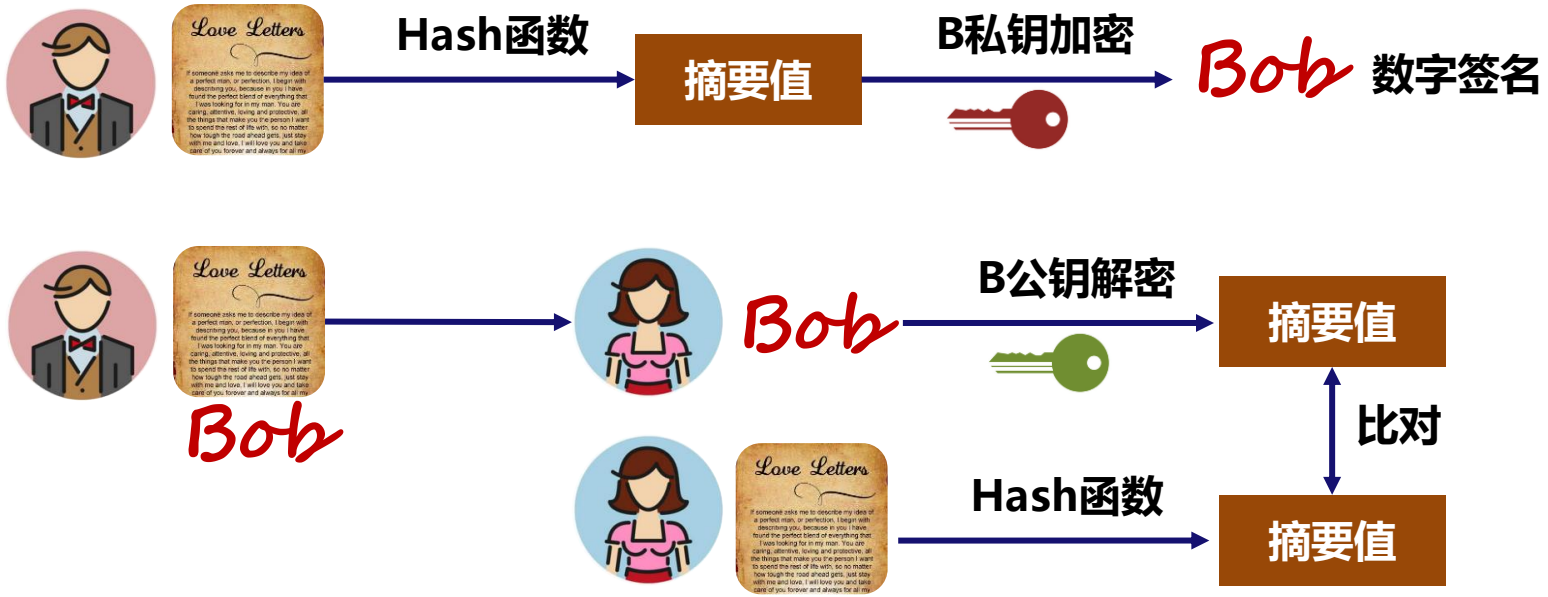
网络安全协议组件

- 数字签名
  - 通常用于确保不可否认性，原理与消息验证码类似，具备认证功能。
  - 基于消息摘要，数字签名使用发送方的**私钥**加密摘要；
  - 接收方在验证数字签名时，利用发送方的**公钥**进行解密。



