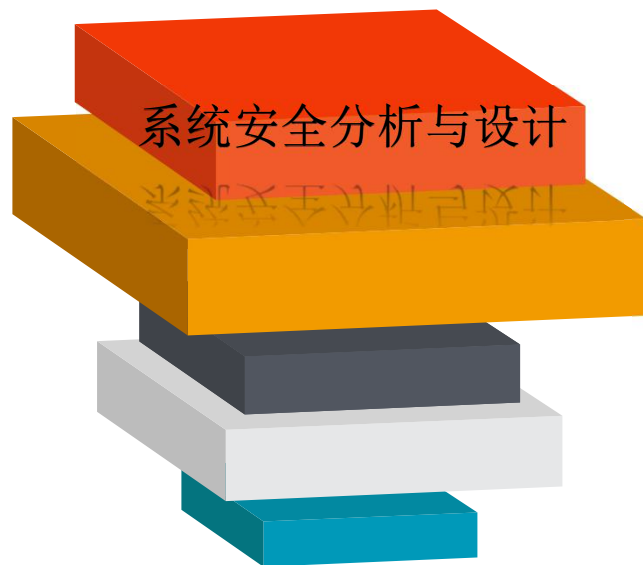




系统架构设计师

DESIGNER: 王川林
系统安全分析与设计





安全基础技术

网络安全

计算机病毒与木马 ★

对称非对称加密 ★★★★★
数字签名 ★★★★★
信息摘要 ★★★★★

安全协议 ★★★★★
防火墙 ★★★★★
入侵检测 ★★★★★

软考教育：帮助客户成功
，创造社会价值

加密



密钥

&@#^&@S&*!@^#*
'!&@#*!@^S*!^@*#^
!@*S^!@*^@!#*^

解密



密钥

软考教育：帮助客户成功
，创造社会价值

缺陷：1.加密强度不高，但效率高。
2.密钥分发困难

常见对称密钥加密算法：

DES： 替换+位移、56位密钥、64位数据块、速度快、密钥易产生

3DES（三重DES）： 两个56位的密钥K1、K2

加密： K1加密→K2解密→K1加密

解密： K1解密→K2加密→K1解密

