密码学基础

范明钰

信息安全研究中心

主要内容

算法分类

算法的使用

密码算法分类-1

按有无密钥

有密钥算法：可还原明文（$E_n(m,k)/D_n(c,k)$）

无密钥算法：不能还原出明文（Hash）

密码算法分类-2

按照保护条件

受限制的(restricted)算法：算法、密钥的保护

基于密钥(key-based)的算法：密钥的保护

密码算法分类-3

可还原的算法，密钥	对称密码算法 (symmetric cipher)
	非对称密钥算法 (asymmetric cipher)
不可还原的算法，Hash	基于分组算法的构造
	定制的

密码算法分类-4

对称密钥密码又分为

- 分组密码：每次对一块（组）数据加密；用于网络数据加密（DES, IDEA, RC6, Rijndael）
- 流密码—序列密码：每次对一位或一字节加密；用于语音加密（One-time padding, Vigenére, Vernam）

密码算法分类-5

公开密钥密码

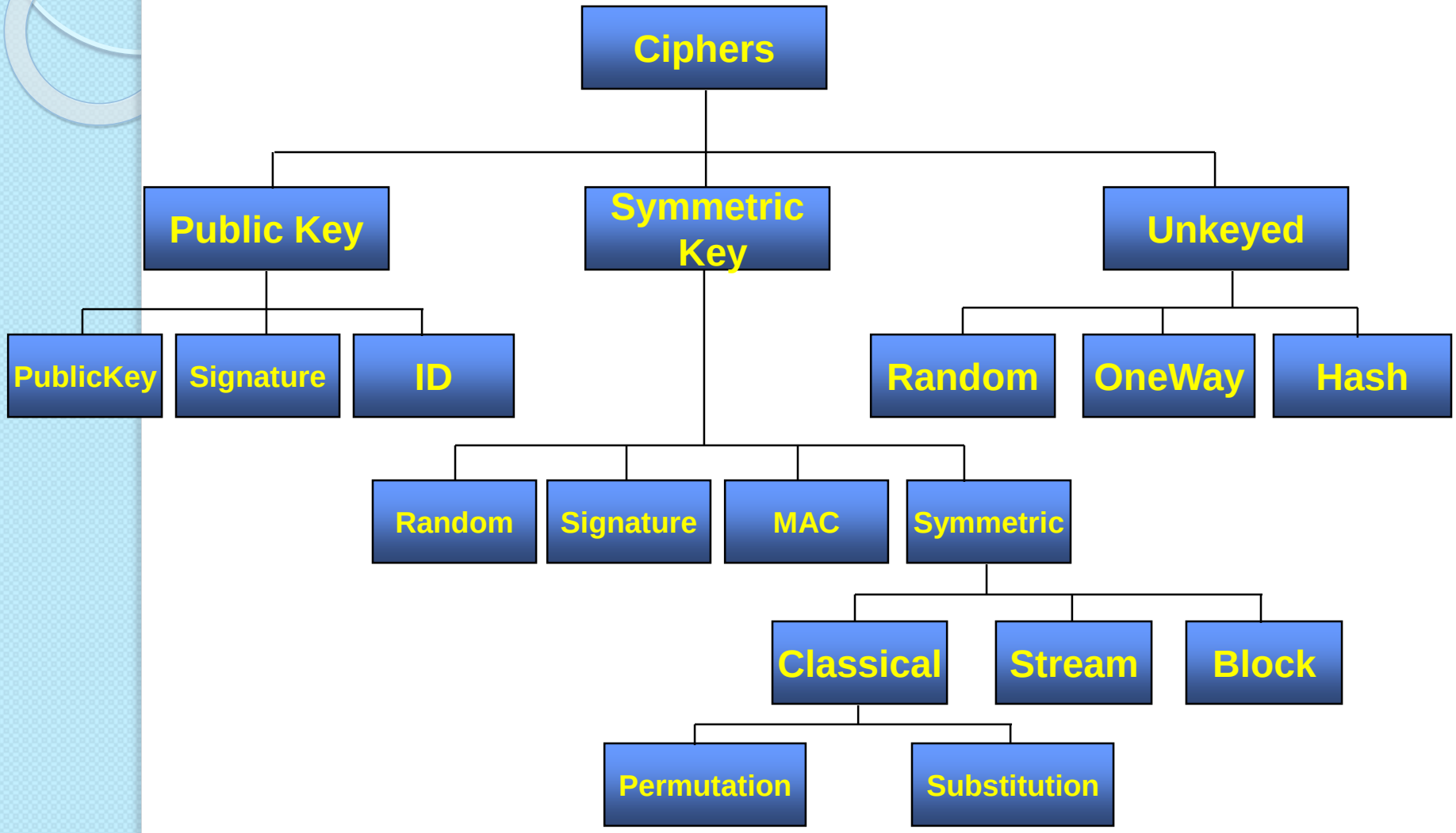
用法：大部分是分组密码，每次对一块数据加密

特点：加密解密速度慢、密文扩展

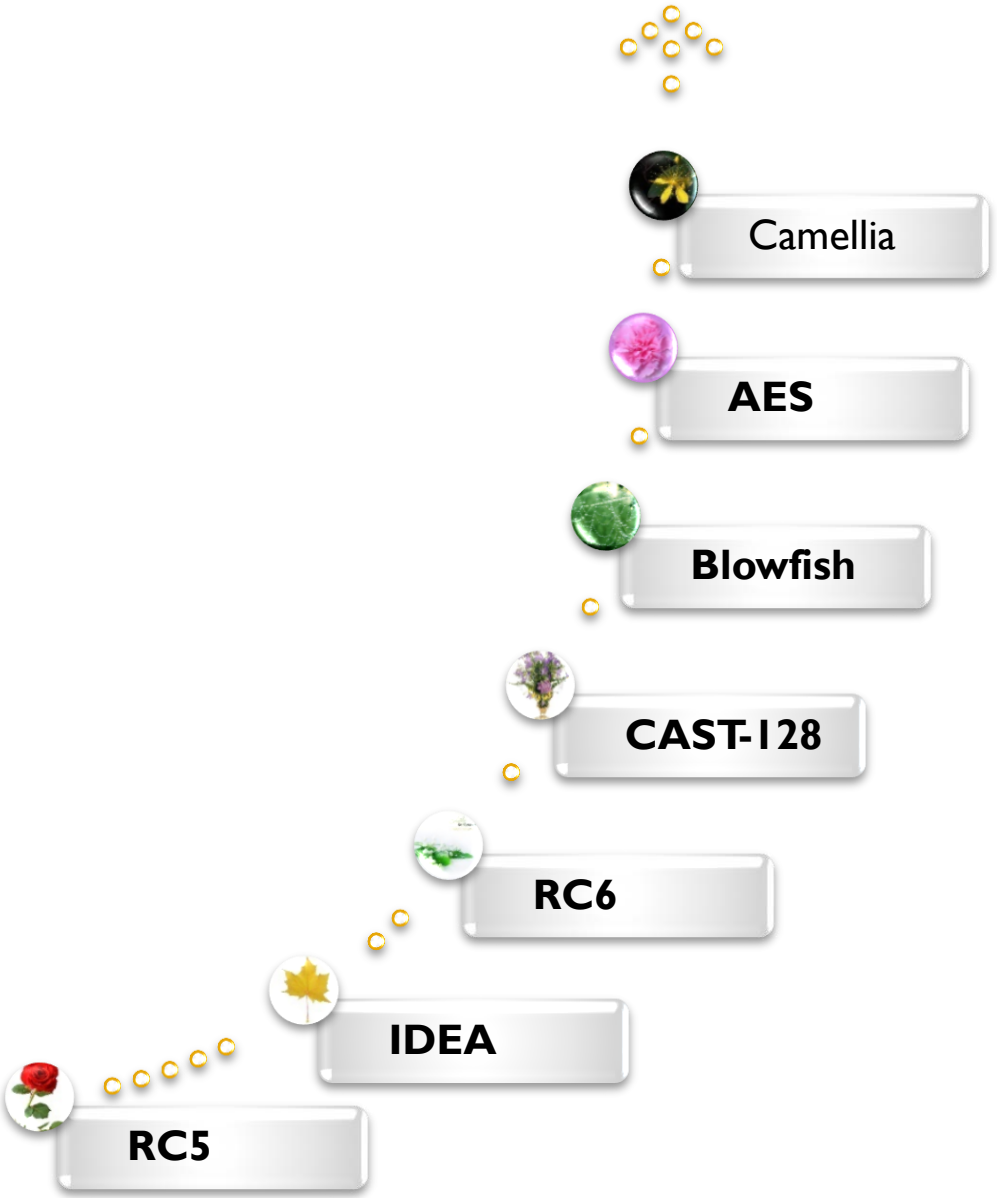
用途：数字签名，身份认证

举例：RSA, ElGamal, ECC

密码算法的分类-小结


Ciphers
Public Key
Symmetric Key
Unkeyed
PublicKey
Signature
ID
Random
OneWay
Hash
Random
Signature
MAC
Symmetric
Classical
Stream
Block
Permutation
Substitution

