电子科技大学 2017 年夏季信软学院研究生班考试试题

课程名称：高级网络安全　任课教师：陈伟

学生人数：＿＿＿＿＿＿　印题份数：＿＿＿＿＿＿　学号：＿＿＿＿＿＿　姓名：＿＿＿＿＿＿＿＿

题号	一	二	三	四	五	六	七	八	九	十	平时	总分
得分												

考试时间	年　月　日	阅卷教师签名	

一、选择题(每小题 2 分，共 30 分)

1．信息安全的基本属性是＿＿＿＿。

A. 保密性　　B.完整性　　C. 可用性、可控性、可靠性　　D. A，B，C 都是

2．假设使用一种加密算法，它的加密方法很简单：将每一个字母加 5，即 a 加密成 f。这种算法的密钥就是 5，那么它属于＿＿＿＿。

A. 对称加密技术　　B. 分组密码技术　　C. 公钥加密技术　　D. 单向函数密码技术

3．密码学的目的是＿＿＿＿。

A. 研究数据加密　　B. 研究数据解密　　C. 研究数据保密　　D. 研究信息安全

4．完整的数字签名过程（包括从发送方发送消息到接收方安全的接收到消息）包括＿＿＿＿和验证过程。

A、加密　　B、解密　　C、签名　　D、保密传输

5．数字签名要预先使用单向 Hash 函数进行处理的原因是＿＿＿＿。

A. 多一道加密工序使密文更难破译　　B. 提高密文的计算速度

C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

D. 保证密文能正确还原成明文

6．身份鉴别是安全服务中的重要一环，以下关于身份鉴别叙述不正确的是＿＿。

A. 身份鉴别是授权控制的基础

B. 身份鉴别一般不用提供双向的认证

C. 目前一般采用基于对称密钥加密或公开密钥加密的方法

D. 数字签名机制是实现身份鉴别的重要机制

7．防火墙用于将 Internet 和内部网络隔离＿＿＿＿。

注：1．试题字迹务必清晰，书写工整。　　本题4页，本页为第1页

2．题间不留空，一般应题卷分开

A. 是防止 Internet 火灾的硬件设施

B. 是网络安全和信息安全的软件和硬件设施

C. 是保护线路不受破坏的软件和硬件设施

D. 是起抗电磁干扰作用的硬件设施

8. PKI 支持的服务不包括_____。

A. 非对称密钥技术及证书管理　　B. 目录服务

C. 对称密钥的产生和分发　　D. 访问控制服务

9. 设哈希函数 H 有 128 个可能的输出(即输出长度为 128 位)，如果 H 的 k 个随机输入中至少有两个产生相同输出的概率大于 0.5，则 k 约等于____。

A. 2^{128}　　B. 2^{64}　　C. 2^{32}　　D. 2^{256}

10. Bell-LaPadula 模型的出发点是维护系统的_____，而 Biba 模型与 Bell-LaPadula 模型完全对立，它修正了 Bell-LaPadula 模型所忽略的信息的_____问题。它们存在共同的缺点：直接绑定主体与客体，授权工作困难。

A. 保密性　可用性　B. 可用性　保密性　C. 保密性　完整性　D. 完整性　保密性

11. PGP 加密技术是一个基于____体系的邮件加密软件。

A、RSA 公钥加密　　B、DES 对称加密　　C、MD5 数字签名　　D、MD5 加密

12. DES 算法有效密钥为_____位。

A、58　　B、64　　C、56　　D、128

13. 下面哪种算法只可用于数字签名_____。

A、DES　　B、DSA　　C、RSA　　D、SHA

14. IPSec 是属于____的安全机制。

A、传输层　　B、应用层　　C、数据链路层　　D、网络层

15. 下列属于 DDoS 攻击的是_____。

A、Land　　B、Ping of Death　　C、TFN　　D、Smurf

二、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。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，对称密码体制和非对称密码体制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. 网络安全中窃取是对信息的_____ 性的攻击。DoS 攻击了信息的_____性。
4. 信息安全的目标是保护信息的_____、_____、_____、_____。
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。密钥生成形式有两种：一种是由_____生成，另一种是由_____生成。
6. 认证技术包括_____、_____和身份认证，而身份认证的方法主要有口令、磁卡和智能卡、_____、_____。
7. 防火墙的类型包括_____、_____和状态检测防火墙。
8. _____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。