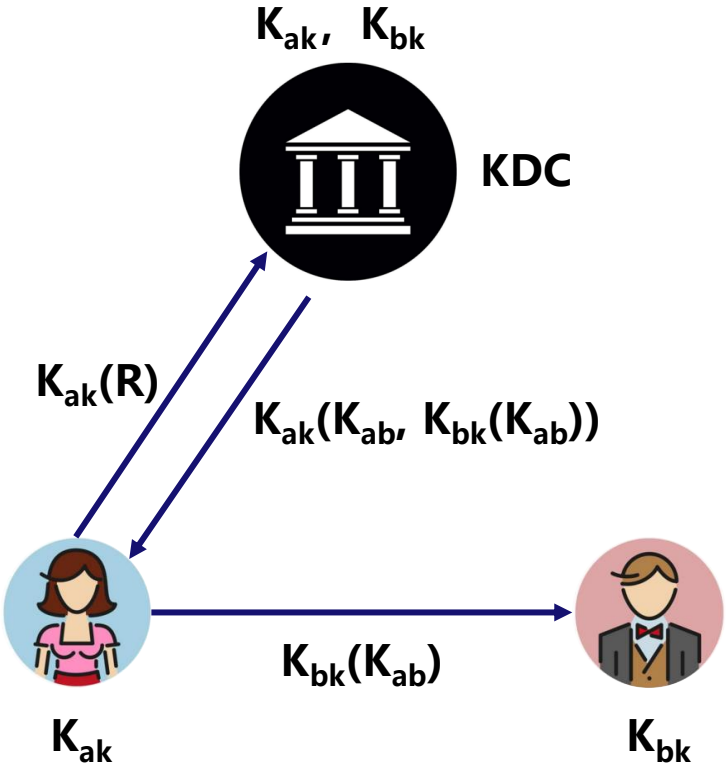
三 网络安全协议组件

数字签名



网络安全协议组件

- 密钥管理
  - 密钥是密码系统的核心，涉及密钥生成、分配、传递、保存、备份和销毁等
- 建立共享密钥
  - 基于可信第三方方式：**密钥分发中心**（Key Distribution Center，KDC）



网络安全协议组件

建立共享密钥

密钥协商方式

- 通信双方交换生成密钥的**素材**，并各自利用这些素材在本地生成共享密钥。密钥协商算法被设计为即便攻击者获得了这些素材，也无法生成密钥。
- **Diffie–Hellman**（D-H）密钥协商：通信双方共享模数p（大质数），发生器g

对于任意z<p，存在W，使得$g^W \bmod p = Z$

假设X<p，计算：$Y = g^x \bmod p$，最终X被作为私钥，Y被作为公钥

设X_a和Y_a是Alice的私钥和公钥，X_b和Y_b是Bob的私钥和公钥

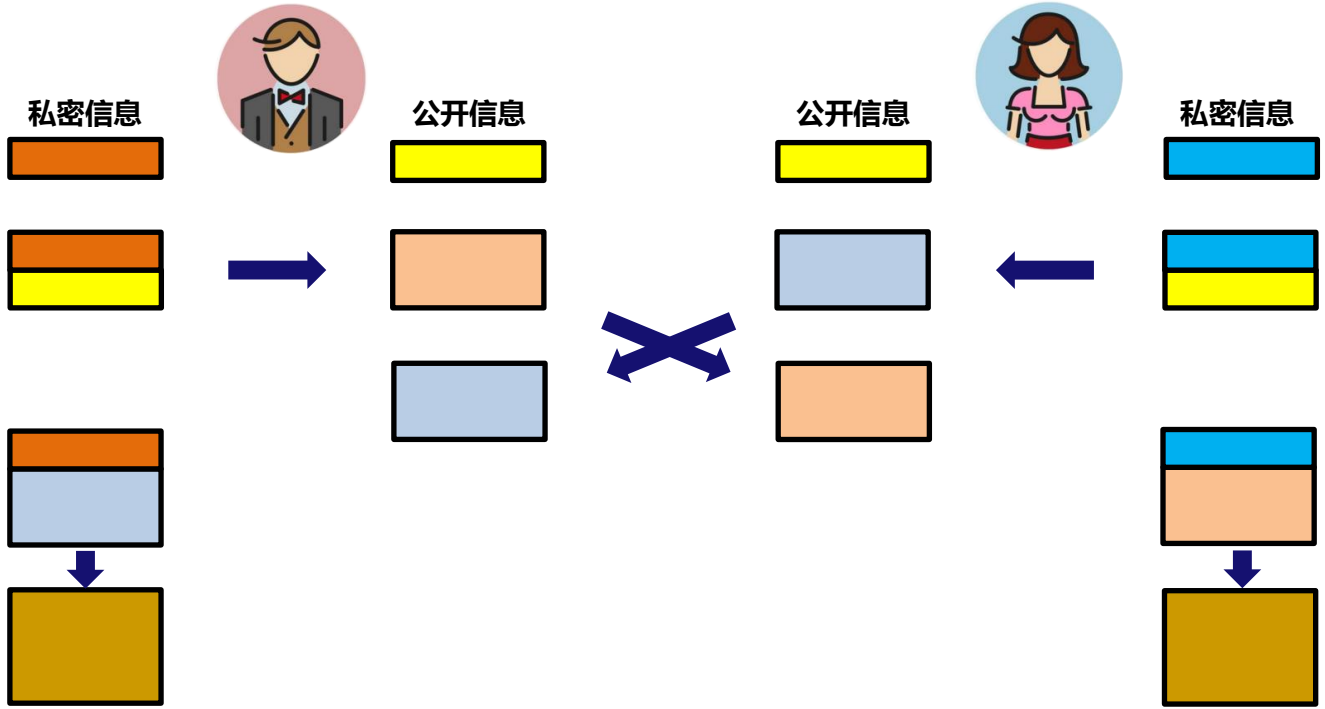
$Y_a = g^{Xa} \bmod p$，$Y_b = g^{Xb} \bmod p$