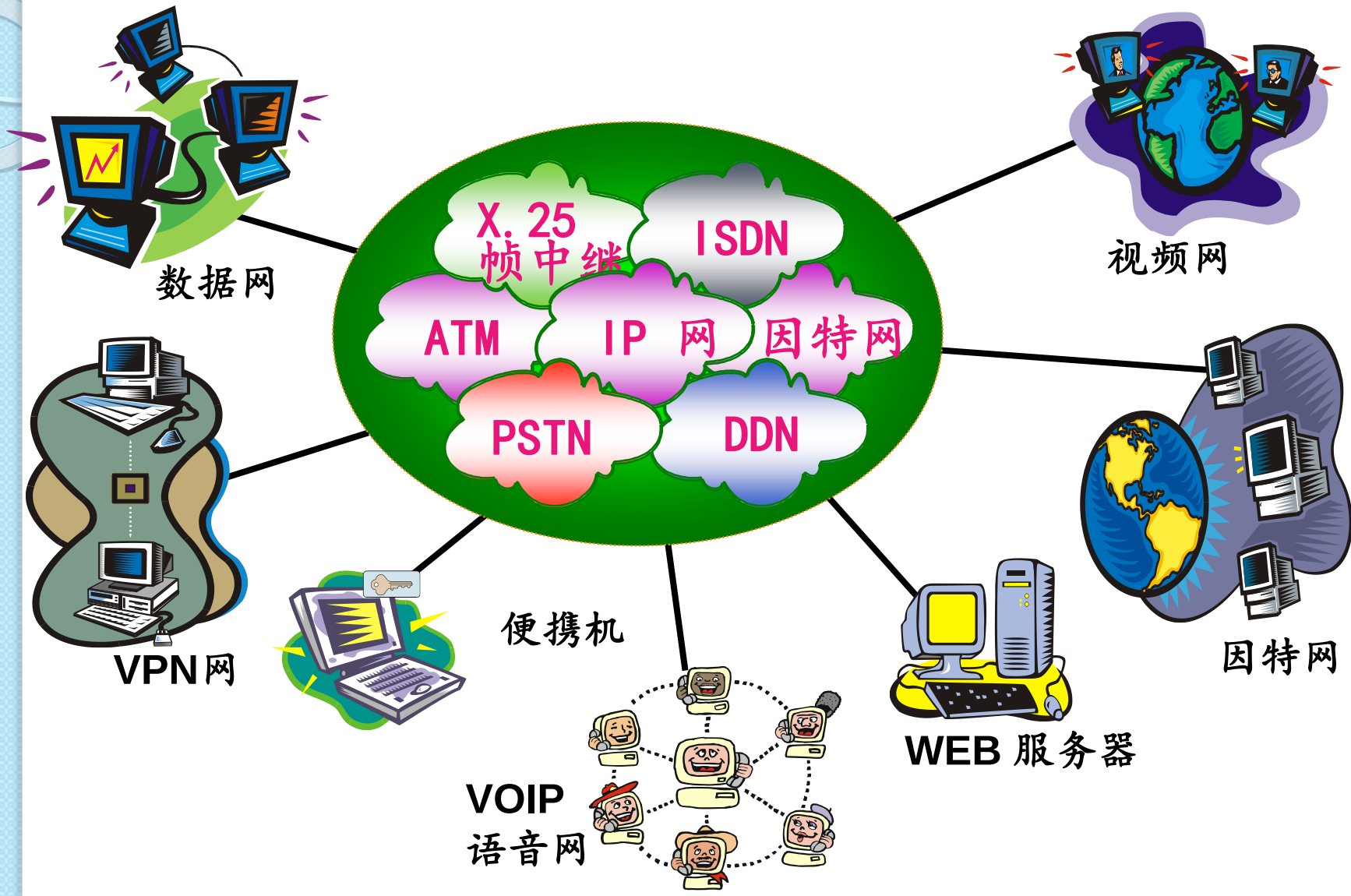
其他密码算法



算法的使用

- 企业网现状、互联需求、潜在的安全问题
- 链路加密与端--端加密
- 流量分析
- 通信网络中的加密覆盖范围
- 密码算法的使用

企业网的现状

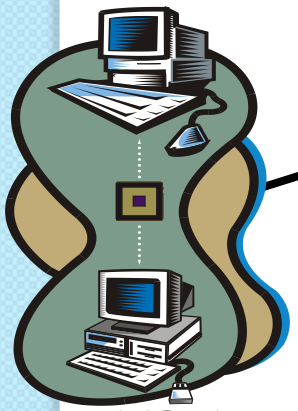

数据网
X.25
帧中继
ISDN
ATM
IP 网
因特网
PSTN
DDN
视频网
VPN网
便携机
因特网
VOIP
语音网
WEB 服务器

企业网互连需求

- 快捷，按需，廉价，安全可靠

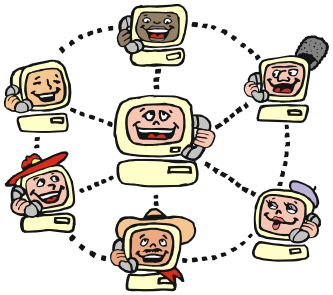
数据网

视频网



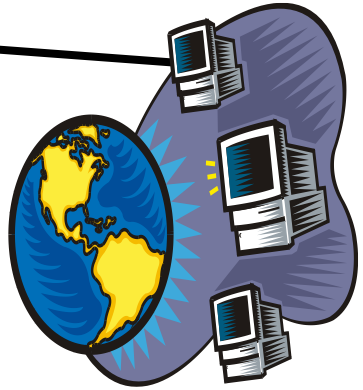
VPN网

便携机



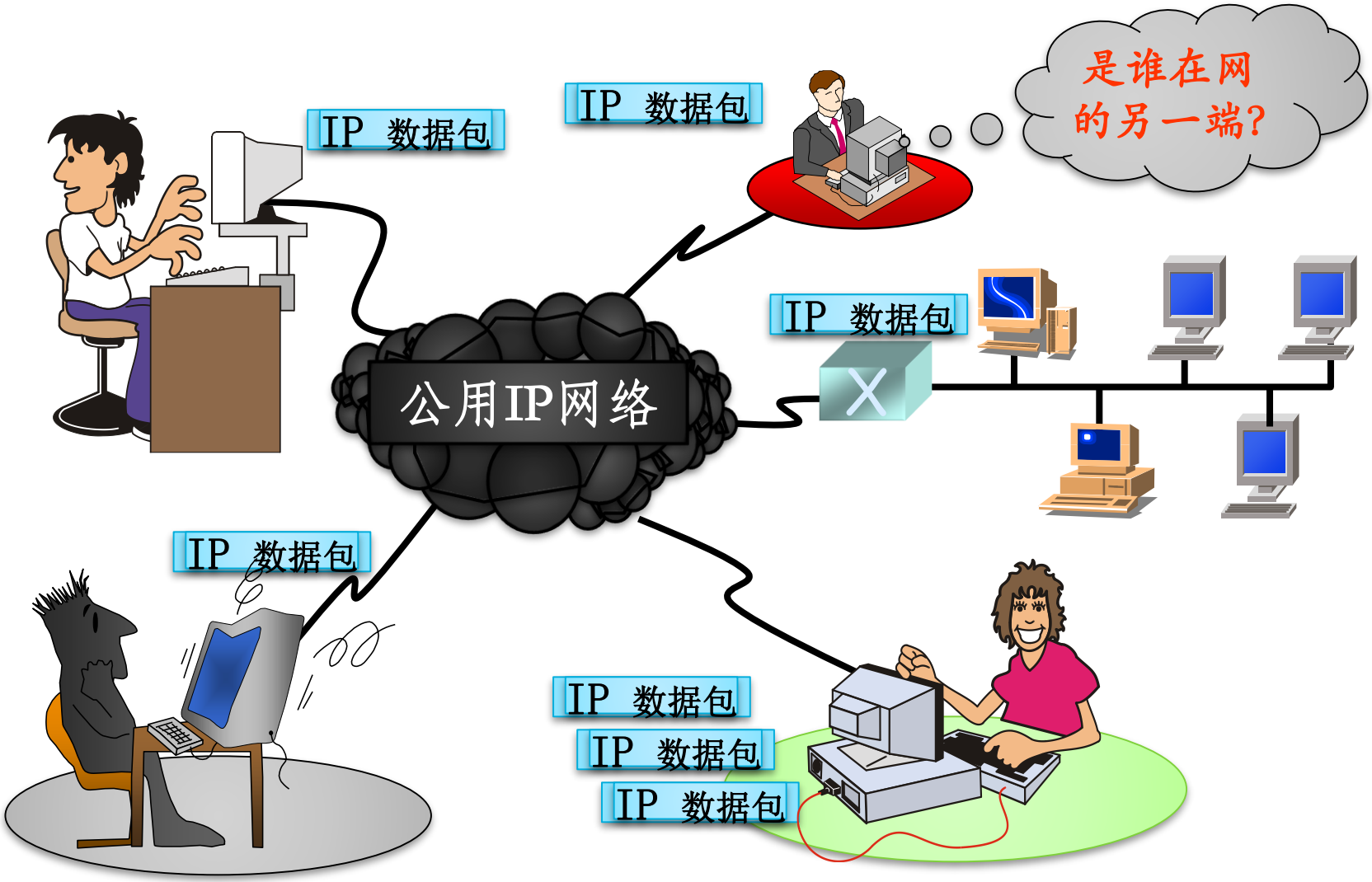
