内 容 简 介

信息安全工程师考试是计算机技术与软件专业技术资格（水平）考试的中级职称考试，是历年各级考试报名的热点之一。本书汇集了从 2018 年到 2022 年的所有试题和权威的解析，欲参加考试的考生认真读懂本书的内容后，将会更加深入理解考试的出题思路，发现自己的知识薄弱点，使学习更加有的放矢，对提升通过考试的信心会有极大的帮助。

本书适合参加信息安全工程师考试的考生备考使用。

图书在版编目（CIP）数据

信息安全工程师 2018 至 2022 年试题分析与解答 / 计算机技术与软件专业技术资格考试研究部主编. -- 北京 : 清华大学出版社, 2024. 8. -- (全国计算机技术与软件专业技术资格（水平）考试指定用书). -- ISBN 978-7-302-67117-6

Ⅰ. TP309-44

中国国家版本馆 CIP 数据核字第 2024JM3332 号

责任编辑：杨如林　邓甄臻
封面设计：杨玉兰
责任校对：徐俊伟
责任印制：

出版发行：清华大学出版社
网　　址：https://www.tup.com.cn，https://www.wqxuetang.com
地　　址：北京清华大学学研大厦 A 座　　邮　编：100084
社 总 机：010-83470000　　邮　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：
经　　销：全国新华书店
开　　本：185mm×230mm　**印　张：**11.75　**防伪页：**1　**字　数：**277 千字
版　　次：2024 年 8 月第 1 版　　**印　次：**2024 年 8 月第 1 次印刷
定　　价：49.00 元

产品编号：103168-01

前　言

根据国家有关的政策性文件，全国计算机技术与软件专业技术资格（水平）考试（以下简称“计算机软件考试”）已经成为计算机软件、计算机网络、计算机应用、信息系统、信息服务领域高级工程师、工程师、助理工程师（技术员）国家职称资格考试。而且，根据信息技术人才年轻化的特点和要求，报考这种资格考试不限学历与资历条件，以不拘一格选拔人才。现在，软件设计师、程序员、网络工程师、数据库系统工程师、系统分析师、系统架构设计师和信息系统项目管理师等资格的考试标准已经实现了中国与日本互认，程序员和软件设计师等资格的考试标准已经实现了中国与韩国互认。

计算机软件考试规模发展很快，年报考规模已超过 100 万人，至今累计报考人数超过 900 万。

计算机软件考试已经成为我国著名的 IT 考试品牌，其证书的含金量之高已得到社会的公认。计算机软件考试的有关信息见网站www.ruankao.org.cn中的资格考试栏目。

对考生来说，学习历年试题分析与解答是理解考试大纲的最有效、最具体的途径之一。

为帮助考生复习备考，计算机技术与软件专业技术资格考试研究部汇集了信息安全工程师 2018 至 2022 年的试题分析与解答，以便于考生测试自己的水平，发现自己的弱点，更有针对性、更系统地学习。

计算机软件考试的试题质量高，包括了职业岗位所需的各个方面的知识和技术，不但包括技术知识，还包括法律法规、标准、专业英语、管理等方面的知识；不但注重广度，而且还有一定的深度；不但要求考生具有扎实的基础知识，还要具有丰富的实践经验。

这些试题中，包含了一些富有创意的试题，一些与实践结合得很好的试题，一些富有启发性的试题，具有较高的社会引用率，对学校教师、培训指导者、研究工作者都是很有帮助的。

由于编者水平有限，时间仓促，书中难免有错误和疏漏之处，诚恳地期望各位专家和读者批评指正，对此，我们将深表感激。

编者

2024 年 4 月

目　录

第 1 章　2018 上半年信息安全工程师

上午试题分析与解答

试题（1）

2016 年 11 月 7 日，十二届全国人大常委会第二十四次会议以 154 票赞成、1 票弃权，表决通过了《中华人民共和国网络安全法》。该法律由全国人民代表大会常务委员会于 2016 年 11 月 7 日发布，自__（1）__起施行。

（1）A．2017 年 1 月 1 日　　B．2017 年 6 月 1 日

C．2017 年 7 月 1 日　　D．2017 年 10 月 1 日

试题（1）分析

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于 2016 年 11 月 7 日通过，自 2017 年 6 月 1 日起施行。