RC-5： RSA数据安全公司的很多产品都使用了RC-5

IDE算法： 128位密钥、64位数据块、比DES的加密性好、对计算机功能要求相对低，PGP。



软考教育：帮助客户成功
，创造社会价值

加密



公钥

&@#^&@S&*!@^#*
'!&@#*!@^S*!^@*#^
!@*S^!@*^@!#*^

解密



私钥

软考教育：帮助客户成功
，创造社会价值

常见非对称密钥加密算法：RSA：512位（或1024位）密钥、计算量极大、难破解
ECC：椭圆曲线算法

缺陷：加密速度慢

单向散列函数、固定长度的散列值。

信息摘要

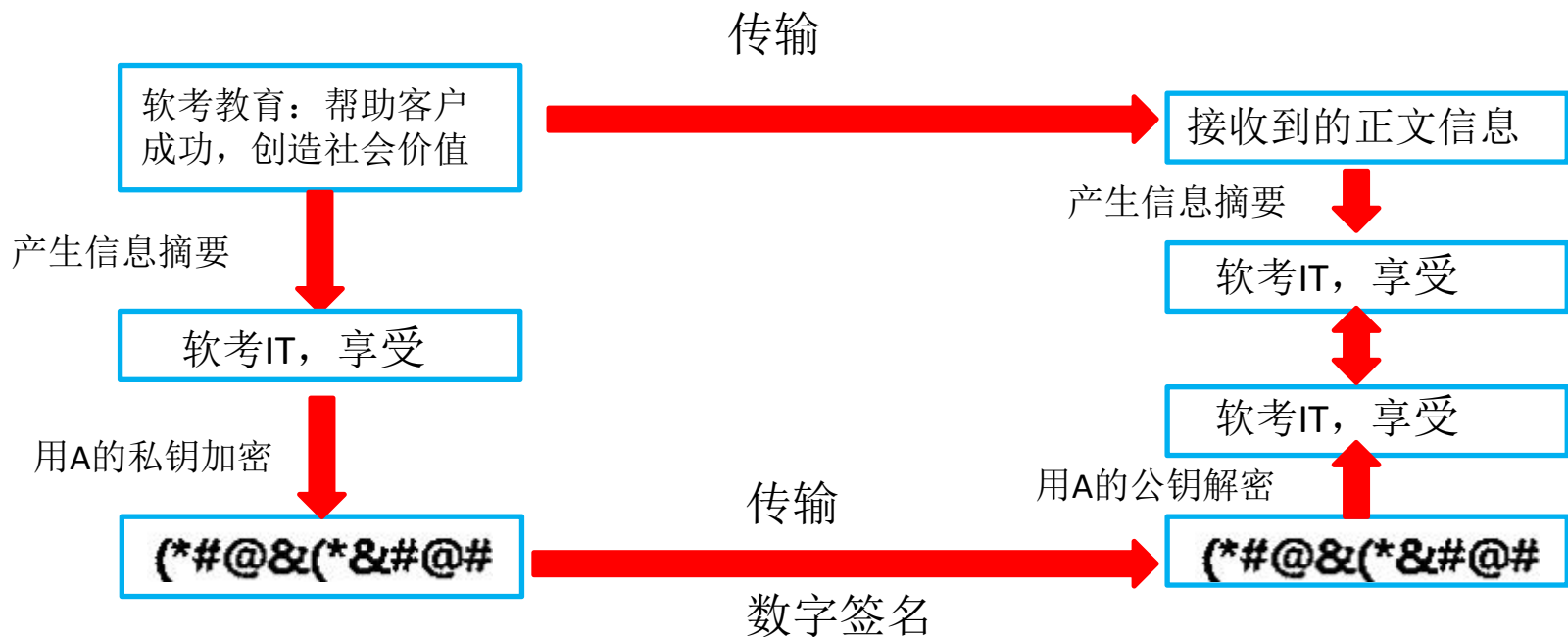
软考教育:IT在线教育平台,
让每个人随时随地享受IT教育

产生信息摘要



%%&^#@(*&(@

常用的消息摘要算法有MD5, SHA等, 市场上广泛使用的MD5, SHA算法的散列值分别为128和160位, 由于SHA通常采用的密钥长度较长, 因此安全性高于MD5。



