密

封

线

7. 根据可利用的数据资源来分类，密码分析者破译密码的类型包括 【 】

A. 仅知密文攻击　　B. 选择明文攻击　　C. 选择密钥攻击

D. 选择公钥攻击　　E. 选择密文攻击

8. PGP 使用随机数可以产生的密钥包括 【 】

A. 生成会话密钥

B. 生成 RSA 密钥对

C. 为伪随机数生成器提供初始种子密钥

D. 在伪随机数生成期间提供附加的输入

E. 生成初始向量

9. 安全服务可以确保系统或数据传输具有足够的安全性，五大类安全服务中包括 【 】

A. 数据保密性　　B. 数据可用性　　C. 数据完整性

D. 不可否认　　E. 鉴别

10. 下列关于身份认证的说法错误的是 【 】

A. 口令认证中只有系统强制性地验证用户的身份，用户无法验证系统的身份

B. 磁卡仅有数据存储能力，而无数据处理能力

C. 指纹识别系统不存在可靠性问题

D. 零知识证明指别人确信自己知道某秘密，而自己又不泄露该秘密

E. 智能卡的持有者都拥有一个卡上标明的 PIN

得分	评卷人	复查人

三、名词解释 （每小题 3 分，共 12 分）

1. 站点认证

2. 密钥托管

3. 虚拟专用网

4. 信息安全

得分	评卷人	复查人

四、简答题 （每小题 5 分，共 20 分）

1. 个人信息安全隐患有哪几类？

2. 防火墙作用是什么？优越性有哪些？

3. 计算机取证有哪些技术？为什么要研究计算机反取证技术？

4. 信息系统的安全需求分析包括哪些内容？