参考答案

（1）B

试题（2）

近些年，基于标识的密码技术受到越来越多的关注，标识密码算法的应用也得到了快速发展。我国国密标准中的标识密码算法是__（2）__。

（2）A．SM2　　B．SM3　　C．SM4　　D．SM9

试题（2）分析

本题考查我国商用密码的相关知识。

标识密码将用户的标识（如邮件地址、手机号码、QQ 号码等）作为公钥，省略了交换数字证书和公钥过程，使得安全系统变得易于部署和管理，非常适合端对端离线安全通信、云端数据加密、基于属性加密、基于策略加密的各种场合。2008 年标识密码算法正式获得国家密码管理局颁发的商密算法型号：SM9（商密九号算法），为我国标识密码技术的应用奠定了坚实的基础。

参考答案

（2）D

试题（3）

《计算机信息系统安全保护等级划分准则》（GB 17859—1999）中规定了计算机系统安全保护能力的五个等级，其中要求对所有主体和客体进行自主和强制访问控制的是__（3）__。

（3）A．用户自主保护级　　B．系统审计保护级

C．安全标记保护级　　D．结构化保护级

试题（3）分析

本题考查计算机信息系统安全等级保护相关知识。

GB 17859—1999 标准规定了计算机系统安全保护能力的五个等级：第一级为用户自主保护级；第二级为系统审计保护级；第三级为安全标记保护级；第四级为结构化保护级；第五级为访问验证保护级。

其中，第四级结构化保护级的计算机信息系统可信计算建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。

参考答案

（3）D

试题（4）

密码分析者针对加解密算法的数学基础和某些密码学特性，根据数学方法破译密码的攻击方式称为__（4）__。

（4）A．数学分析攻击　　B．差分分析攻击

C．基于物理的攻击　　D．穷举攻击

试题（4）分析

本题考查密码分析方法的相关知识。

数学分析攻击是密码分析者针对加解密算法的数学基础和某些密码学特性，通过数学求解的方法来破译密码。

参考答案

（4）A

试题（5）

《中华人民共和国网络安全法》明确了国家落实网络安全工作的职能部门和职责，其中明确规定，由__（5）__负责统筹协调网络安全工作和相关监督管理工作。

（5）A．中央网络安全与信息化小组　　B．国务院

C．国家网信部门　　D．国家公安部门

试题（5）分析

本题考查网络安全法相关法条的基础知识。

《中华人民共和国网络安全法》第八条明确规定了网信部门是负责统筹和监督网络安全工作的机构。管理归属网信部门，企业需积极配合。

参考答案

（5）C

试题（6）

一个密码系统如果用 E 表示加密运算，D 表示解密运算，M 表示明文，C 表示密文，则下面描述必然成立的是__（6）__。

（6）A．E(E(M))=C　　B．D(E(M))=M

C．D(E(M))=C　　D．D(D(M))=M

试题（6）分析

本题考查对称密码系统加密和解密之间的关系。

对消息 M 加密以后再用相同密钥解密就可以恢复消息明文 M。

参考答案

（6）B

试题（7）

S/Key 口令是一种一次性口令生成方案，它可以对抗__（7）__。

（7）A．恶意代码攻击　　B．暴力分析攻击

C．重放攻击　　D．协议分析攻击

试题（7）分析

本题考查一次性口令生成方案的安全性。

S/Key 每次使用时临时生成一个口令，从而可以有效抵御口令的重放攻击。

参考答案

（7）C

试题（8）

面向数据挖掘的隐私保护技术主要解决高层应用中的隐私保护问题，致力于研究如何根据不同数据挖掘操作的特征来实现对隐私的保护。从数据挖掘的角度，不属于隐私保护技术的是__（8）__。