VOIP
语音网

WEB 服务器



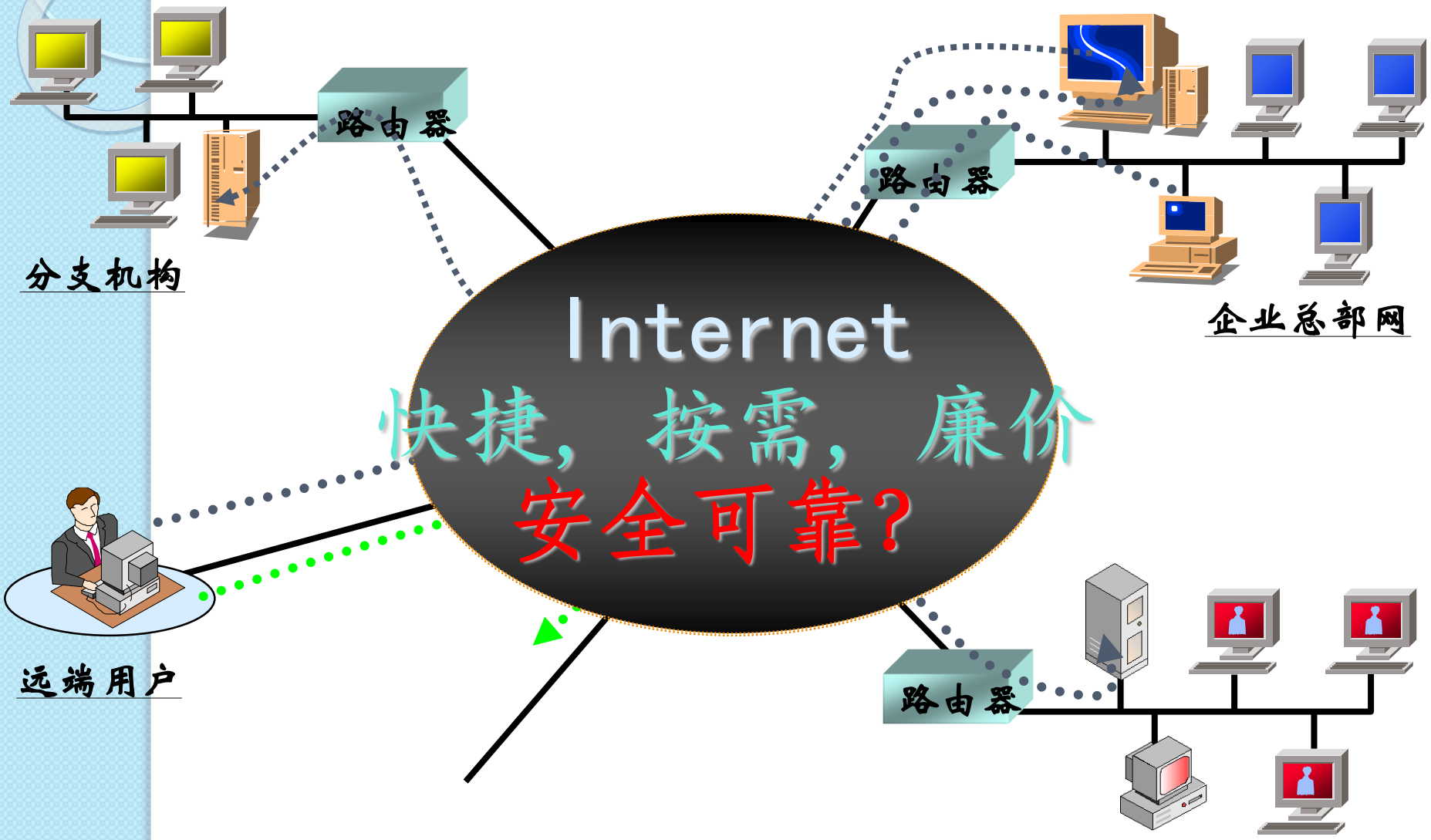
因特网

互联网潜在安全问题

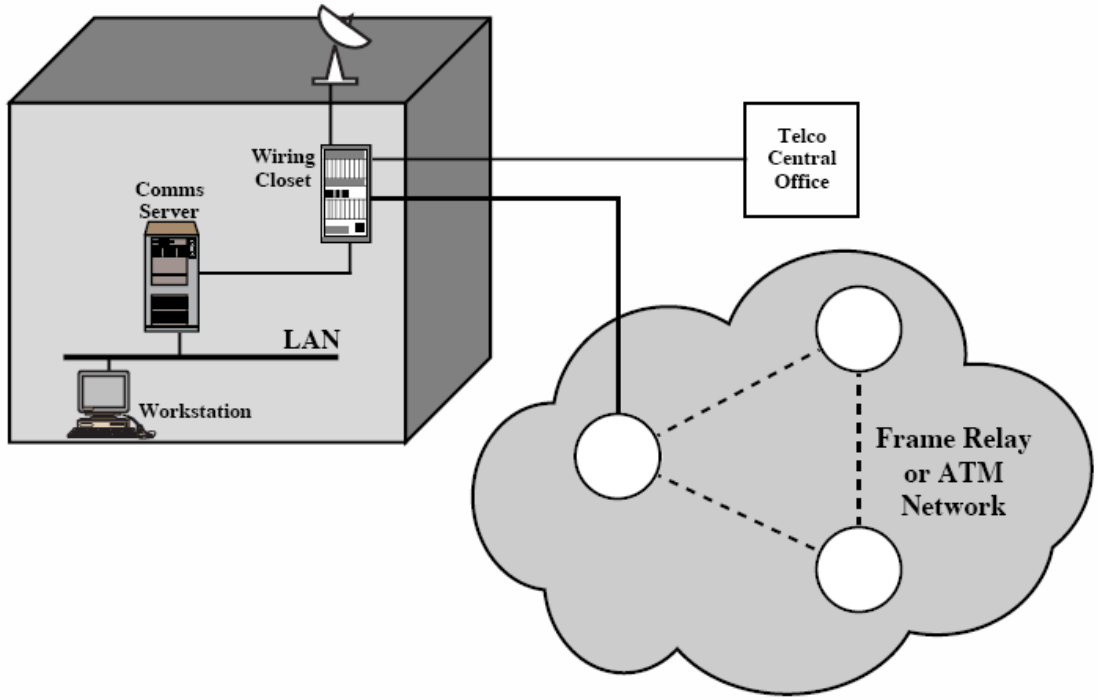


企业网互连的趋势之一

- 基于公用网的 VPN

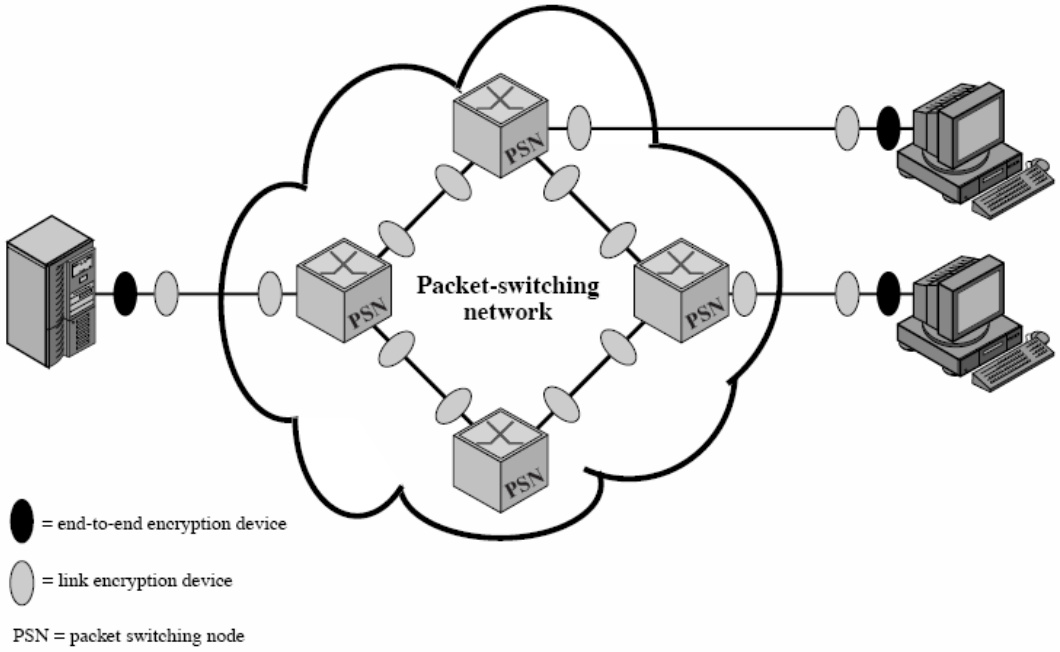


网络中的安全隐患



- 在同一局域网中发起的窃听
- 使用拨号或外部路由进入局域网进行窃听
- 嵌入配线室窃听
- 在外部链路上对通信业务的监听和修改

防御方法：链路加密与端-端加密



- 链路加密
  - 每个链接独立加密
  - 结点需要解密、加密操作，结点处消息为明文
  - 需要更多加/解密设备及成对的密钥
- 端到端加密
  - 在初始源与最终目的之间加密
  - 每个终端需要加/解密设备和共享密钥

流量分析

- 使用端到端加密时，须保留数据包头不加密，这样通信内容可以保护，通信流量信息无法保护
- 利用流量分析攻击，可获得：
  - 哪些通信实体参与了通信过程，身份、关系等
  - 通信双方的通信频率
  - 消息格式、长度、数量，推断是否有重要消息
  - 特定通信双方特定会话内容所涉及的事件
- 一种防御方法是，把所有数据单元都填充到一个统一的长度

多种方案的防御

- 端到端加密，并提供认证
- 链路加密保护数据包头信息
- 流量填充（traffic padding）保护数据流量信息
- 代价是？

加密的逻辑位置

- 网络协议层次结构：
  - OSI框架七层协议：物理层，数据链路层，网络层，传输层，会话层，表示层，应用层
  - TCP/IP协议：物理层，数据链路层，IP层，TCP层，应用层
- 在OSI模型中
  - 链路加密位于低层网络：物理层、链路层
  - 端到端加密位于高层网络：网络层、传输层、表示层、应用层