请依据已学习的加密技术，以及信息摘要，数字签名解决以下问题：

请设计一个安全邮件传输系统，要求：

该邮件以加密方式传输，邮件最大附件内容可达到500MB，发送者不可抵赖，若邮件被第三方截获，第三方无法篡改。



该邮件以加密方式传输，邮件最大附件内容可达500MB，发送者不可抵赖，若邮件被第三方截获，第三方无法篡改。

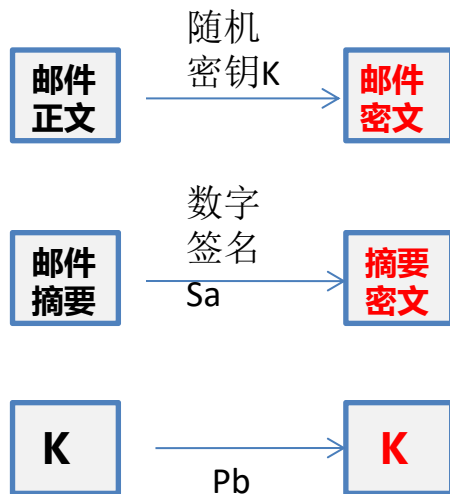
加密解密技术

对称加密

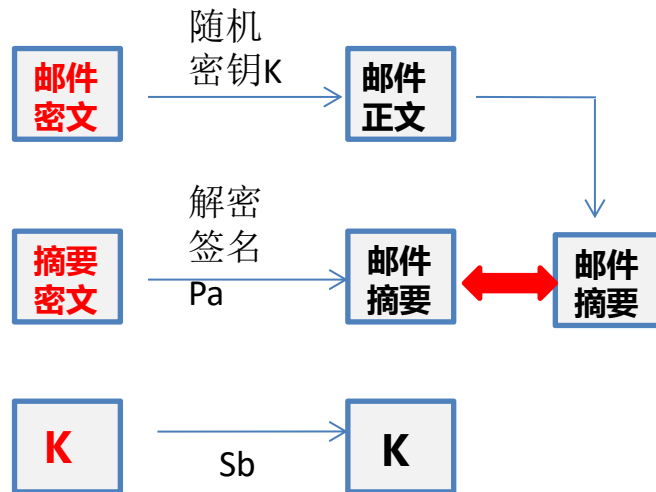
数字签名

信息摘要技术

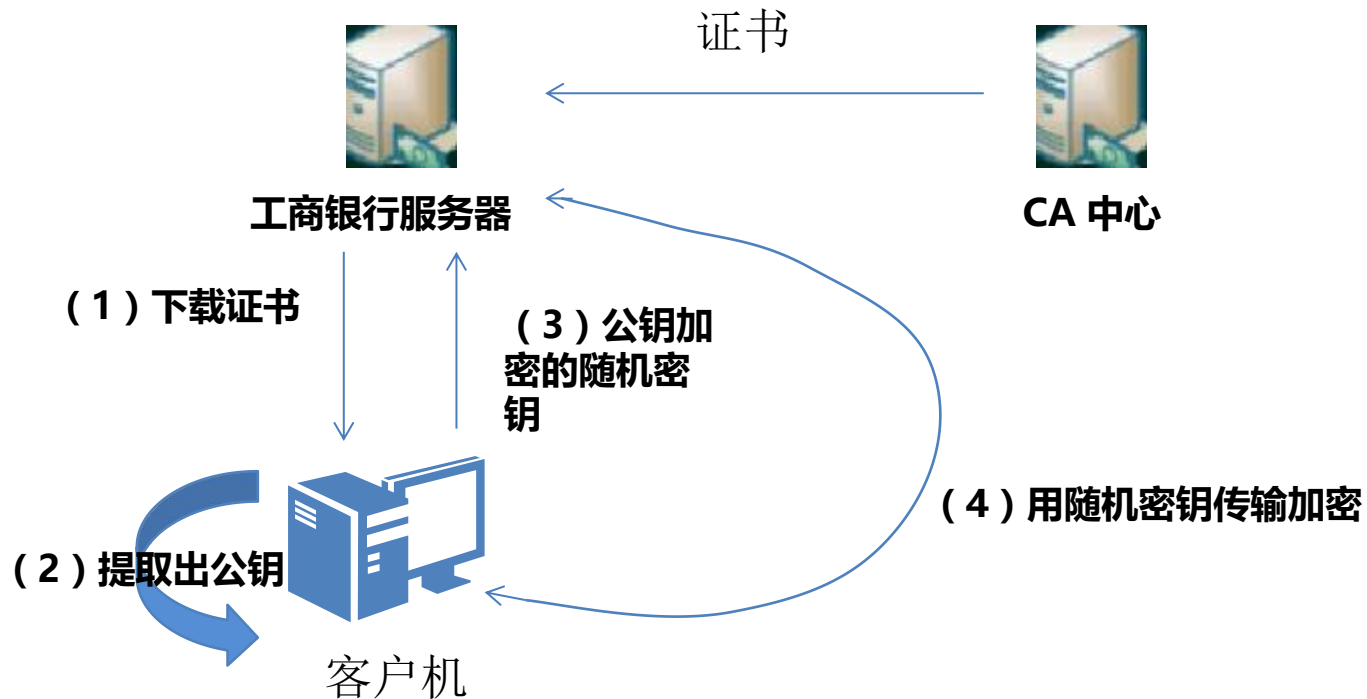
发送方A（公钥：Pa，私钥：Sa）：