三、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。

1. 对称和非对称密码的优缺点

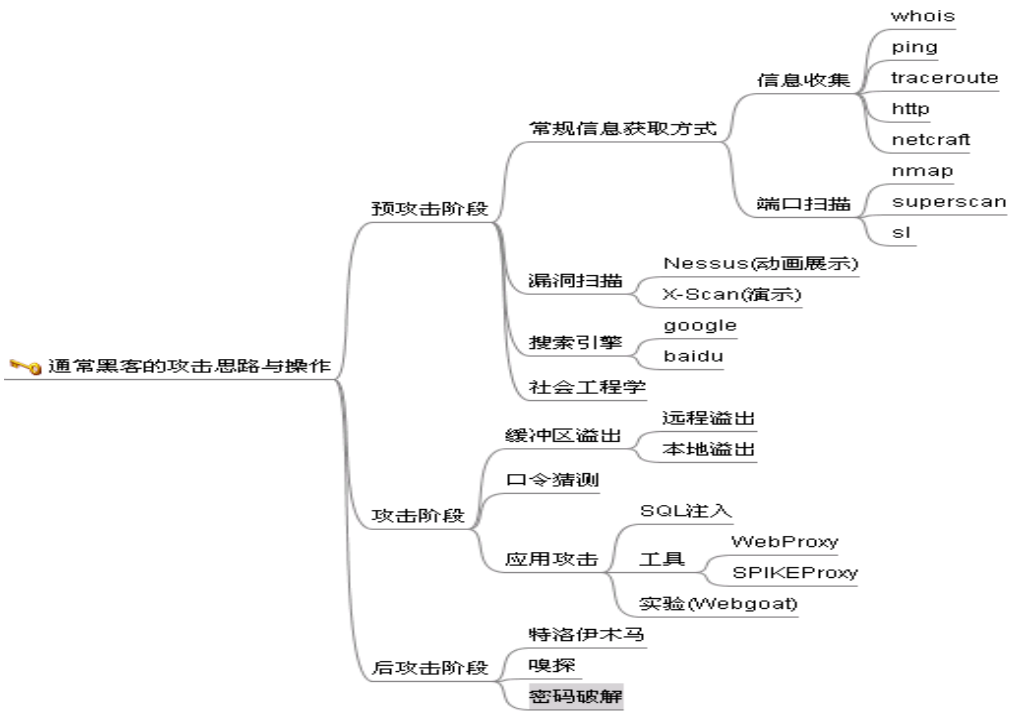
对称的优点：计算开销小，算法简单，秘钥较短，适用大量数据加密
对称的缺点：规模复杂，通信前安全秘钥交换，没法鉴别，无法签名
非对称的优点：秘钥数量很小；秘钥发布不成问题；数字签名
非对称的缺点：秘钥尺寸大，加密/解密时的速度慢，适用于少量数据加密

2、信息隐藏和数据加密的主要区别是什么？

区别：目标不同：加密仅仅隐藏了信息的内容；信息隐藏既隐藏了信息内容，还掩盖了信息的存在。实现方式不同：加密依靠数学运算；而信息隐藏充
分运用载体的冗余空间。应用场合不同：加密只关注加密内容的安全，而信息隐藏还关注载体与隐藏信息的关系。联系：理论上相互借用，应用上互补。信息先加密，再隐藏。

2、解释数字签名的概念，并阐述它在信息安全中的主要作用。

4、阐述黑客攻击的一般过程，分别用什么工具或方法？



5、信息安全有哪些常见的威胁？信息安全的实现有哪些主要技术措施？

常见威胁有非授权访问、信息泄露、破坏数据完整性，拒绝服务攻击，恶意代码。信息安全的实现可以通过物理安全技术，系统安全技术，网络安全技术，应用安全技术，数据加密技术，认证授权技术，访问控制技术，审计跟踪技术，防病毒技术，灾难恢复和备份技术

四、应用题（每小题 10 分，共 20 分）

1、 结合实际，谈谈信息安全研究的内容主要有哪些，它们分别可以实现信息的哪些方面的安全。如何运用信息安全知识防范你生活中可能遇到的安全问题。

2、设想一下，如果你为单位设计了一个网站，出于安全与使用的角度，你能使用哪些安全原理？