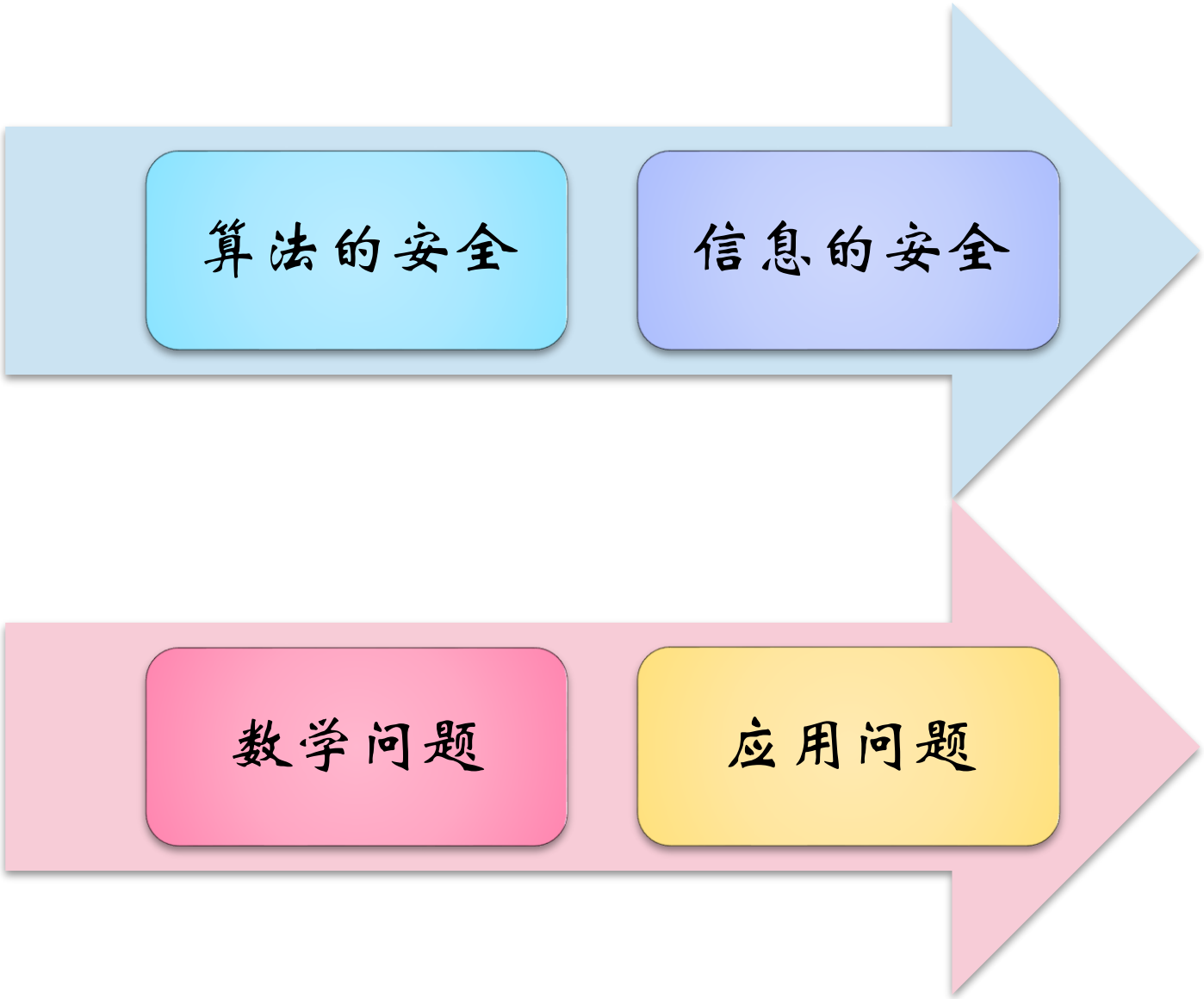
通信网络中的加密覆盖范围

- 将加密设备用于**低层**，如：网络层，TCP层，可以提供整个网络的端对端的安全性；不能用于网络之间的服务
- 将加密设备用于**高层**，如应用层，越高的层次，所需加密的信息越少，而安全性越高；但涉及的实体多，所需的密钥也多

密码算法的使用

- 使用目的
  - 保密（略）
  - 认证
  - 签名
- 方法：协议
- 协议的基本设计准则

密码算法的安全与信息安全



Bruce Schneier德国密码学家

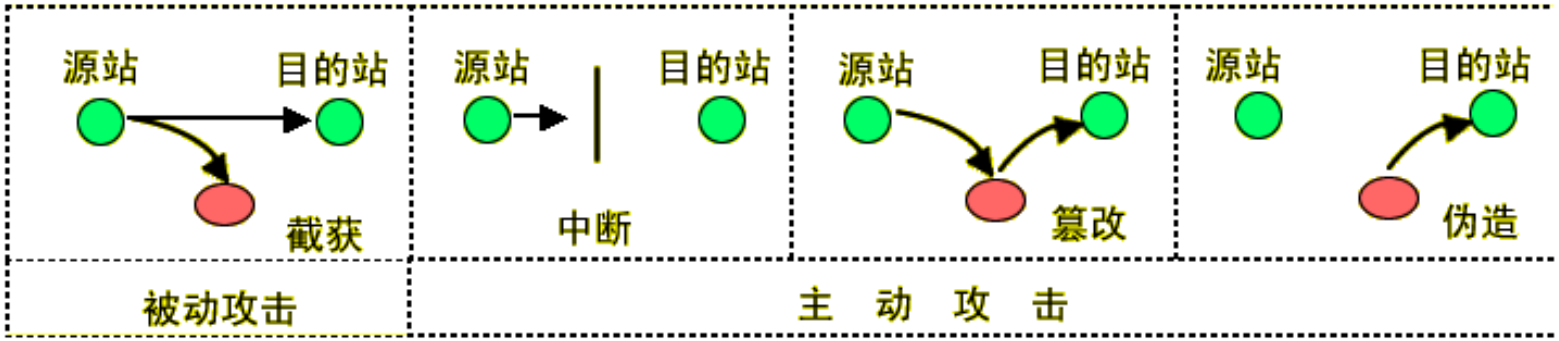
- 《Applied Cryptography: protocols, algorithms, and source code in C》1994年第一版，1996年第二版
- 主要认知：**算法安全的需求**
- 书中描述了一个数学的乌托邦：密码算法能将你最深的秘密保持数千年，安全协议能安全而可靠地执行最难以想象地电子交互，如不规则的赌博、不可检测的认证、匿名货币等。密码学是超凡的技术均衡器，任何人只要有一台便宜的计算机，就可以达到与最强大的政府同样的安全性。
- “仅靠法律保护自己还远远不够，还需要用数学保护我们自己”

Bruce Schneier德国密码学家

- 《Secrets and Lies: Digital Security in a Networked World》2000年HZ BOOKS出版
- 主要认知：**算法安全还不够**
  - “我写这本书，部分原因是为了纠正一个错误”，*密码学并不能做那么多的事情*
  - 密码学并非存在于真空之中：数学是完美的，而现实是主观的；数学是精确的，而计算机却充满矛盾；数学是遵循逻辑的，而人却是反复无常的、甚至是难以理解的；把密码学说成了灵丹妙药，我真的有些天真。
  - 安全性弱点与数学毫无关系：它们存在于硬件、软件、网络以及人身上；糟糕的编程、差的操作系统、不当的口令字选择

网络安全面临的问题

- 安全需求的扩展：密码学的新应用
- 主动攻击和被动攻击



网络安全含义

- 计算机网络通信安全的五个目标：
  - (1) 防止析出报文**内容**；
  - (2) 防止信息**流量**分析；
  - (3) 检测**更改**报文流；
  - (4) 检测**拒绝服务**；
  - (5) 检测伪造初始化连接——**冒充**。

信息安全的目标

- **保密性** (Confidentiality)
  - 保证信息被授权者享用而不会泄露给非授权的任何人
- **完整性** (Integrity)
  - 确认信息完整如初，历经空间或时间的变化而未经非授权的篡改或损坏
- **真实性** (Authentication)
  - 确认与信息关联的实体如其所声明一样是真实的
- **可用性** (Availability)
  - 保证信息和信息系统随时为授权者提供服务，而不出现非授权者滥用或对授权者拒绝服务的情况
- **可控性** (Controllability)
  - 保证管理者能够对信息实施必要的控制管理，以对抗社会犯罪和外敌侵犯
- **不可否认性** (Non-repudiation)
  - 保证信息行为人不能否认自己的行为，必要时可为依法管理提供所需的公证和仲裁等证据

如何达到信息安全目标

- 协议
- 利用密码算法
- 构造安全协议
  - 认证
  - 签名

协议

- 是两个或两个以上的参与者，为完成某项特定的任务而采取的一系列步骤
  - 包括两方或多方
  - 一系列步骤：是必须依次完成的序列
  - 目的是完成一项任务
- 协议执行的条件
  - 协议参与者都了解协议，预知所要完成的步骤
  - 协议参与者都同意并遵循
  - 协议本身是清楚的，每一步定义明确，不会引起误解
  - 协议本身是完整的，没种可能的情况都必须规定具体的动作

密码协议

- 是使用密码学的协议
- 例子：
  - 密钥协商协议
  - 密钥分配协议
  - 不经意传输协议
  - 认证协议
  - 盲签名协议
  - 电子商务协议

密码协议的种类

- 仲裁协议
  - 由仲裁者帮助互不信任的双方完成协议
- 裁决协议
  - 每次都要完成的非仲裁子协议
  - 有争议时才执行的裁决子协议
- 自动执行协议
  - 协议本身就保证了公平性