Alice计算：$K_{ab} = (Y_b)^{Xa} \bmod p = (g^{Xb})^{Xa} \bmod p = g^{Xb \cdot Xa} \bmod p$

Bob计算：$K_{ba} = (Y_a)^{Xb} \bmod p = (g^{Xa})^{Xb} \bmod p = g^{Xa \cdot Xb} \bmod p$

网络安全协议组件

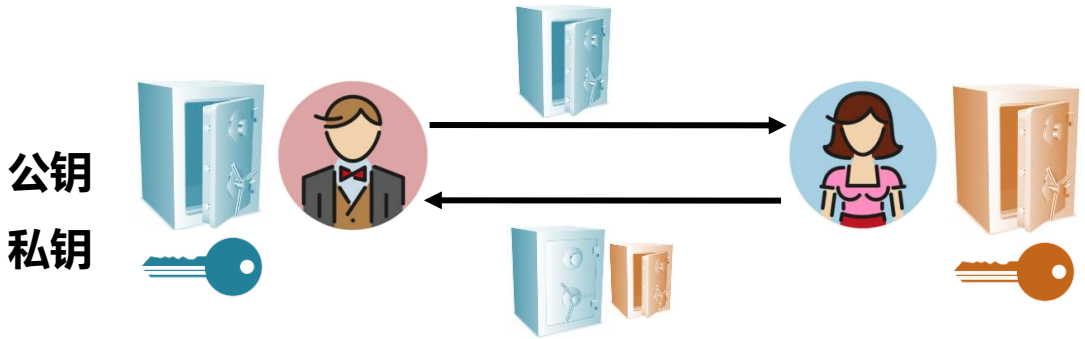
- 建立共享密钥：D-H密钥协商图解“颜料混合”



