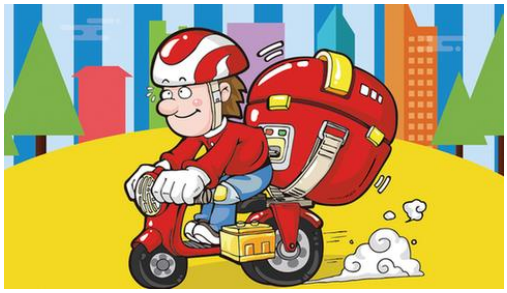
作业 4 示例（仅供参考）



今天校园里到处是快递小哥，同学们也经常帮别人取快递，快递小哥不会很细致的核实身份，就允许代领，存在很多不安全因素。 设计一款基于手机的 app，用于快递小哥验证身份，顾客领取快递。具体认证方法不限，简单易行。 给出：app 包含哪些部分（可加图示），每部分的功能；模仿 kerberos 的写法，描述交互过程，并加说明。{做一个漂亮的 PPT，下节课讨论}

方案：

一、前提条件

（1）App 分为三个模块：快递公司、快递员、客户（收件人及代收人）。

快递公司：为注册用户签发 CA，接受电商交付货物、下发给快递员及用户物流信息，修改物流状态。

快递员：验证收货人（代收人）信息，交付货物，反馈收货确认,扫描客户提供的收货（代收）验证码；

客户：接受快递公司推送信息，生成并出示收货信息二维码，请求代收人，帮人代收，生成并出示代收信息二维码。

（2）快递员、客户据信任快递公司，并保存快递公司的证书 CA0，私钥自由自己知道，快递公司为每个用户（含快递员）签发证书:

CA=(name||ID||KUuser||Lifetime||Ekr0[H(name||ID||Lifetime)]);

（3）系统角色及代号：

快递公司-0（CA0：自签），快递员-1（CA1），收件客户-2（CA2），代收人-3（同为注册用户，有 CA3）

（4）为了简化内容，App 传输采用 SSL 加密传输。不考虑传输被攻击问题；

二、快递发送签收过程

（1）物流交付

电商->0：O(order form)；同时提交货物

电商->2：O；发货信息

（2）物流通知

0->1：O||CA2||Ekr0（H（O||CA2））

0->2：O||CA1||Ekr0（H（O||CA1））

（3）交付确认

2->1: O||Eku1[Ekr2[H(O)||time]];2 生成二维码，1 扫码验证，1 把货物交给 2

1->0: O||Ekr2[H(O)||time]||Ekr1[H(O||Ekr2[H(O)||time])]

;1 告诉 0 已确认收货，0 修改物流状态

（4）代收交付确认（2 向 3 请求代收，3 同意）

3->2: CA3；2 验证 CA3

2->3: O||CA2||Eku3[Ekr2[H(O)||CA3]]

3->1: O||CA2||CA3||Eku1[Ekr2[H(O)||CA3]|| Ekr3[H(O)||time]]；3 生成二维码，1 扫码验证，1 把货物交给 3

1->0: O|| Ekr2[H(O)||CA3]|| Ekr3[H(O)||time]||Ekr1[O|| Ekr2[H(O)||CA3]|| Ekr3[H(O)||time]]

;1 告诉 0 已确认代收货，0 修改物流状