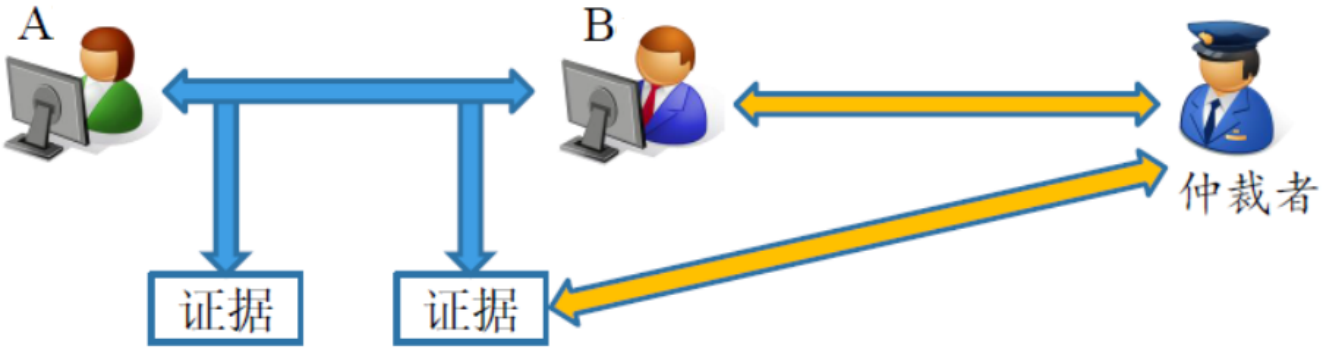
仲裁协议

- 仲裁者在协议中没有既得利益，与通信参与者没有利害关系
- 所有人都接受：
  - 仲裁者说的都是真实的
  - 仲裁者做的都是正确的
  - 仲裁者会忠实地完成协议中涉及他的部分

仲裁协议的问题

- 互相信任的双方，很容易找到仲裁者；互相怀疑的双方，很可能也怀疑仲裁者
- 仲裁者的劳务费
- 仲裁带来延迟
- 仲裁者需要处理每一次会话，成为网络瓶颈
- 破坏者更愿意攻击仲裁者

裁决协议



- 仲裁者不直接参与每一次会话
- 通信双方发生争议时，仲裁者才出场
- 仲裁协议是为了发现，而不是阻止欺骗

自动执行协议

- 是最好的协议
- 但，一般不存在这种协议

密码协议的安全性质

- 认证性
  - 确认身份，获取信任
- 保密性
  - 保护协议消息不泄露给非授权人
- 完整性
  - 保护协议消息不被非法篡改、删除或替代
- 非否认性
  - 收集参与协议人的证据，使其不可否认

对密码协议的攻击

- 攻击目标通常有三个：
  - 协议中采用的**密码算法**
  - **实现**该算法和协议的密码技术
  - **协议本身**
    - ✓被动攻击：
      - 窃听
    - ✓主动攻击：
      - 中间人攻击、重放攻击、类型攻击、交织攻击、与实现相关的攻击、绑定攻击、封装攻击
      - 局外人，或协议参与者（骗子）
      - 窃取信息、欺骗、阻碍合法使用

对密码协议的主动攻击

- 重放攻击：
  - 捕获过往协议或当前协议中的消息，在当前协议中重播
    - ✓获取非法权限、伪造密钥等等
  - 防止方法：添加nonce、时间戳，不同阶段的消息在结构上不对称（例如前面用{A,msg}，后面用{msg,A}）
- 类型攻击：
  - 协议双方对消息成分的位序列有不同的解释
    - ✓例如：密钥和随机数nonce都是随机比特串，攻击者可能把加密的密钥挪到加密的nonce的位置，诱使协议方将密钥误认为nonce而公布出来
  - 防止方法：协议中不同成分采用不同的形式

对密码协议的主动攻击

- 交织攻击：
  - 同时运行多次协议，将其中某些的消息用于形成另一次运行中的消息。
    - ✓ 目前没有非常有效的防止方法
- 与实现相关的攻击：
  - 与实现时具体采用的技术有关
    - ✓ 例如：A→B: $E_k(N)$；B→A: $E_k(N-1)$
    - ✓ 如果采用按位加密算法，且N碰巧是奇数（末位为1），则$E_k(N)$与$E_k(N-1)$的差别仅仅是末位相反，因而可攻击
  - 防止方法：选择合适的密码算法和密码体制

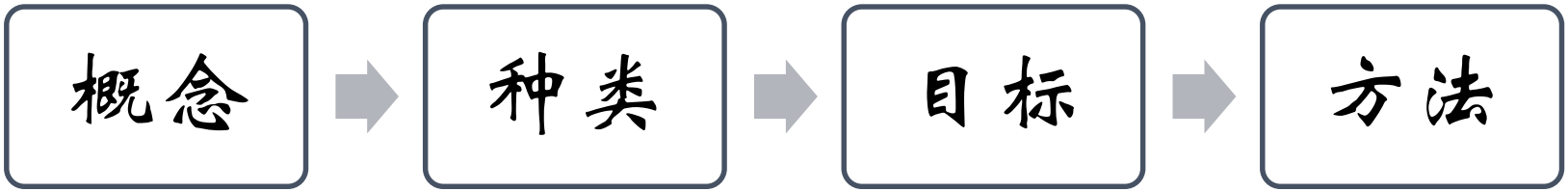
对密码协议的主动攻击

- 绑定攻击
  - 假冒身份/公钥
  - 防止方法：在消息中添加主体的身份信息，并签名
- 封装攻击
  - 攻击者做为协议参与一方，将它所需要的消息封装为合法消息的一部分，诱使另一方解密、签名等
  - 防止方法：添加完整性校验

设计密码协议的注意事项

- 最少的安全假设
- 用一次性随机数代替时间戳
  - 回避时钟同步
- 具备抵抗常见攻击的能力
- 明确用于网络结构的哪个协议层
- 明确所需的数据处理能力
- 明确所采用的密码算法
- 便于进行功能扩充

认证



认证的概念

- 是证实信息交换过程有效性和合法性的一种手段
- 认证的目的
  - 防窃听、防假冒或拦截、防窃取、防重放等
- 认证的内容：包括对通信对象的认证(身份认证)和报文内容的认证(报文认证)，起到数据完整性的保护
  - 信息的真实性
  - 存储数据的真实性
  - 接收方提供回执
  - 发送方不可否认
  - 时效性和公证可能性

认证的种类

- 两种
- 消息认证（也称报文认证，MDC、MAC、数字签名）
  - 在产生消息时进行
  - 涉及的是特定实体所声称的特定消息
- 身份认证（也称实体认证）
  - 在协议执行时进行
  - 通常涉及的是特定实体所具有某些信息，而非传递的消息

身份认证

- 主要内容
  - 识别：明确访问者身份
  - 验证：确认访问者声称的身份，依据：
    - ✓ 已知事物：口令（或密钥）、个人识别码（PIN）、在挑战－相应协议中被证实的秘密或私钥
    - ✓ 已拥有的事物：磁卡、IC卡、智能卡、口令生成器
    - ✓ 固有事物：生物特征（指纹、唇纹、虹膜）、下意识行为（笔迹）
- 主要研究身份认证
  - 确认通信各方身份，并交换会话密钥（需要的话）
  - 单向认证或相互认证
  - 关键问题：
    - ✓ 及时性——防止重放攻击
    - ✓ 机密性——保护会话密钥

身份认证协议的设计目标

- 1.A向B认证自己，即完成协议后B认可A的身份；
- 2.（不可传递性）B不能利用和A身份认证过程的数据，向第三方C假冒A；
- 3.（不可假冒）任何不同于A的实体C，假冒A执行协议，使得B完成协议并接受A的身份的概率可忽略不计；
- 4.上述3点恒为真，即使
  - 敌手C观察到大量A和B之间的认证
  - 敌手C参与了A和B中一方或双方的身份认证协议的执行
  - 敌手C可以发起并行攻击，同时运行多个实例

身份认证协议的性能

- 身份认证的交互性：
  - 相互认证
  - 单向认证
  - 可信中继
  - 群认证
- 计算效率：执行协议所需要的操作数
- 通信效率：传输的步数和需要的带宽或总传输量
- 第三方（若有）是否需要实时参与
- 第三方（若有）所需要的可信性
- 安全保证性：认证信息不被泄漏
- 秘密存储：存储关键密钥材料的位置和方法

身份认证的方法

- 口令认证（弱认证）
- 挑战--响应身份认证（强认证）
- 零知识的身份认证

口令(弱认证)

- 口令：用户与系统共享的秘密
  - 传统的口令方案归类为单向认证
- 须防御的威胁
  - 重放、泄漏（系统外）和搭线窃听（系统内）
  - 强力搜索
  - 猜测
  - 字典攻击

