密码学第一次作业

1. 当使用 POS 机刷银行卡进行支付时，用户通过提供个银行卡和个人身份识别码（PIN）来访问其账户，从而完成支付。请给出该支付系统相关机密性、完整性等所需的安全需求，并针对每个安全需求给出重要性程度。

2. 对于下面的资产，发生保密性、可用性和完整性损失时，分别为其产生的影响划分低、中和高等级，并陈述理由：

合同签订机构的大单收购信息系统，包含敏感、预投标阶段的合同信息和例行的行政信息，分别评价这两份信息资产的影响情况及整个信息系统的影响情况。

3. 2021 年 8 月，日本加密货币交易所 Liquid 遭到网络攻击，9400 万美元失窃。由于攻击事件，Liquid 已停止所有加密货币取款业务。经过调查，网络攻击者通过：

1) 收集目标相关的互联网信息和使用的开源系统的源代码；
2) 利用钓鱼邮件和水坑攻击收集用户登陆凭证信息，窃取用户私钥；
3) 使用被攻击者账户（即合法账户）来部署攻击合约；
4) 使用被攻击者账号进行交易，将所有资产转移到攻击合约中；
5) 攻击合约自动执行，通过 Uniswap 等去中心化交易所将资产转出，防止项目方启动应急机制锁定被盗资产；

请分析在此事件中攻击者的能力（以上各条攻击手段分别是主动攻击或被动攻击中的哪种）、攻击者破坏了哪些安全服务。针对攻击者所破坏的安全服务，应采用哪些安全机制以降低风险？

攻击手段	攻击者能力	破坏的安全服务	应采用的安全机制
1）			

2）			
3）			
4）			
5）			

4. 云计算是通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并可按需自助获取和管理资源的模式。在国标文件 GA_T 1390.2-2017 中规定了云计算安全扩展需求。请选取以下安全需求中的 5 条，分类并给出等级评价，并阐述理由：

1）在控制器和设备之间必须建立双向验证机制

2）确保云租户账户信息、鉴别信息、系统信息等不被泄露

3）只有在管理设备授权下，云服务商或第三方才具有用户数据的管理权限

4）屏蔽资源故障，当某台设备崩溃后，不会影响到整个系统和其他虚拟机

5）提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改

6）采取加密或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问

7）确保虚拟机迁移过程中，重要数据不被损坏

8）云租户的口令不能被窃取

9）能够监测异常数据的来源，能够记录攻击类型、攻击时间、攻击流量等

10）能够及时识别假冒的用户，并向系统发出警告

11）服务器中日志不能被随意删除

12）当系统中流量较大时，系统能够正常运行

安全目标	保密性	完整性	可用性	真实性	可追溯性
安全需求					
安全等级					

5. 请查阅资料，结合一个近年的网络安全事件，指出这起事件中相关系统的 3 条安全需求及对应的安全目标与安全等级，并简要阐述理由。

注意：

以上作业请使用 **pdf** 文档格式提交，于 **2023 年 3 月 9 日（星期四）23:59** 之前，在 OJ 系统上提交，并将作业命名为“**学号_姓名_密码学第一次作业**”。如“21371234_张三_密码学第一次作业”。