（8）A．基于数据分析的隐私保护技术　　B．基于数据失真的隐私保护技术

C．基于数据匿名化的隐私保护技术　　D．基于数据加密的隐私保护技术

试题（8）分析

本题考查隐私保护技术。

利用数据挖掘实现隐私保护技术可以通过数据失真、数据匿名化和数据加密来实现。

参考答案

（8）A

试题（9）

从网络安全的角度看，以下原则中不属于网络安全防护体系在设计和实现时需要遵循的基本原则的是__（9）__。

（9）A．最小权限原则　　B．纵深防御原则

C．安全性与代价平衡原则　　D．Kerckhoffs 原则

试题（9）分析

本题考查网络安全系统设计需要遵循的基本原则。

Kerckhoffs 准则认为，一个安全保护系统的安全性不是建立在它的算法对于对手来说是保密的，而是应该建立在它所选择的密钥对于对手来说是保密的。这显然不是网络安全在防护设计时所包含的内容。

参考答案

（9）D

试题（10）

恶意软件是目前移动智能终端上被不法分子利用最多、对用户造成危害和损失最大的安全威胁类型。数据显示，目前安卓平台恶意软件主要有__（10）__四种类型。

（10）A．远程控制木马、话费吸取类、隐私窃取类和系统破坏类

B．远程控制木马、话费吸取类、系统破坏类和硬件资源消耗类

C．远程控制木马、话费吸取类、隐私窃取类和恶意推广

D．远程控制木马、话费吸取类、系统破坏类和恶意推广

试题（10）分析

本题考查安卓平台下的恶意软件分类方法。

利用安卓手机移动平台传播恶意软件是目前主流传播途径，涉及的主要类型有远控、吸费、窃取隐私和破坏系统。

参考答案

（10）A

试题（11）

以下关于认证技术的描述中，错误的是__（11）__。

（11）A．身份认证是用来对信息系统中实体的合法性进行验证的方法

B．消息认证能够验证消息的完整性

C．数字签名是十六进制的字符串

D．指纹识别技术包括验证和识别两个部分

试题（11）分析

本题考查身份认证技术。

数字签名是只有信息的发送者才能产生而别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者所发送信息真实性的一个有效证明。数字签名的本质是消息进行某种计算得到包含用户特定特征的字符串，十六进制只是其中的一种表示形式而已。

参考答案

（11）C

试题（12）

对信息进行均衡、全面的防护，提高整个系统“安全最低点”的安全性能，这种安全原则被称为__（12）__。

（12）A．最小特权原则　　B．木桶原则

C．等级化原则　　D．最小泄露原则

试题（12）分析

本题考查网络安全系统设计原则。

网络信息安全的木桶原则是指对信息均衡、全面地进行保护。木桶的最大容积取决于最短的一块木板。安全机制和安全服务设计的首要目的是防止最常用的攻击手段，根本目的是提高整个系统的“安全最低点”的安全性能。

参考答案

（12）B

试题（13）

网络安全技术可以分为主动防御技术和被动防御技术两大类，以下属于主动防御技术的是（13）。

（13）A．蜜罐技术　　B．入侵检测技术
　　C．防火墙技术　　D．恶意代码扫描技术

试题（13）分析

本题考查主动和被动安全防御技术。

上述安全防御技术中，只有蜜罐技术利用信息欺骗技术，主动获取攻击者的各种攻击信息，学习攻击使用的行为、方法和手段。

参考答案

（13）A

试题（14）

如果未经授权的实体得到了数据的访问权，这属于破坏了信息的（14）。

（14）A．可用性　　B．完整性
　　C．机密性　　D．可控性

试题（14）分析

本题考查网络安全的安全目标。

网络信息安全与保密的目标主要表现在系统的机密性、完整性、真实性、可靠性、可用性、不可抵赖性等方面。机密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。

参考答案

（14）C

试题（15）

按照密码系统对明文的处理方法，密码系统可以分为（15）。

（15）A．对称密码系统和公钥密码系统　　B．对称密码系统和非对称密码系统
　　C．数据加密系统和数字签名系统　　D．分组密码系统和序列密码系统

试题（15）分析

本题考查密码系统组成的基础知识。

密码系统通常从 3 个独立的方面进行分类：

一是按将明文转化为密文的操作类型分为替换密码和移位密码；

二是按明文的处理方法可分为分组密码（块密码）和序列密码（流密码）；

三是按密钥的使用个数分为对称密码体制和非对称密码体制。

参考答案

（15）D

试题（16）

数字签名是对以数字形式存储的消息进行某种处理，产生一种类似于传统手书签名功效的信息处理过程。实现数字签名最常见的方法是__（16）__。

（16）A．数字证书和 PKI 系统相结合

B．对称密码体制和 MD5 算法相结合

C．公钥密码体制和单向安全 Hash 函数算法相结合

D．公钥密码体制和对称密码体制相结合

试题（16）分析

本题考查数字签名的相关知识。

数字签名就是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。数字签名是非对称密钥加密技术与数字摘要技术的应用。

