**信息安全概论 课程设计（2020春）**

--------------------------------------------------------------------------------

**截止时间：2020-06-30，24：00之前给教师发邮件。**

**学号：**

**姓名：**

**教师信箱： zhaijh\_hit@126.com和Conandor@126.com 两个邮箱各发一份，提交形式（学号-姓名.pdf）**

-------------------------------------------------------------------------------------------

**成绩：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 题号 | （1） | （2） | （3） | 合计 |
| 成绩 |  |  |  |  |

-------------------------------------------------------------------------------------------

**课程设计要求**

目前国内区块链技术发展应用迅速，且有广阔的前景，区块链最初应用起源于比特币，其实现与密码学紧密相连。

认真回答下列问题，注意格式规范，结构合理，语言流畅、图表清晰。如果格式排版混乱，**总分成绩可减5分**。（小标题黑体小四号，正文宋体五号，图表名及内部字体小五号，长度不限，可自由调整。）

1. **简述区块链原理及安全机制，分析其有哪些特点，并说明该特点的实现是否与密码学相关，说明如何相关。（5分，）**
2. **方案设计（共20分）**

设计一个彩票中心销售服务方案，包括发布、销售、兑奖等环节（兑奖：视频摇奖，直接公布获奖号码列表），彩票销售、兑奖等环节均线上实现，线上交易模仿SET协议，充分利用课内相关知识，也可参考区块链安全解决方法及自己合理发挥。（20分）

彩票销售过程参考：

1. 彩民线上购买彩票，选择彩票号码及投注数，购买资金汇入彩票中心的银行账户；
2. 彩民保存购买彩票号码和投注数，重要信息加密签名后提交彩票中心保存；
3. 彩票开奖过程，视频直播开奖，网上公布获奖彩票号码列表；
4. 彩民依据购买彩票信息，向彩票中心申请兑奖；
5. 彩票中心验证无误，提交奖金转账信息给银行；
6. 银行核对信息无误，将奖金转给彩民账户。

前置条件：

（1）实体：彩票中心TC（Ticket Center），顾客User，认证中心CA（绝对安全可信），兑奖银行（Bank）

（2）User、TC和银行均已在CA认证中心注册，拥有证书CAuser、CAtc和CAbank 。

（3）User和TC均已以在银行Bank注册，拥有账户（BankAccount）BAuser和BAtc；

**（在方案设计区的相应小标题下，填写你的相关设计说明即可，长度不限，随意调整；彩票销售兑奖等过程步骤，大家需做需求调研，具体方案内容大家可以合理发挥）**

------------------------------------

**方案设计区**

一、基于区块链的彩票销售系统整体架构（本问题5分）

（1）系统功能描述

（2）物理拓扑结构示意（建议使用Visio画图）

（3）功能模块划分与定义

（4）区块链技术在彩票销售过程中的作用（解决的问题）

二、用户在彩票中心注册过程与说明（协议描述格式与形式，模仿Kerberos双向交互形式写法，后边要有注释说明，具体的密码使用可以采用对称密钥密码，也可以采用公开密钥密码）（本问题3分）

三、彩票销售购买过程与说明（参照Kerberos写法，后边要有注释说明）（本问题3分）

四、彩票兑奖过程与说明（参照Kerberos写法，后边要有注释说明）（本问题3分）

五、系统风险分析（分析是否存在“用户隐私信息泄漏”、“重放攻击”、“身份欺诈”、“冒名兑奖”、“彩票中心否认用户获奖”、“用户谎称没有收到奖金”等威胁，系统是如何应对这些威胁的，一一说明。）（本问题6分）

1. **在你设计彩票中心销售系统时，如果彩票中心领导要求可以查看用户购买彩票情况（号码），以及用户相关信息，便于管理及公安等部门依法处理有关事宜，希望你开发这样的功能。（共5分）**

一、你将如何做，谈谈你的想法，为什么？（此问题 3分）？

二、你准备采取何种技术措施，简单描述。（此问题 2分）