接收方B（公钥：Pb，私钥：Sb）：



钓鱼网址何意？

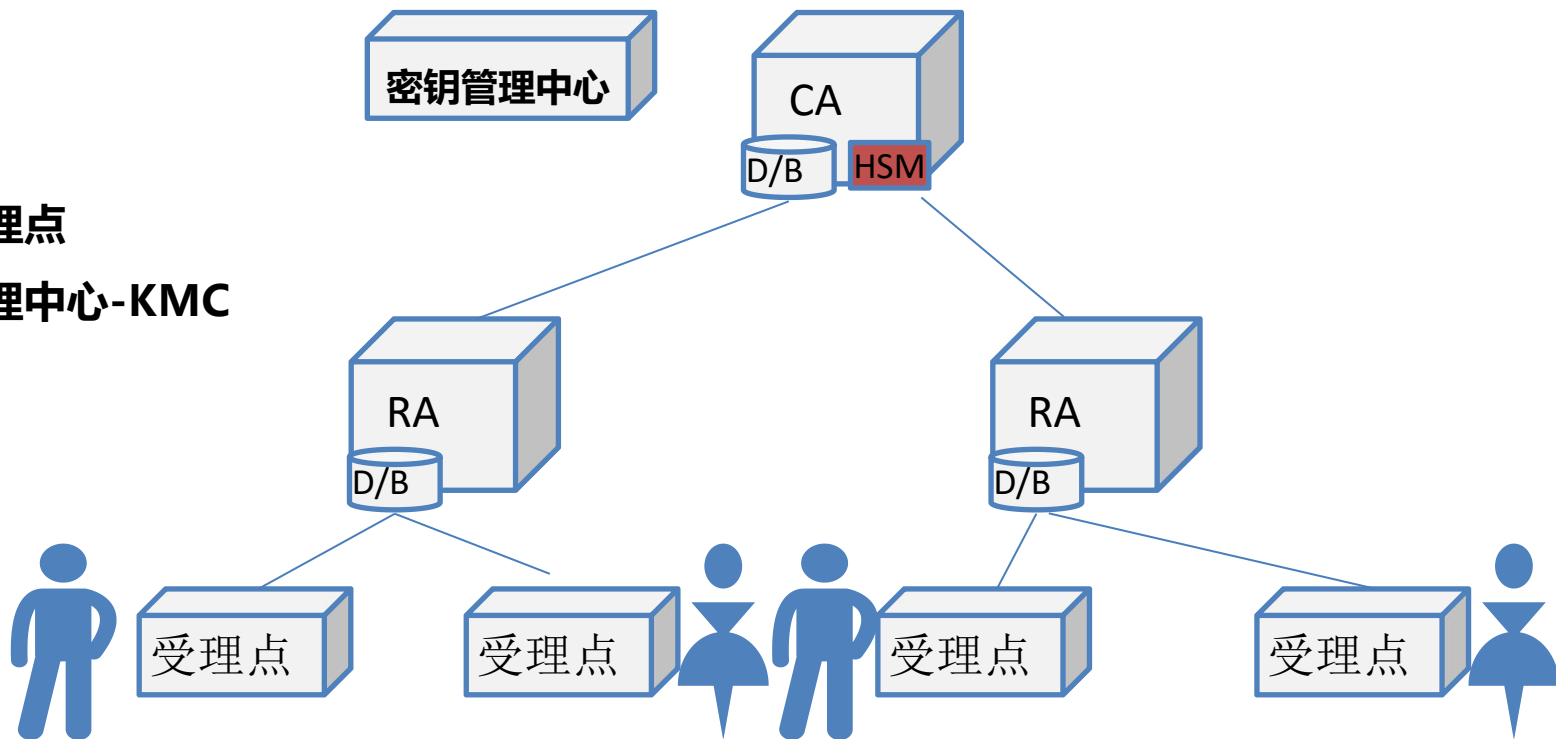


CA

RA

证书受理点

密钥管理中心-KMC



X.509数字证书内容

证书的版本信息；

证书的序列号，每个证书都有一个唯一的证书序列号；

