作业提交截至时间：2019年5月15日

作业1：

考虑一个银行B和一个用户A，用户A可能向银行B发送转账指令等。用学习到的密码学知识，描述如何实现A和B之间的安全通信。

提示：需要涉及到身份认证、防止伪冒攻击、密钥协商、保护数据机密性、保证数据完整性、消息的不可否认等。尽量考虑周全。

（50分）

作业2：

考虑一个假想的Bitcoin系统：系统初始没有任何块；初始时区块奖励为20比特币，每10个块更新一次区块奖励值至原来的1/2；初始时系统内有10个参与者，记为U1~U10（仅用于描述方便），每个参与者的算力均为1芯片，初始时挖矿难度为1，每5个块更新一次挖矿难度，期望系统每5分钟产生一个有效区块；每个区块内至多包含4个交易（由于区块大小的原因）。其余机制与真实的Bitcoin系统相同，例如，签名机制、地址机制等。

现在假设系统开始运行，系统时间T=0（可以假想为分钟，注意这个时间仅为了我们描述方便，不可做时间同步）

1. 到T=20时，系统产生了5个区块。请在以上规则下，想象和描述这5个块及其包含交易的信息，可结合图、表，以充分体现比特币系统的各种特性及规则为准则。【交易费在一两个块里体现就行，其他的块的交易可让交易费为0】。
2. 到T=35时，U1~U10购买了新的算力，每个参与者的算力变为2芯片，同时，有两个新的参与者U21（算力为8芯片）、U22（算力为12芯片）加入。请在此假想情况下，在问题1）的基础上，描述系统内前n个区块及其内交易的情况（n>=20）【交易情况可只描述关键交易】，以充分体现比特币系统的各种特性及规则为准则。
3. 描述某一时刻后，U1~U5形成了以U1为矿池管理员的矿池后，10个区块及其内交易的情况【交易情况可只描述关键交易】，以充分体现比特币系统的各种特性及规则为准则。

（50分）

作业3（选作，100分）

请考虑如何解决（课件中）Deterministic Wallet和Stealth Address中的安全缺陷。