信息安全理论与技术参考答案

1. 填空题
2. 保密性、可用性、可控性、可审查性 p2
3. 密码编译学、密码分析学 P39
4. 抗攻击 P159
5. 证书初始化注册阶段、颁发使用阶段、撤销阶段 P111
6. 选择题

1-5:CADAB 6-10:BCCDA

11-15:BADBC 16-20:CABDA

1. 判断题

1-5：√××√× 6-10：√××√√

第四题和第五题要参考李飞编著的《信息安全理论与技术》，下面都是该书页码。

1. 简答题
2. P52、P62
3. P101
4. 信安实验一实验原理
5. P109、P110
6. P155
7. P159、P160
8. 综合应用题

1.（1）P81

（2）P182

2.P193

3、如何防御日蚀攻击？请说明具体的防御措施。

答：1、采用节点身份验证机制，通过身份验证防止攻击者伪造节点身份；

2、对矿工的加密签名进行验证，并将该矿工的身份与共识信誉表中已知矿工的身份进行比对，当共识得分大于50%时，网络节点才会接受该矿工的区块；

3、采用高成本的多身份申请机制，通过提高身份伪造成本缓解女巫攻击，减少女巫攻击就可以减少日蚀攻击；

4、区块链节点可以通过随机取样的方式选取区块链中已有的区块，根据其中包含的交易类型、金额、数量等特征计算出该区块生成者的权重。然后随机选择节点并请求包含其心跳信息和上一区块哈希值在内的活性证明，如果该节点成功证明自身活性，则验证者累计已验证节点的权重，并重复上述操作直至累计权重达到预先设置的阈值；若被选中节点未通过或未参与活性检测，则证明区块链网络发生分区，应立即停止出块。