网络安全协议组件

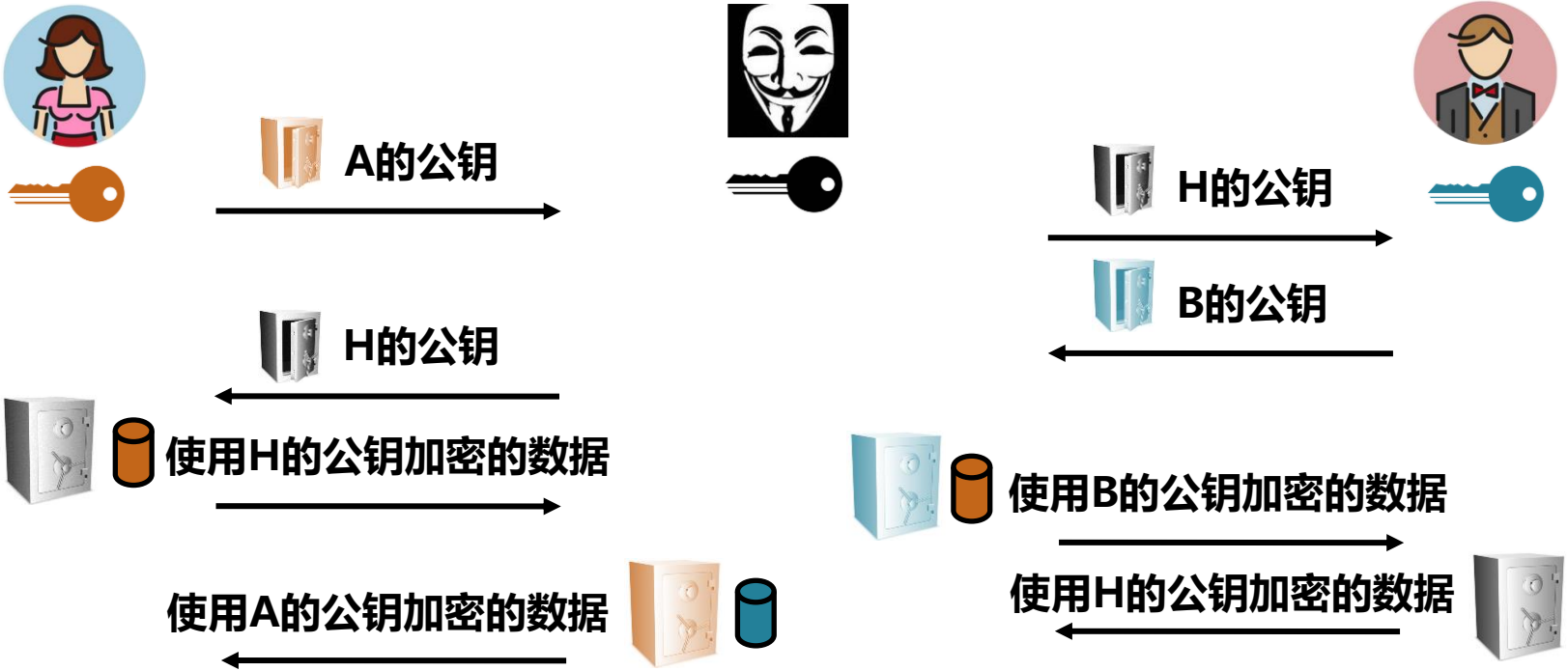
建立共享密钥

- 密钥传输的核心思想是由通信一方生成共享密钥，并通过某种途径将该密钥传递到通信对等端，保证传输过程的安全。
- 公钥密码体制保护共享密钥
  - 通信一方生成共享密钥后，用对方的公钥进行加密并传递。
  - 对方利用其私钥解密该数据，从而实现密钥的共享。



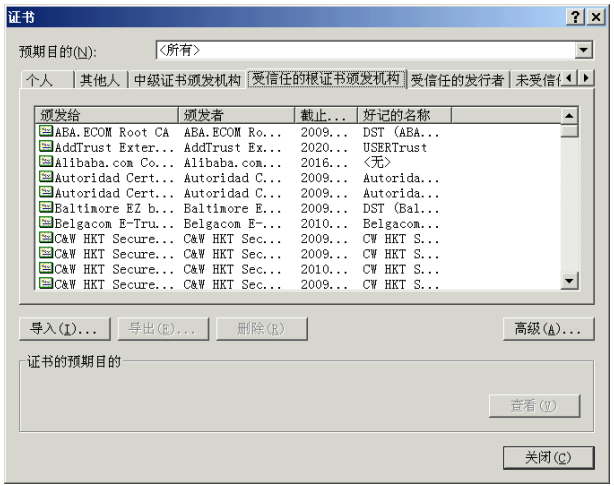
网络安全协议组件

- 公钥管理可能面临“中间人攻击”