证书所使用的签名算法；

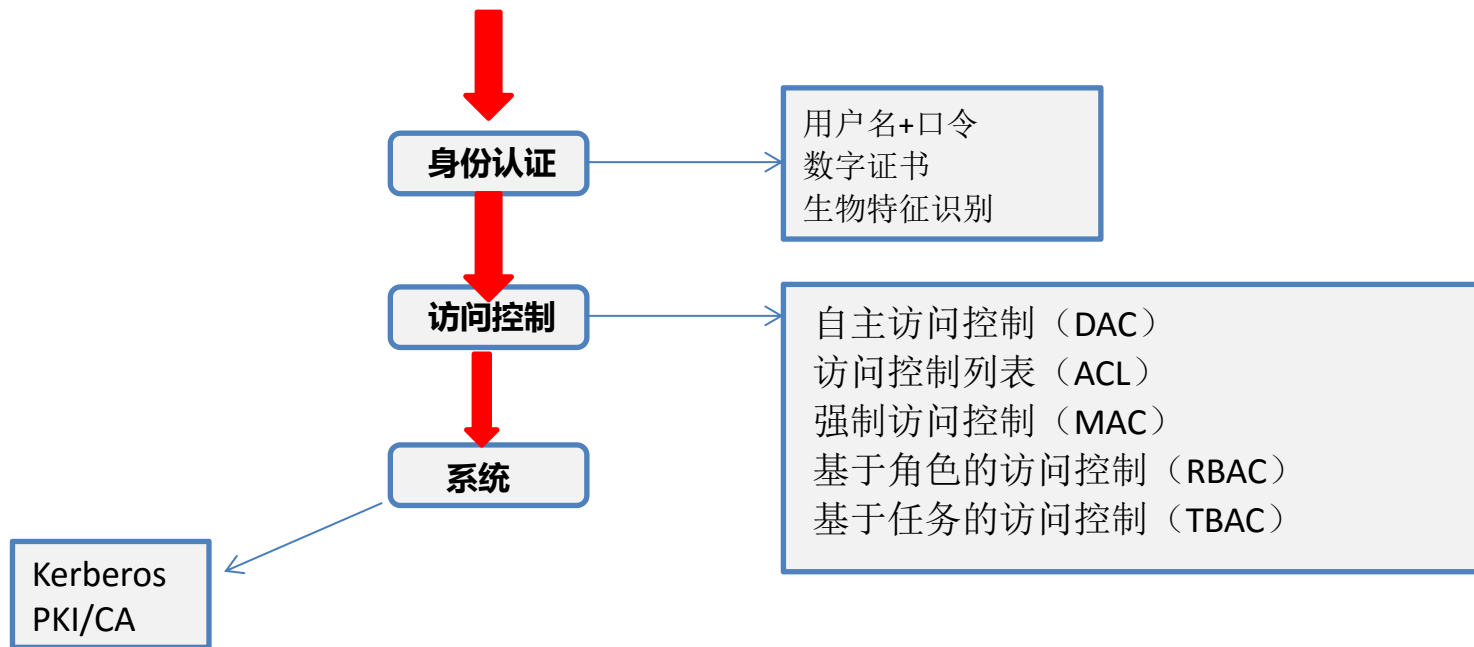
证书的发行机构名称，命名规则一般采用X.500格式；

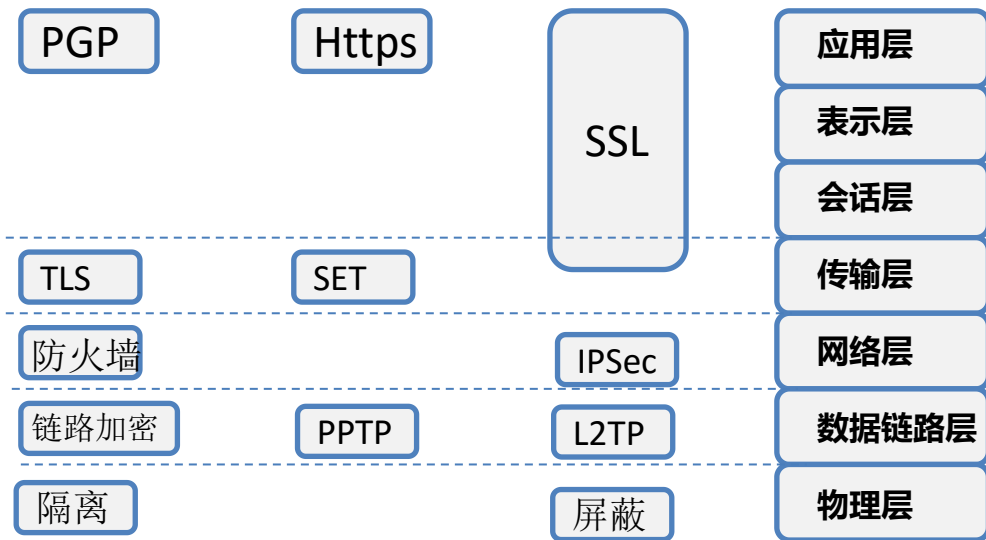
证书的有效期，现在通用的证书一般采用UTC时间格式，它的计时范围为1950-2049；

