

主管  
领导  
审核  
签字

哈尔滨工业大学 2017 学年 春 季学期

## 信息安全概述试 题

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

片纸鉴心 诚信不败

### 一、填空（每空 1 分共 20 分）

- 1、信息安全的三个基本目标是机密性，\_\_\_\_\_，\_\_\_\_\_。
- 2、每个 SA 通过三个参数来标识\_\_\_\_\_。
- 3、信息安全保障体系包括四个的部分内容，保护，检测，\_\_\_\_\_和\_\_\_\_\_。
- 4、防电磁信息泄漏主要包括三个层面\_\_\_\_\_，\_\_\_\_\_和相关干扰。
- 5、DES 中其它算法都是线性的，而\_\_\_\_\_运算则是非线性的。\_\_\_\_\_的目的是提供密雪崩效应。
- 6、IKE 建立 SA 的第一阶段定义了两种信息交换模式为\_\_\_\_\_。
- 7、经典访问控制的模型包括\_\_\_\_\_。
- 8、传统病毒一般有三个主要模块组成，包括\_\_\_\_\_和破坏模块。
- 9、经典加密技术包括\_\_\_\_\_。

### 二、名词解释（每题 3 分共 15 分）

1、非对称密钥算法

2、证书

3、CA

4、堡垒主机

5、电子信封

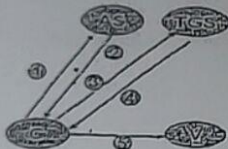
### 三、简答题（共 55 分）

1、（10 分）简述 Diffie-Hellman 密钥交换协议过程

2、（5 分）简述 Nimda 传播途径

(5分) 防火墙如何判定会话结束以及如何删除临时记录的

4、(10分) 简述图中每次会话包含的内容



线

5、(5分) 简述什么是拒绝服务攻击，并举例说明拒绝服务攻击有哪两类

纸张记忆复印  
18245035278

6、(5分) 简述双重数字签名及使用过程

7、(5分) 用图示表示 ESP 传输模式前后包头的变化以及验证区域和认证区域

8 (5分)、简述缓冲区溢出的原理及注入码的构成

纸张记忆复印

9、(5分) 简述证书的验证过程

四、计算题 (10分)

已知公钥为  $(5, 323)$ ，求私钥，并指出 RSA 算法的安全性由什么决定的。

纸张记忆复印  
18245035278