固定口令方案要素

- 存储的口令文件：明文存储，读写保护
- 加密的口令文件：存储口令的单向函数值
- 口令规则：口令的长度、字符集
- 口令时效
- 放慢口令映射：迭代运算，不影响正常使用下增加试探口令的攻击时间
- 口令加盐（salt）：降低字典攻击的效率，防止口令重复
  - 口令的散列值和盐值均记录在文件中
- 通行短语

消息认证

- 是证实某事是否名副其实，或是否有效的过程
- 消息认证与消息加密的区别：
  - 加密用以确保数据的保密性，阻止对手的被动攻击，如截取、窃听
  - 认证用以确保报文发送者和接受者的真实性以及报文的完整性，阻止对手的主动攻击，如冒充、篡改、重播等
- 认证往往是应用系统中安全保护的第一道防线，极为重要，消息认证也是如此。

消息认证

- 内容的认证
  - 通过计算校验和，或者报文摘要的方法实现
- 源的认证
  - 判定发送者的真实身份
  - 依据：
    - ✓ 共享数据（加密密钥）
    - ✓ 通行字（口令）
    - ✓ 网络地址
- 时间性认证
  - 时间戳加密
  - 报文按时间顺序编号
  - 预约报文通行字表
  - 使用标识符

消息认证的目标

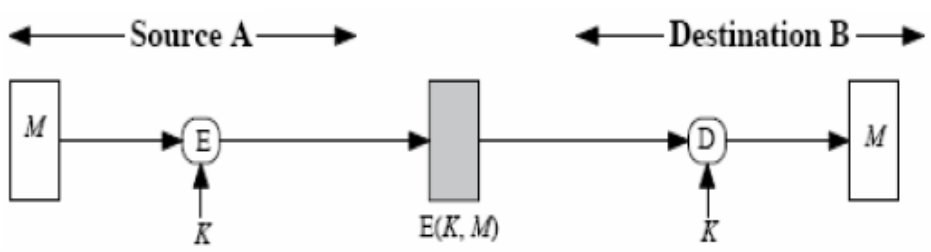
- 信息来源的
  - **可信性**，即信息接收者能够确认所获得的信息不是由冒充者所发出的；
  - **完整性**。信息接收者能够确认所获得的信息在传输过程中没有被修改、延迟和替换；
  - **不可抵赖性**。信息的发送方或接收方不能否认自己所发出或已收到了的信息；
  - **访问控制**。拒绝非法用户访问系统资源，合法用户只能访问系统授权和指定的资源。

消息认证的方法

- 三种
  - 加密
  - 消息认证码message authentication code (MAC)，帧校验码(FCS)
  - Hash

加密

- 消息加密本身能够提供一定的认证功能
- 使用对称密钥：
  - 发报人身份确认：仅有收发双方拥有密钥
  - 报文完整性确认：当报文中有足够的格式信息、冗余或校验时，修改密文会破坏这些信息
- 使用公钥密码：
  - 公钥加密提供报文保密性确认，不能提供身份确认：任何人都可以拥有公钥
  - 私钥签名提供信源身份确认，不提供保密性：也需要报文具有特定格式、冗余或校验



(a) Symmetric encryption: confidentiality and authentication

A → B: E(*K*, *M*)
- Provides confidentiality
  - Only A and B share *K*
- Provides a degree of authentication
  - Could come only from A
  - Has not been altered in transit
  - Requires some formatting/redundancy
- Does not provide signature
  - Receiver could forge message
  - Sender could deny message

(a) Symmetric encryption

(b) Public-key encryption: confidentiality

A → B: E(PU_b, *M*)
- Provides confidentiality
  - Only B has PR_b to decrypt
- Provides no authentication
  - Any party could use PU_b to encrypt message and claim to be A

(b) Public-key (asymmetric) encryption: confidentiality

(c) Public-key encryption: authentication and signature

A → B: E(PR_a, *M*)
- Provides authentication and signature
  - Only A has PR_a to encrypt
  - Has not been altered in transit
  - Requires some formatting/redundancy
  - Any party can use PU_a to verify signature

(c) Public-key encryption: authentication and signature

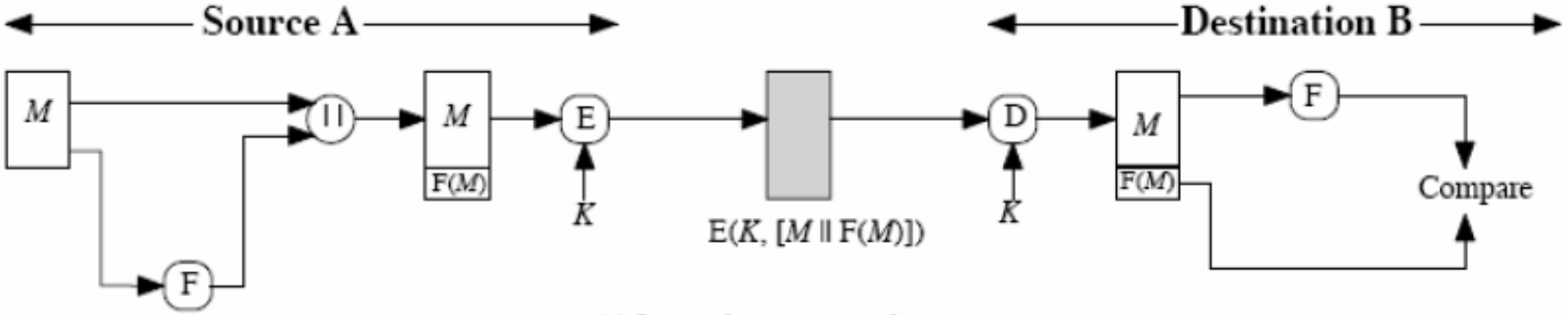
(d) Public-key encryption: confidentiality, authentication, and signature

A → B: E(PU_b, E(PR_a, *M*))
- Provides confidentiality because of PU_b
- Provides authentication and signature because of PR_a

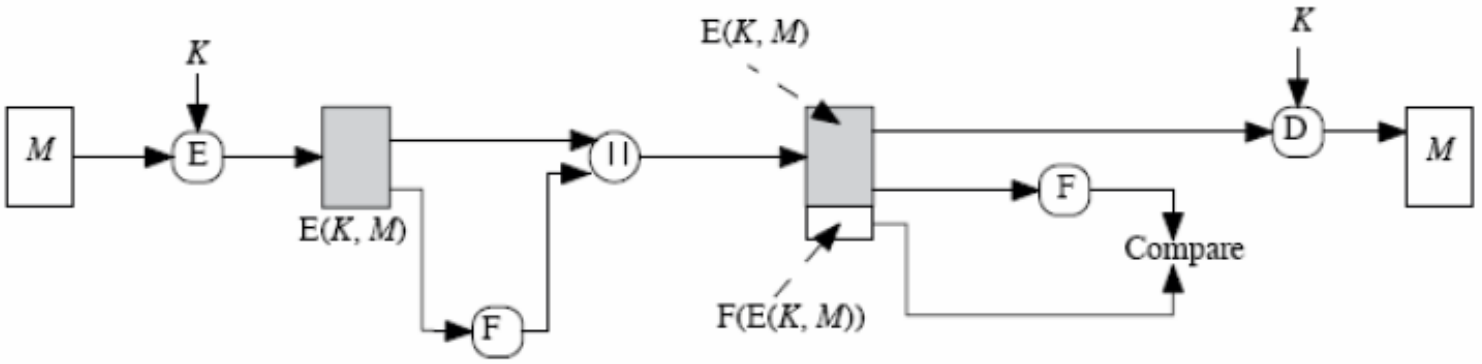
(d) Public-key encryption: confidentiality, authentication, and signature

帧校验码(FCS)

