网络安全理论与技术

本试卷由 Xovee 制作，从一来源未明的图片试卷转制而成。

填空题（每空 1 分，共 20 分

1. ISO 7498-2 确定了五大类安全服务，即鉴别、_____、数据保密性、数据完整性和不可否认性。同时，ISO 7498-2 也确定了八类安全机制，即加密机制、数据签名机制、访问控制机制、数据完整性机制、_____、业务填充机制、路由控制机制和公证机制。

2. 古典密码包括_____ 和置换密码两种，对称密码体系和非对称密码体系都属于现代密码体制。传统的密码系统主要存在两个缺点：一是_____；二是_____. 在实际应用中，对称密码算法与非对称密码算法总是结合起来的，对称密码算法用于加密，而非对称算法用于保护对称算法的密钥。

3. 根据使用密码体制的不同可将数字签名分为_____ 和_____，根据其实现目的的不同，一般又可将其分为_____ 和_____。

4. DES 算法密钥是 64 位，其中密钥有效位是_____ 位。RSA 算法的安全是基于分解两个大素数的积的困难。

5. 网络安全中窃取是对信息的_____ 性的攻击。Dos 攻击了信息的_____ 性。

6. 信息安全的目标是保护信息的_____、_____、_____、_____。

7. 密钥管理的主要内容包括密钥的生成、分配、使用、存储、备份、恢复和销毁。密钥生成形式由两种：一种是由_____ 生成，另一种是由_____ 生成。

8. 认证技术包括_____、_____ 和身份认证，而身份认证的方法主要由口令、磁卡和智能卡、_____、_____。

9. NAT 的实现方式有三种，分别是_____、_____、_____。

10. 防火墙的类型包括_____、_____ 和状态检测防火墙。

11. _____ 是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。

简答题（每小题 6 分，共 30 分

1. 比较对称密码体制与公钥码体制的优缺点。

2. 信息隐藏和数据加密的主要区别是说明?

部分答案

1. ISO 7498-2 确定了五大类安全服务，即鉴别、访问控制、数据保密性、数据完整性和不可否认性。同时，ISO 7498-2 也确定了八类安全机制，即加密机制、数据签名机制、访问控制机制、数据完整性机制、认证交换、业务填充机制、路由控制机制和公证机制。

2. 古典密码包括代替密码 和置换密码两种，对称密码体系和非对称密码体系都属于现代密码体制。传统的密码系统主要存在两个缺点：一是密钥管理与分配问题；二是认证问题. 在实际应用中，对称密码算法与非对称密码算法总是结合起来的，对称密码算法用于加密，而非对称算法用于保护对称算法的密钥。

3. 根据使用密码体制的不同可将数字签名分为基于对称密码体制的数字签名 和基于公钥密码体制的数字签名，根据其实现目的的不同，一般又可将其分为直接数字签名 和可仲裁数字签名。

4. DES 算法密钥是 64 位，其中密钥有效位是64 位。RSA 算法的安全是基于分解两个大素数的积的困难。

5. 密钥管理的主要内容包括密钥的生成、分配、使用、存储、备份、恢复和销毁。密钥生成形式由两种：一种是由中心集中 生成，另一种是由个人分散 生成。

6. 认证技术包括站点认证、报文认证 和身份认证，而身份认证的方法主要由口令、磁卡和智能卡、生理特征识别、零知识认证。

7. NAT 的实现方式有三种，分别是静态转换、动态转换、端口多路复用。

8. 数字签名 是笔迹签名的模拟，是一种包括防止源点或终点否认的认证技术。