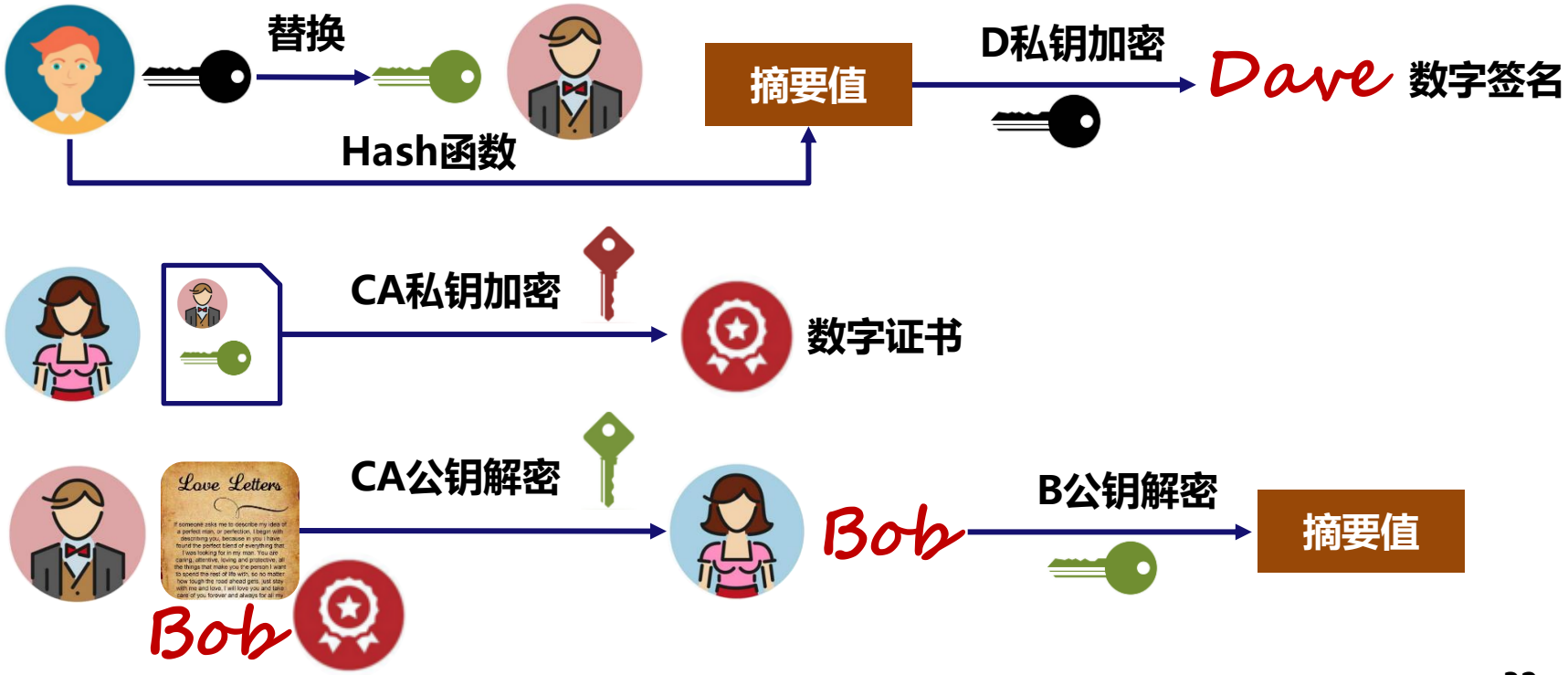
网络安全协议组件

- 公钥管理：
  - 证书授权中心（Certificate Authority，CA）
    - 负责证书的颁发、管理、归档、撤销。
  - 数字证书：
    - 公钥：证书所有者的公钥
    - 签名：颁发该证书的CA用自己私钥对证书所做的签名
  - 国际标准：X.509标准
    - 版本、序列号（唯一标识符）、签名算法、颁发者名称、主体名称、有效期等
    - 证书撤销列表（Certificate Revocation List，CRL)



