北京邮电大学 2023—2024 学年第一学期

《网络空间安全导论》期中考试试卷

（总分：50 分）

班级_____ 学号_____ 姓名_____

1．是非判断题（5 分，每题 1 分，“v”表示正确，“x”表示错误）

(1) 网络空间安全的目标就是保证网络空间的绝对安全。（ ）

(2) 现代密码系统的安全性不应取决于不易改变的算法，而应取决于可改变的密钥。（ ）

(3) RSA 算法的安全性是依赖于基于分解大整数的困难问题，如果这个难题被攻破，那么 RSA 算法就不安全了。（ ）

(4) 防火墙是网络安全的重要一环，通过合理地配置防火墙才能发挥出防火墙所具备的功能。（ ）

(5) 目前，网络攻击基本都来自于个人行为，其目的就是获取经济利益。（ ）

2．选择题（5 分，每题 1 分，每题只有一个选项最符合题目要求）

(1) 按现在的计算能力，对称密码的密钥长度至少为（ ）才是安全的。

A. 64 位 B. 128 位 C. 256 位 D. 1024 位

(2) 公钥密码体制的出现，解决了对称密码体制的密钥分发问题，在公钥密码算法中，加密对称密钥所使用的密钥是（ ）。

A. 发送方的公钥 B. 发送方的私钥 C. 接受方的公钥 D. 接受方的私钥

(3) 设 hash 函数的输出长度为 n 比特，则安全的 hash 函数寻找碰撞的复杂度应该为（ ）。

A. $O(n)$ B. $O(2n)$ C. $O(2^{n-1})$ D. $O(2^{n/2})$

(4) 防火墙哪项技术能够实现不公开内部服务器真实 IP 地址及隐藏内部网络结构。（ ）

A. 包过滤技术 B. IP 与 MAC 的绑定 C. MAP (地址/端口映射) D. 带宽管理

(5) 下面哪项安全技术能够对网络和主机的安全性进行风险分析和评估。(　　)

A.防火墙　　B.入侵检测系统　　C.漏洞扫描系统　　D.防病毒软件

3. 填空题（10 分，每空 1 分）

(1) 信息安全保障包括保护、_____、_____和恢复四个子过程，是一个完整的动态、不断循环上升的过程。

(2) Enigma 密码机出现是近代密码发展史中里程碑的事件，从这个事件得到启示，实用密码设备应必备四要素，即_____、_____、成本、易用。

(3) 消息认证的目的是指_____、_____。

(4) 计算机病毒的生命周期包括创造期、传播期、_____、发病期、发现期、_____和灭绝。

(5) 从安全属性看，攻击类型可分为 5 类：截取攻击、篡改攻击、_____、阻断攻击和_____。

4. 术语解释（共 6 分）

(1) 完整性（2 分）

(2) Hash 函数（2 分）

(3) 防火墙（2 分）

5. 简答题（共 18 分）

(1) 请指出公钥密码体制的优点与不足。(6 分)

(2) 请描述数字签名实现的的基本过程。(4 分)

(3) 请指出恶意软件的特征有哪些。(说出 4 点即可) 。(4 分)

(4) 简要描述分布式拒绝服务(DDoS)的攻击过程。(4 分)

6. 灵活题（6 分）

(1) 通过这门课的学习，谈谈你的收获和期望。(3 分)

(2) 请评价这门课的教学（包括助教的工作）。(3 分)