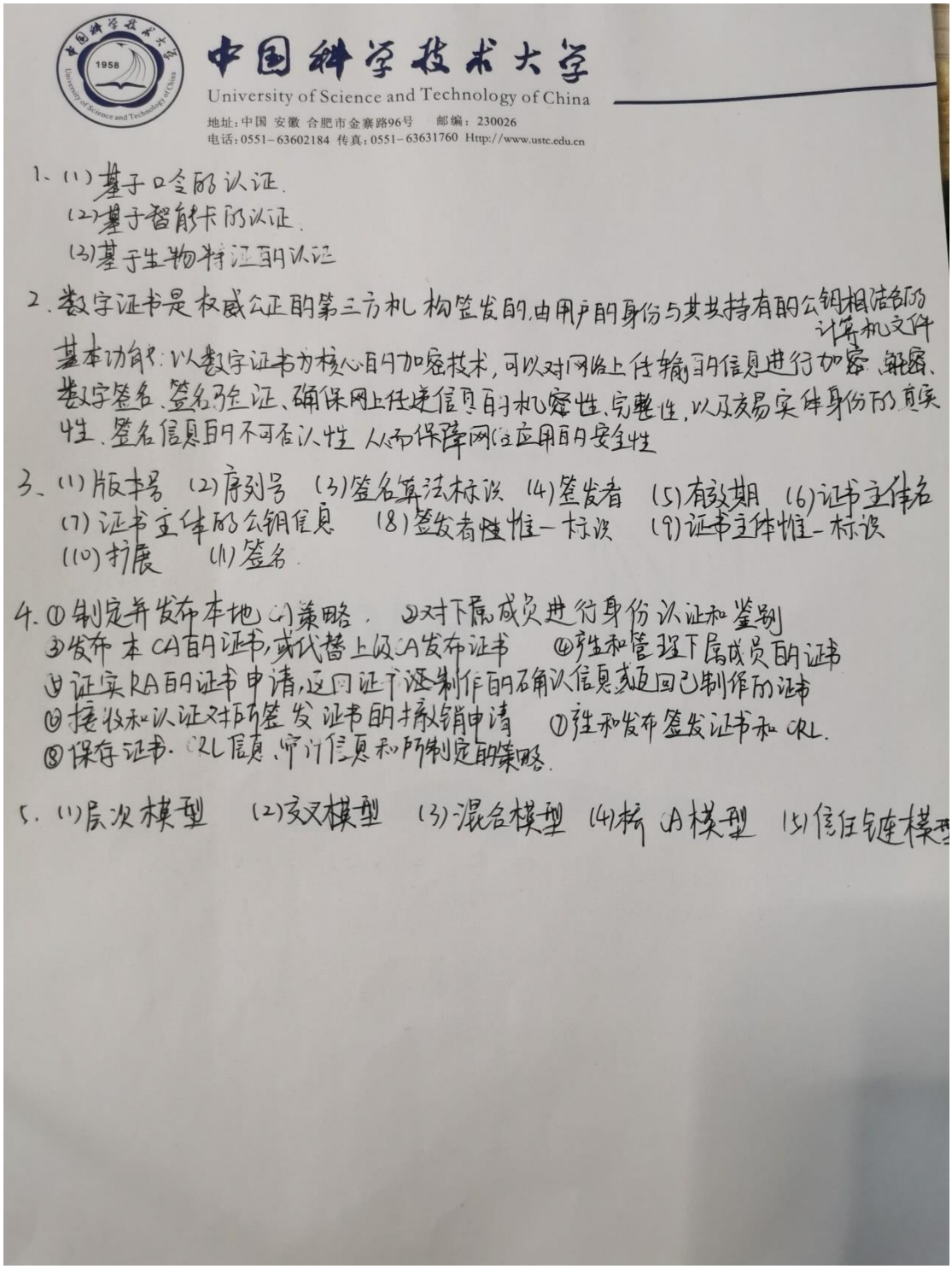
第三次作业

PB19111708 杨云皓



中国科学技术大学
University of Science and Technology of China
地址：中国 安徽 合肥市金寨路96号 邮编：230026
电话：0551-63602184 传真：0551-63631760 Http://www.ustc.edu.cn

1. (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. 数字证书是权威公正的第三方机构签发的,由用户的身份与其持有的公钥相结合的计算机文件
基本功能: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、解密、数字签名、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

3. (1)版本号 (2)序列号 (3)签名算法标识 (4)签发者 (5)有效期 (6)证书主体名
(7)证书主体的公钥信息 (8)签发者性惟一标识 (9)证书主体性惟一标识
(10)扩展 (11)签名.

4. ①制定并发布本地CA策略. ②对下属成员进行身份认证和鉴别
③发布本CA的证书,或代替上级CA发布证书 ④产生和管理下属成员的证书
⑤证实RA的证书申请,返回证实证书制作的确认信息或返回已制作的证书
⑥接收和认证对所签发证书的撤销申请 ⑦产生和发布签发证书和CRL.
⑧保存证书、CRL信息、审计信息和所制定的策略.

5. (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