证书所有人的名称，命名规则一般采用X.500格式；

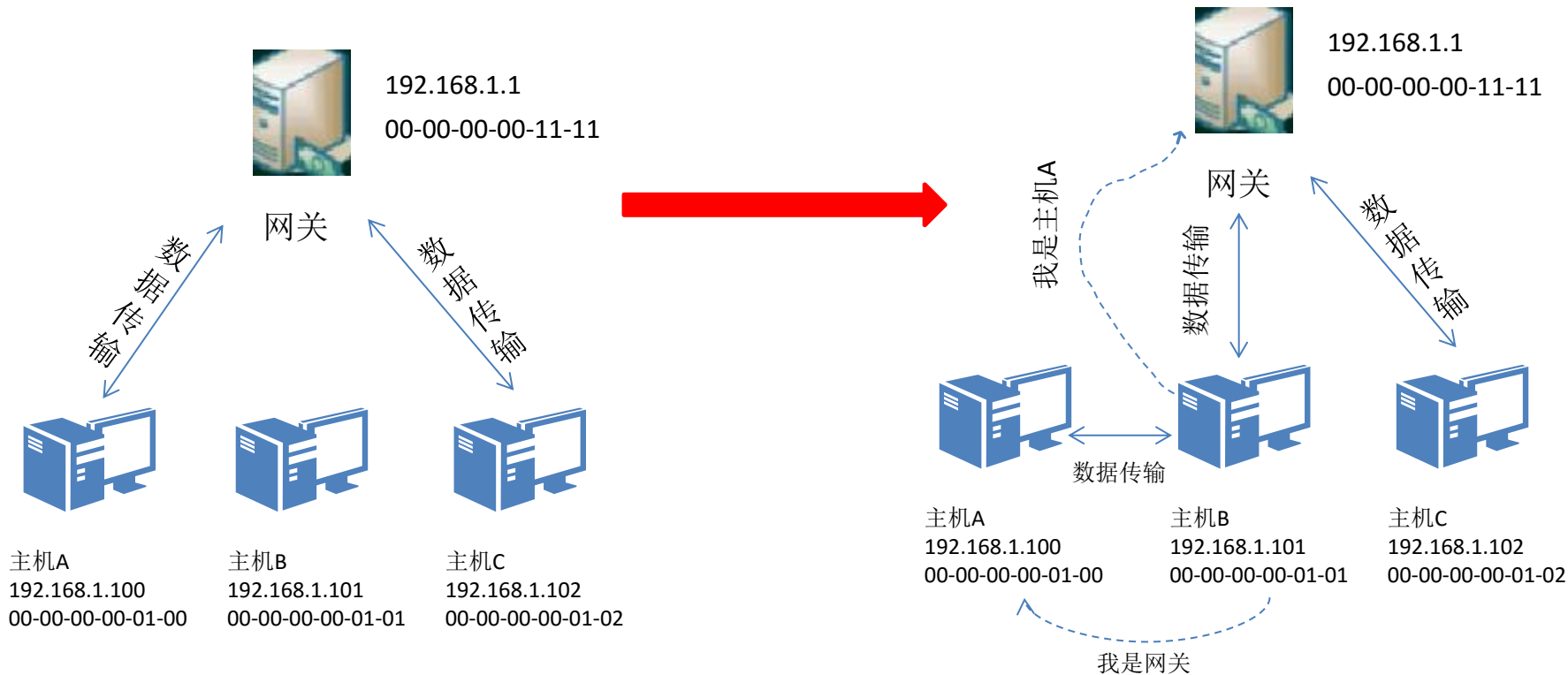
证书所有人的公开密钥

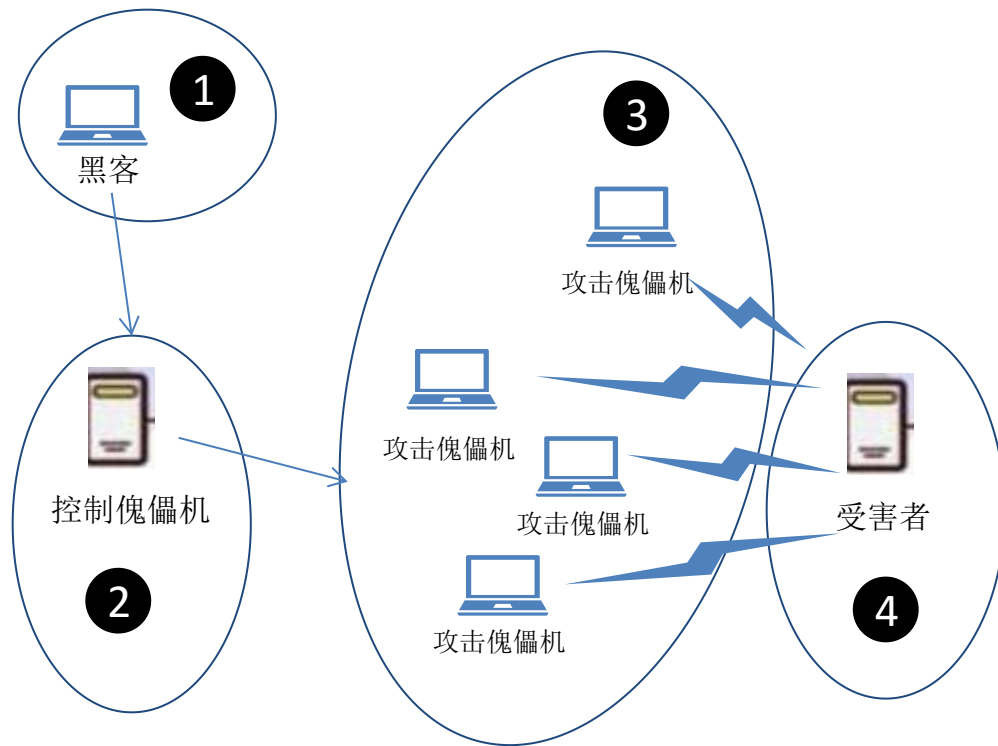
证书发行者对证书的签名





- ✓ ARP欺骗攻击
- ✓ DoS（拒绝服务）与DDoS
- ✓ 重放攻击





计算机信息系统安全保护等级划分准则（GB17859-1999）

用户自主保护级：适用于普通内联网用户

系统审计保护级：适用于通过内联网或国际网进行商务活动，需要保密的非重要单位

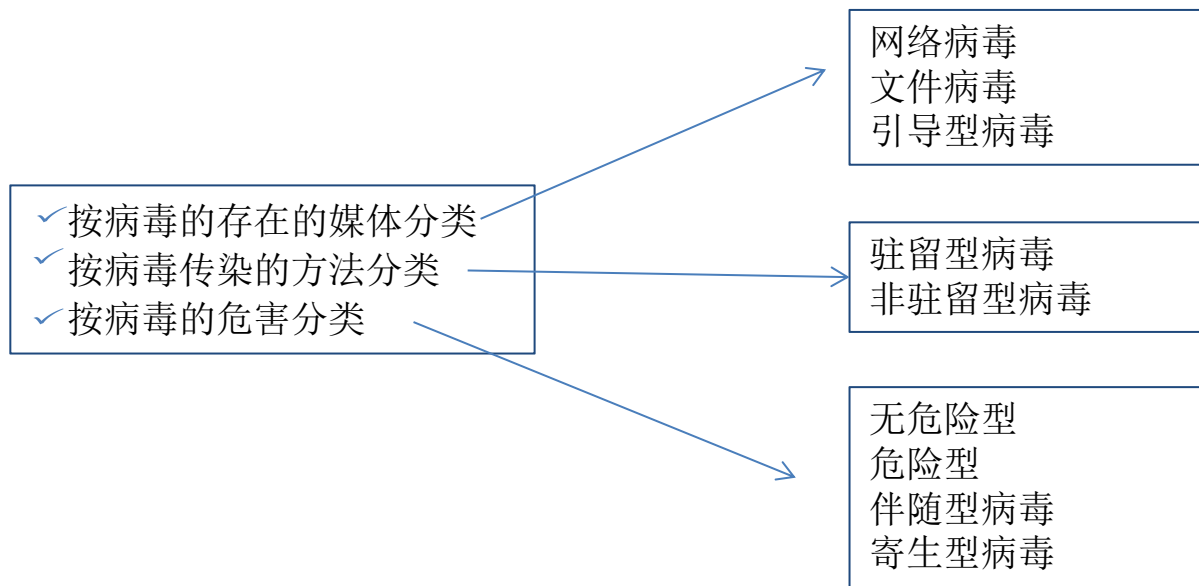
安全标记保护级：适用于地方各级国家机关、金融机构、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位

结构化保护级：适用于中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部门、尖端科技企业集团、国家重点科研机构和国防建设等部门

访问验证保护级：适用于国防关键部门和依法需要对计算机信息系统实施特殊隔离的单位

病毒：编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机适用并且能够自我复制的一组计算机指令或者程序代码。

木马：计算机木马是一种后门程序，常被黑客用作控制远程计算机的工具。



系统病毒 (前缀 : Win32、PE、W32 , 如 : KCOM——Win32.KCOM)

蠕虫病毒 (如 : 恶鹰——Worm.BBeagle)

木马病毒、黑客病毒 (如 : QQ消息尾巴木马——Trojan.QQ3344)

脚本病毒 (如 : 红色代码——Script.Redlof)

宏病毒 (如 : 美丽莎——Macro.Me l isaa)

后门病毒 (如 : 灰鸽子——Backdoor.Win32.Huigezi)

病毒种植程序病毒 (冰河播种者——Dropper.BingHe2.2C)

破坏性程序病毒 (杀手命令——Harm.Command.Killer)

玩笑病毒 (如 : 女鬼——Joke.Girl ghost)

捆绑机病毒 (如 : 捆绑QQ——Binder . QQPass.QQBin)