1. PKI公钥基础设施

\*目的：从技术上解决网上身份认证、电子信息的完整性和不可抵赖性等安全问题，为网络应用提供可靠的安全服务。

\*任务：确立可信任的数字身份。

\*组成：（1）证书机构（CA）:负责发放和管理数字证书、提供网络身份认证服务。

（2）注册机构(RA):注册机构是数字证书注册审批机构，是认证中心的延伸。

（3）证书发布库:用于集中存放CA颁发证书和证书撤销列表。

（4）密钥备份与恢复

（5）证书撤销

（6）PKI应用接口

2.数字证书

\*基本概念：一个用户的身份与其所持有的公钥的结合，由一个可信任的权威机构CA来证实用户的身份，然后由该机构对该用户身份及对应公钥相结合的证书进行数字签名，以证明其证书的有效性。

\*包含的信息：（1）主体名

1. 公钥
2. 序号
3. 有效期
4. 签发者名

\*数字水印的生成过程：