- 用来提供特定结构，确保密文不被篡改
- FCS和加密函数的顺序，是关键



(a) Internal error control



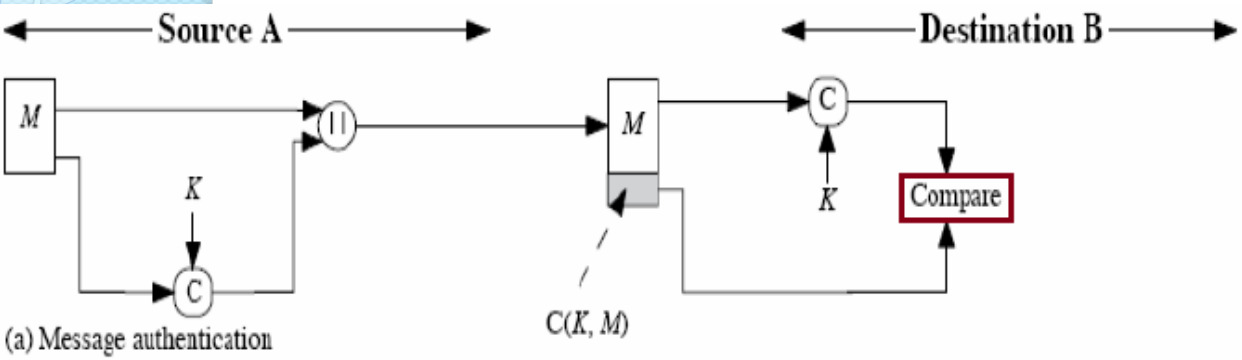
(b) External error control

消息认证码MAC

- 使用密钥产生短小的定长数据分组，即所谓的密码校验MAC，将它附加在报文中
- 通信双方共享密钥k，发送方计算$MAC=C_k(m)$并附在报文后。接收方根据m重新计算MAC，并与接收到的MAC比较。若密钥不公开且MAC匹配，则：
  - 接收方可以确信报文未被更改；
  - 接收方可以确信报文来自声称的发送者。
  - MAC函数类似加密，但非加密，也无需可逆
  - 报文鉴别不提供保密
  - 常将MAC直接与明文并置，然后加密传输

- MAC的性质
  - MAC是一种密码校验和：$MAC = C_k(m)$
  - 用于对可变长消息m编写摘要
  - 使用密钥k
  - 产生一个定长的认证码
- 显然，MAC是多对一的映射
  - 多个消息可能具有相同的MAC
  - 但根据指定MAC构造消息很难

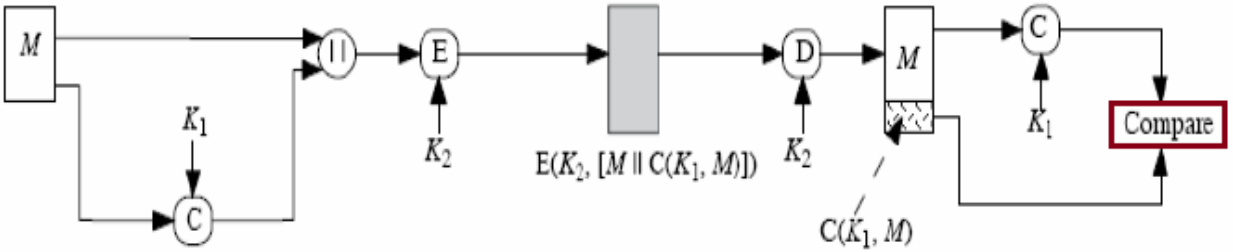
MAC的基本使用方式



(a) Message authentication

$A \rightarrow B: M \| C(K, M)$
- Provides authentication
  - Only A and B share K

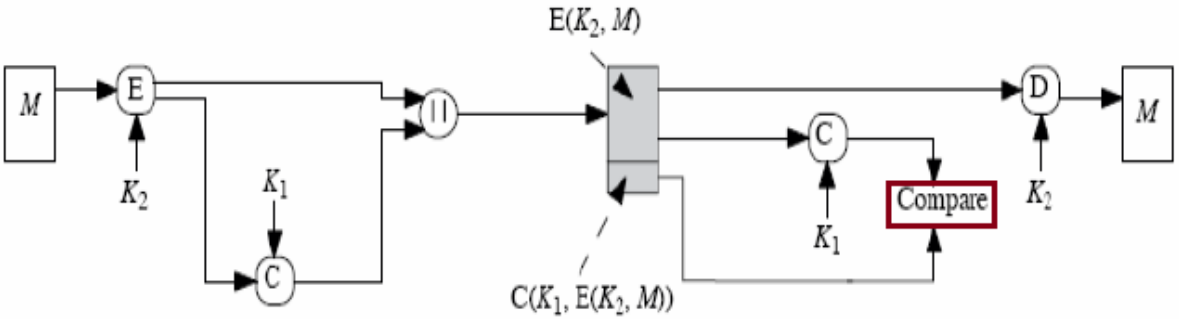
(a) Message authentication



(b) Message authentication and confidentiality; authentication tied to plaintext

$A \rightarrow B: E(K_2, [M \| C(K, M)])$
- Provides authentication
  - Only A and B share K_1
- Provides confidentiality
  - Only A and B share K_2

(b) Message authentication and confidentiality: authentication tied to plaintext



(c) Message authentication and confidentiality; authentication tied to ciphertext

$A \rightarrow B: E(K_2, M) \| C(K_1, E(K_2, M))$
- Provides authentication
  - Using K_1
- Provides confidentiality
  - Using K_2

(c) Message authentication and confidentiality: authentication tied to ciphertext

MAC的应用场合

- 对称加密同时提供保密和认证，为什么还要用只提供认证的MAC？
  - 将一条非秘密消息广播给很多人时——不需要加密，也不需要每个人都做认证
  - 信息传输速度过快，没时间逐个解密——可以随机选择认证
  - 计算机程序的防篡改——每次运行都解密是很麻烦的
  - 用户不希望做认证的人/机构得到明文——不让外人解密
  - 认证和保密性的分开，有利于系统的层次化设计

对MAC的要求

- 应考虑对MAC函数的各种类型的攻击
- 当密钥k保密时，MAC函数应满足：
  - 1.已知消息和MAC值，构造另一个具有相同MAC值的消息在计算上不可行的
  - 2.MAC值应当均匀分布：抗基于选择明文的穷举攻击
  - 3.MAC函数应当等概地使用消息的所有比特位

对MAC的攻击

- 穷举攻击
  - 若密钥长度(k)大于MAC长度(n)
    - ✓对消息m1及对应MAC1尝试密钥，平均会有2k-n个匹配密钥
    - ✓对消息m2及对应MAC2尝试上面得到的密钥，平均会有2k-2n个匹配密钥
    - ✓重复下去，直到得到唯一密钥
  - 若密钥长度(k)小于MAC长度(n)
    - ✓很可能第一次尝试就得到唯一密钥
- 消息构造攻击
  - MAC必须仔细设计

数字证书

- 是标志网络用户身份信息的数据，用于证明某一主体（如个人用户、服务器等）的身份以及其公钥的合法性的一种权威性的电子文档，由权威公正的第三方机构，即CA中心签发
- 拥有者可以将其提供给其他人、Web站点及网络资源，以证实其身份，并且与对方建立加密的、可信的通信
- 以数字证书为核心的加密技术，可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及交易实体身份的真实性，签名信息的不可否认性，从而保障网络应用的安全性
- 数字证书的内部格式遵循X.509标准

数字摘要

- 又称为数字指纹，将任意长度的消息变成固定长度的消息，使用 Hash函数
- 应用

数字摘要的使用过程 —数字签名

发送方：

①对原始明文使用Hash运算得到数字摘要

②将数字摘要与原文一起发送

接收方：

①将收到的原文应用Hash函数产生新的数字摘要

②将新的数字摘要，与发送方发来的数字摘要进行比较：若两者相同则表明原文在传输中没有被修改，否则原文被修改过。

下次内容

- 密钥管理