作业 2

1、从保密通信的需求出发，分析为什么需要 PKI。

随着全球经济一体化的到来，越来越多的应用必须通过网络来完成。那么怎样构建一个安全的网络环境呢？国际标准化组织 ISO 制定的 OSI 安全体系结构定义了网络安全服务、安全机制及安全管理的功能，并给出了 OSI 网络层次安全服务和安全机制之间的逻辑关系。它规定的五种标准的安全服务———访问控制服务、数据保密服务、数据完整性服务、对象认证安全服务和防抵赖安全服务———就是目前网络环境安全研究要达到的标准。

假设 Alice 要通过网络发送一份极其重要的、保密的文件给千里之外的 Bob，如何才能安全地发送此文件？

(1) 采用何种加密技术？采用对称密码体制算法加密文件内容，如 DES、3DES。

(2) Bob 如何获得密钥？采用非对称密码体制算法加密密钥后发送给 Bob。

(3) 为什么不直接用非对称密码体制加密文件内容？加密速度慢，且加密后文件内容变长。

(4) 黑客假冒 Alice 使用对称密钥加密假文件内容，并用 Bob 公钥加密对称密钥发送给 Bob，如何鉴别？使用数字签名算法。

(5) Alice 如何确定其使用的公钥的确是 Bob 的公钥？使用数字证书绑定公钥与公钥所属人。

(6) Bob 收到文件后 Alice 否认曾签署过此文件？采用可信时钟服务，用可信时间戳与签名者一起对文件联合签名。

(7) Bob 如何确定与他进行文件传输的确实是 Alice 本人？使用强口令、认证令牌、智能卡和生物特征等技术对使用私钥的用户进行认证。

通过以上问题，解决了保密通信的需求。同时，将以上问题的解决方案整合，这就是 PKI 公钥基础设施。

PKI 是 Public Key Infrastructure 的缩写，其主要功能是绑定证书持有者的身份和相关的密钥对（通过为公钥及相关的用户身份信息签发数字证书），为用户提供方便的证书申请、证书作废、证书获取、证书状态查询的途径，并利用数字证书及相关的各种服务（证书发布，黑名单发布，时间戳服务等）实现通信中各实体的身份认证、完整性、抗抵赖性和保密性。**PKI 产生的根本原因是把非对称密钥管理标准化**。其中：

(1) CA 证书授权中心：解决数字证书权威认证、签发问题；

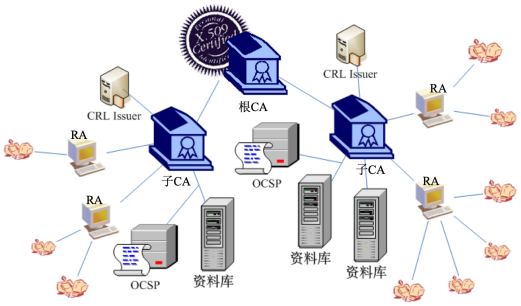
(2) 数字证书：解决公钥与用户绑定认证问题；

(3) LDAP 轻型目录访问协议：解决数字证书查询和下载的性能问题，避免 CA 中心成为性能瓶颈；

(4) CRL 证书作废列表和 OCSP 在线证书状态协议：方便用户快速获得证书状态。

(5) RA 注册机构：方便证书业务远程办理、方便证书管理流程与应用系统结合。

2、根据 PKI 的基本结构图，描述 PKI 的初始化流程、用户服务流程及证书验证流程。



初始化流程：

(1) 根 CA 产生自己的密钥对和自签名证书。
(2) 根 CA 建立子 CA：子 CA 产生密钥对，向根 CA 申请证书；子 CA 从根 CA 得到证书；每个子 CA 分别建立自己的 RA。
(3) 建立 RA：CA 给 RA 管理员签发证书；RA 管理员添加“RA 录入员、审核员”； CA 给 RA 录入员、审核员签发证书。
(4) 建立资料库，使用 OCSP 协议。
(5) 设置 CRL Issuer，产生密钥对，向其 CA 申请证书；CA 签发 CRL Issuer 证书。

用户服务流程：

(1) 订户产生公钥密钥对。
(2) 将自己的公钥和信息交给 RA 录入员，并且录入 RA 系统。
(3) RA 审核员审核信息的真实性。
(4) 发送证书请求给子 CA。
(5) 子 CA 签发证书，返回给 RA，并交给订户。
(6) 子 CA 随时响应用户的查询。

证书验证流程：

(1) Alice 收到 Bob 的证书和 CA 的根证书。
(2) 验证证书是否处于有效期中。
(3) 验证证书是否被撤销：
    - 没有 OCSP 协议时：获取证书相应的 CA（或者 CRL Issuer）所签发的、处于有效期的 CRL、验证 CRL 上的数字签名是否有效、证书序列号是否在 CRL 上面。
    - 有 OCSP 协议时：向 OCSP Server 查询序列号，Server 返回证书状态。
(4) 验证证书数字签名：通过 CA 根证书里的 CA 公钥解密 Bob 证书的 CA 签名得到 Hash 值；将 Bob 证书内容进行 Hash，得到另一个 Hash 值；对比两个 Hash 值是否一致。一致则通过，否则不通过。
(5) 验证终点为自签名证书。