

信息安全导论第三次作业

1. 计算机对人进行认证的方法主要有:

- ①基于口令的认证
- ②基于智能卡的认证
- ③基于生物特征的认证

2. 证书是在互联网通讯中标志通讯各方身份信息的一个数字认证
基本功能是用来识别通讯方的身份

3. X.509数字证书包含以下信息:

- ①版本号 ②序列号 ③签名算法标识 ④签发者 ⑤有效期月 ⑥证书主体名
- ⑦证书主体的公钥信息 ⑧签发者唯一标识 ⑨证书主体唯一标识
- ⑩扩展 ⑪签名

4. 信任模型就是提供用户双方相互信任机制的框架

- 主要有以下模型: ①层次模型 ②交叉模型 ③混合模型 ④桥CA模型
- ⑤信任链模型