上海交通大学在线考试诚

SJTU Online Examination Ho

考试不仅是对学习成效的检查，更是对道德[illegible]风考纪，营造公平、公正的考试环境是全体同学的共同责任和义务。特别在疫情防控的特殊时期，更应强化自律意识，恪守诚信，拒绝舞弊，做一名诚实守信的新时代大学生，用诚信的考试构筑诚信的人生。

Examination is the evaluation of both learning effect and morality. It is the responsibility and obligation of all students to consciously maintain the school's common examination practice, abide by the discipline and create a fair and just examination environment. Especially in the special period of epidemic prevention and control, we should strengthen the consciousness of self-discipline, abide by the integrity, refuse to cheat, be an honest and trustworthy college student in the new era, and build an honest life from the integrity test.

我郑重承诺 I solemnly promise:

（1）本人将履约践诺，知行统一；遵从诚信规范，恪守学术道德；自尊自爱，自省自律。I will fulfill my promise, unify between knowledge and action, abide by the rules of integrity, academic ethics, be self-respected and self-disciplined.

（2）在线考试过程中，自觉遵守学校和老师宣布的考试纪律（详见《上海交通大学本科生学生手册》中的《学生考试纪律规定》，沪交教【2019】28号），不剽窃，不违纪，不作弊。In the process of online examination, I will consciously abide by the examination discipline announced by the school and the teachers (see the regulations on student examination discipline in the undergraduate student handbook of Shanghai Jiao Tong University, HJJ [2019] No. 28), and do not plagiarize, violate discipline or cheat.

（3）若违反相关考试规定和纪律要求，自愿接受学校的严肃处理或处分。In case of violation of relevant examination regulations and discipline, students shall bear the serious treatment or punishment from the school.

承诺人 Committed by: 杨一凡

（学号 Student No: 520021911080）

日期 Date (Y/M/D): 2022年 6月 10日

上 海 交 通 大 学 答 题 纸

(20__ 至 20____ 学年 第____学期)

班级号 F2003602 学号 520021911080 姓名 杨一凡

课程名称 _____ 成绩 _____

16. 不应该为元素件安全性分计算上安全性吗?

66. $\begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix}$ $\begin{pmatrix} 7 & 23 \\ 18 & 11 \end{pmatrix}$

行列式的计算如下

$det \Rightarrow \begin{pmatrix} 4 & 5 \\ 20 & 5 \end{pmatrix}$ $\begin{pmatrix} 3 & 4 \\ 19 & 4 \end{pmatrix}$

矩阵计算如下

$\begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix}\begin{pmatrix} 3 & 4 \\ 19 & 4 \end{pmatrix} = \begin{pmatrix} 18 & 8 \\ 13 & 12 \end{pmatrix} \Rightarrow \begin{pmatrix} s & i \\ n & m \end{pmatrix}$

因此可得加密为 $sinm$

通 大 学 答 题 纸

至 20____ 学年 第____学期)

姓名 杨一凡
520021911080

67. (1) 信息安全分级保护:

其要求涉密系统对国家机密进行相应的分级，并且按照所分的等级进行相应的分级保护。其中国家信息按照重要程度可以分为秘密、机密和绝密。不同分级的信息使用相应分级的保护手段。其中国家安全局、保密局为相应的主管部门

(2) 信息安全等级保护:

针对于国家信息、公民、法人和组织的信息以及其它社会信息进行相应的分级保护。其中等级保护的核心为分类以及保护。其可以分为系统定级、安全备案、建设整改、等级测评、监督检查等几个步骤。其中系统的备案为核心，其所保护的对象为信息系统

68. VPN的分类:

(1) VPN可按照协议层面进行分类 (IPsec / SSL VPN)

(2) VPN可以按照访问方式进行分类:

其可以分为远程访问VPN以及网关—网关VPN

其中远程访问VPN：主要用于VPN客户端与VPN网关之间的链接

而网关—网关VPN：主要用于网关与网关直接的链接的VPN

其又可分为内联网以及相应的外联网

通 大 学 答 题 纸

至 20____ 学年 第____学期)

姓名 杨一凡
520021911080

69. (1) 一次一密：

其中所采取的密钥为随机的，并且仅仅只使用一次，因此即便攻击者获得了此时间的密文和密钥也没有办法获取下一时刻的密钥。因此，其在理论上为安全的

(2) 存在的问题：

① 生成大规模的随机密钥存在一定的难度

② 密钥的分配与管理存在一定的难度

70. 防火墙的局限性：

(1) 其并不对内部的攻击进行相应的防范

(2) 其并不对绕过防火墙的攻击进行相应的防范

(3) 其并不对计算机病毒或恶意程序进行相应的防范

(4) 防火墙并不可以处理一些新型的攻击手段

71. 目前网络空间所面临的形势：① 计算机病毒层出不穷
② 黑客攻击的常态化
③ 设计工艺上的不完善，导致设备存在相应的漏洞
④ 各国加紧对于信息战的研究

网络空间安全所面临的威胁：① 信息的泄露 ② 完整性破坏 ③ 拒绝服务 ④ 非法使用

P2DR 基于时间的网络安全模型的构成：安全策略、防护、监测以及响应

因此由上述内容可知，我们可以从以下几个方面来进行安全防护的加强：

① 采取更加先进的安全策略，其中安全策略是信息安全的核心内容。

② 可以改进防护、监测以及响应的手段：a. 可以使用更加先进的防火墙，从而可以把安全保障在其OSI工作的层与协议上进行升级，得到最合适的防火墙。

b. 可以使用更加先进的异常监测的IDS，从而可以对入侵进行相应的防护以及监测的响应效果

通 大 学 答 题 纸

至 20____ 学年 第____学期)

姓名 杨一凡

520021911080

c. 可以使用更加先进的计算机病毒查杀手段

从而对计算机病毒有更加高的防护能力.

可以利用云存储，人工智能/大数据抓取查杀

d. 可以使用更加先进的漏洞扫描技术.

从而可以更快的进行漏洞的检查.

② 可以完善对更加成熟的安全手段.

可以使用以下的多大安全机制. 认证. 加密. 访问控制. 数据完整性

以制交换. 路由控制. 公证. 以及流量填充

从而可以减小安全威胁,

③ 可以实施相应的风险管理:

进行更加完善的风险认为风险控制手段.

12 其中的代码为:

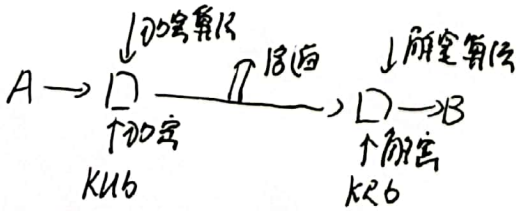
(1) 加密算法分解密算法不相同. 可以进一步增强通信的安全性与相应的灵活性

(2) 明文以密文双方进行通信的过程. 从而使过程更加安全

(3) 还可进行数字签名身份认证. 从而可以进一步保证安全性 (4) 改动更难改破

(4) 并且可以进行加密解密双方的把握

相应的通信过程.



其中 A发送自使用B的公钥 KUb 进行

相应信息的加密. 以及 B接收到信息之后

使用自己的私钥 KRb 进行相应的解密

从而可以建立安全的通信

其中公钥用于加密分签名的认证

而私钥可以用于解密分签名