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 诚信不欺

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，_____和相关手段。

4、防电磁信息泄漏主要包括三个层面_____，_____

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

密 封 线

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的如何删除临时条目的

密

4、（10分）简述图中每次会话包含的内容

封

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

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的范围

8（5分）、简述缓冲区溢出的原理及注入码的构成

9、（5 分）简述证书的验证过程

密

封

线

四、计算题（10 分）

已知公钤为（5，323），求私钥，并指出 RSA 算法的安全性由什么决定的？