网络安全协议组件

- 公钥管理：



提纲

一、网络安全协议的引入

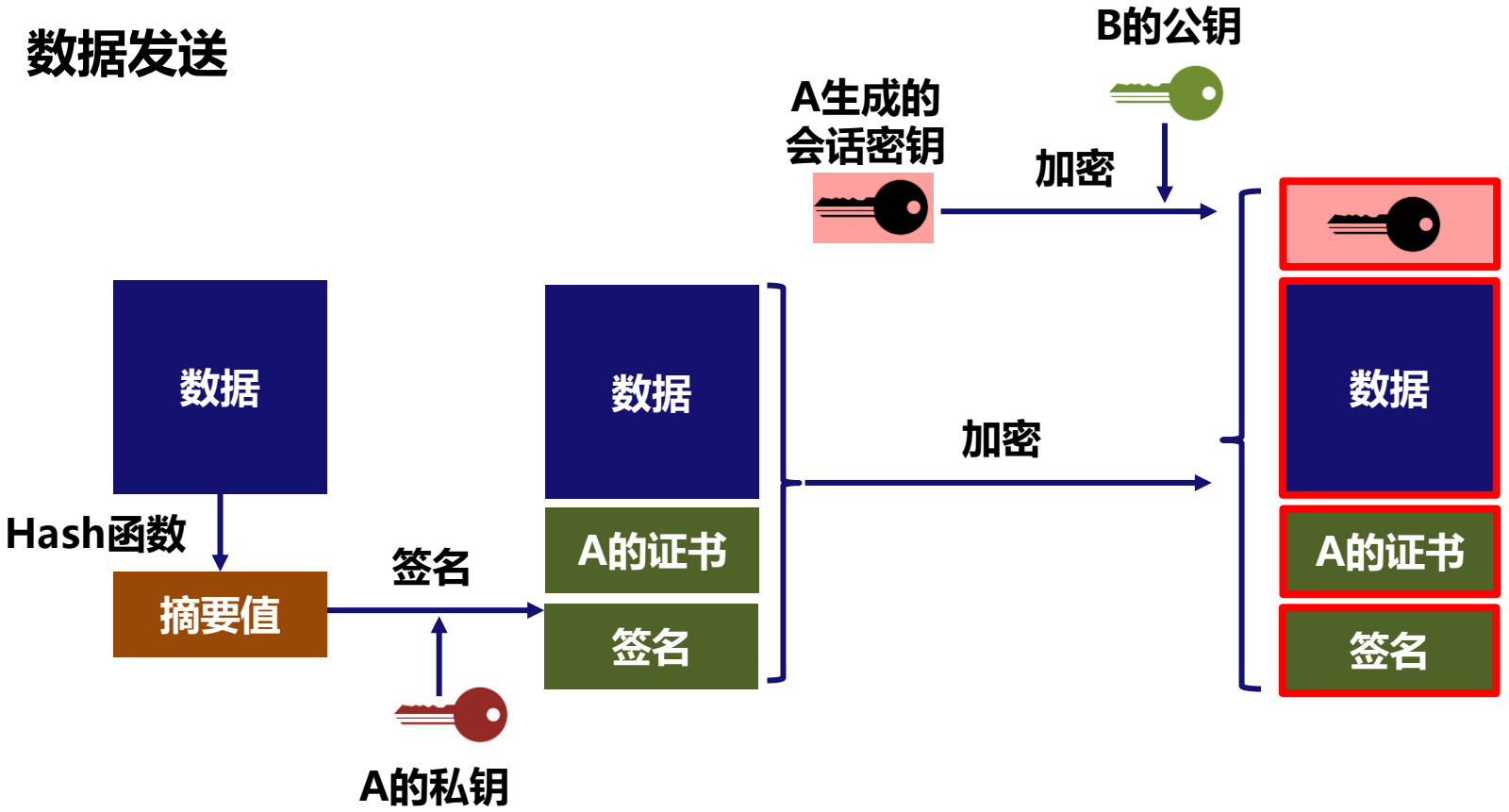
二、网络安全协议的定义

三、网络安全协议组件

四、网络安全协议设计要素

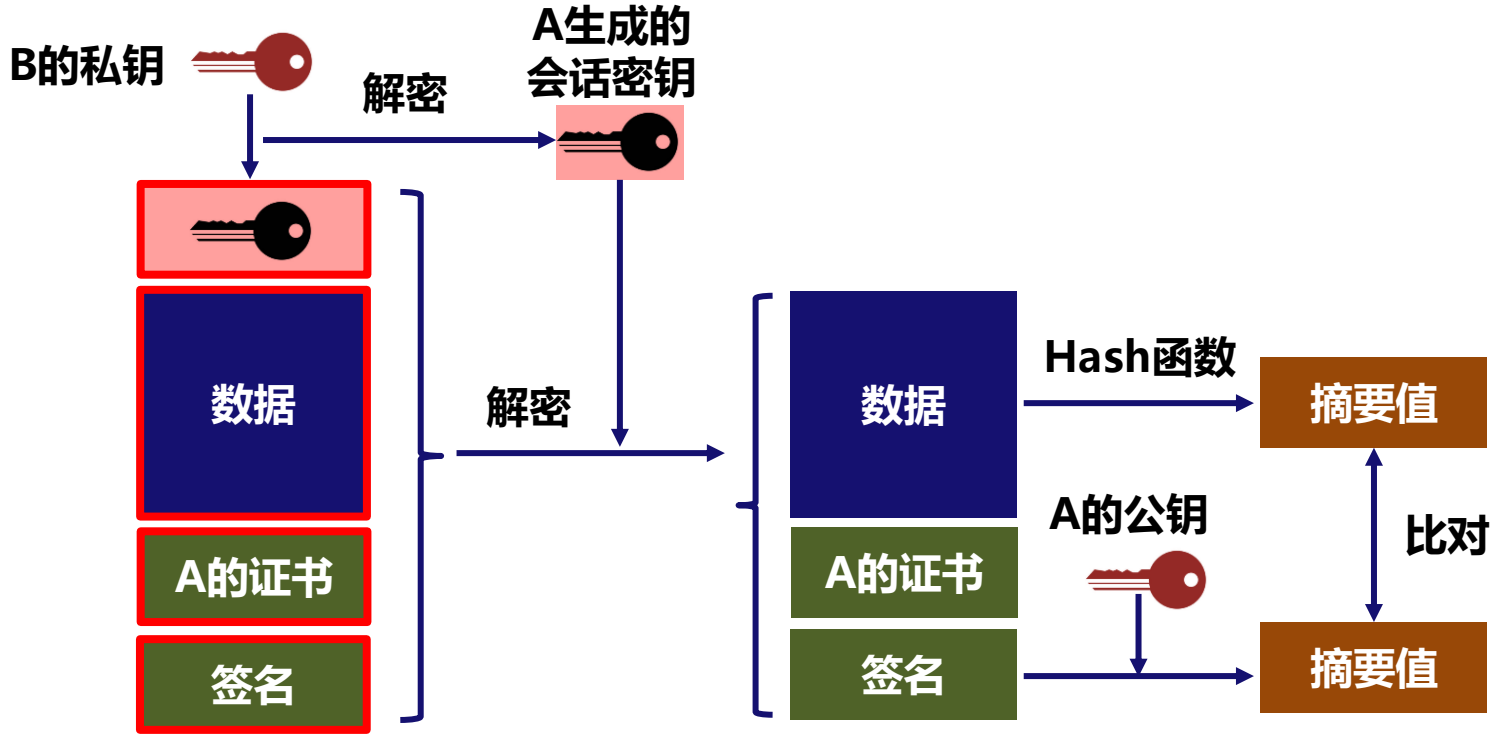
网络安全协议设计

- 数据发送



网络安全协议设计

数据接收



网络安全协议设计

- 存在的主要问题
  - 在A发送数据之前，已经默认B是自己预期的通信对等端，但在实际通信中往往并非如此，该方案忽略了**身份认证**过程。
  - A使用的加密算法、散列算法和签名算法必须与B一致，否则两者无法完成数据通信，该方案忽略了**算法协商**过程。
  - 数据传输时，除了数据本身，还需要附加证书和共享密钥信息。

网络安全协议设计

- 在规定网络安全协议的语法、语义和时序时，主要考虑：
  - 应用场景
  - 协议栈层次
  - 安全性

网络安全协议设计

- 应用场景的考虑
  - 安全套接层（Secure Sockets Layer，SSL）源于网景公司（Netscape）的Web浏览器：
    - 服务器认证必选，客户端认证可选
  - 安全协议套件IPSec：
    - 通信双方相互认证
  - DNS安全扩展DNSsec

网络安全协议设计

- 协议栈层次的考虑
  - 下层是服务提供者，上层是服务使用者
  - 安全协议工作的层次越低，所提供的安全服务越通用
- 网络通信
  - IP层及以下：点到点（Point to Point）
    - 安全协议可以在任意两个通信节点部署
  - 传输层/应用层：端到端（Peer to Peer）
    - 安全协议通常在两个通信端点上部署

四 网络安全协议设计

- 安全性考虑
  - 通信双方经过一系列的数据交互完成算法协商、密钥生成及身份认证
  - 网络安全协议则规定了通过网络交互数据的语法、语义和时序
- 形式化分析
  - 基于模态逻辑技术
  - 基于模型检测技术
  - 基于定理证明技术

推荐教材

- 寇晓蕤等，网络安全协议：原理、结构与应用（第2版），高等教育出版社

办公地点：理科大楼B1715

联系方式：17621203829

邮箱：liuhongler@foxmail.com