参考答案

（16）C

试题（17）

以下选项中，不属于生物识别方法的是__（17）__。

（17）A．掌纹识别　　B．个人标记号识别　　C．人脸识别　　D．指纹识别

试题（17）分析

本题考查身份认证技术与生物识别技术。

生物识别技术是通过计算机与光学、声学、生物传感器和生物统计学原理等高科技手段密切结合，利用人体固有的生理特性（如指纹、脸、虹膜等）和行为特征（如笔迹、声音、步态等）来进行个人身份的鉴定。

参考答案

（17）B

试题（18）

计算机取证是将计算机调查和分析技术应用于对潜在的、有法律效力的证据的确定与提取。以下关于计算机取证的描述中，错误的是__（18）__。

（18）A．计算机取证包括保护目标计算机系统、确定收集和保存电子证据，必须在开机的状态下进行

B．计算机取证围绕电子证据进行，电子证据具有高科技性、无形性和易破坏性等特点

C．计算机取证包括对以磁介质编码信息方式存储的计算机证据的保护、确认、提取和归档

D．计算机取证是一门在犯罪进行过程中或之后收集证据的技术

试题（18）分析

本题考查计算机犯罪和取证相关的基础知识。

计算机取证可以在离线或者在线状态下完成。

参考答案

（18）A

试题（19）

在缺省安装数据库管理系统 MySQL 后，root 用户拥有所有权限且是空口令。为了安全起见，必须为 root 用户设置口令。以下口令设置方法中，不正确的是__（19）__。

（19）A．使用 MySQL 自带的命令 mysqladmin 设置 root 口令

B．使用 set password 设置口令

C．登录数据库，修改数据库 MySQL 下 user 表的字段内容设置口令

D．登录数据库，修改数据库 MySQL 下的访问控制列表内容设置口令

试题（19）分析

本题考查口令安全和数据库安全操作。

修改数据库 MySQL 下的访问控制列表是无法完成口令设置的。

参考答案

（19）D

试题（20）

数字水印技术通过在多媒体数据中嵌入隐蔽的水印标记，可以有效实现对数字多媒体数据的版权保护等功能。以下不属于数字水印在数字版权保护中必须满足的基本应用需求的是__（20）__。

（20）A．保密性　　B．隐蔽性　　C．可见性　　D．完整性

试题（20）分析

本题考查数字水印技术。

数字版权标识水印是目前研究最多的一类数字水印。数字作品既是商品，又是知识作品，这种双重性决定了版权标识水印主要强调隐蔽性、保密性、鲁棒性，而对数据量的要求相对较小。

参考答案

（20）C

试题（21）

__（21）__是一种通过不断对网络服务系统进行干扰，影响其正常的作业流程，使系统响应减慢甚至瘫痪的攻击方式。

（21）A．暴力攻击　　B．拒绝服务攻击　　C．重放攻击　　D．欺骗攻击

试题（21）分析

本题考查常见的网络攻击方法。

拒绝服务攻击是攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一。对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。

参考答案

（21）B

试题（22）

在访问因特网时，为了防止 Web 页面中恶意代码对自己计算机的损害，可以采取的防范措施是__（22）__。

（22）A．将要访问的 Web 站点按其可信度分配到浏览器的不同安全区域

B．利用 SSL 访问 Web 站点

C．在浏览器中安装数字证书

D．利用 IP 安全协议访问 Web 站点

试题（22）分析

本题考查互联网安全使用的常识。

要阻止恶意代码对计算机的破坏，必须限制页面中恶意代码的权限或者禁止其执行，选项中只有 A 有此功能。

参考答案

（22）A

试题（23）

下列说法中，错误的是__（23）__。

（23）A．数据被非授权地增删、修改或破坏都属于破坏数据的完整性

B．抵赖是一种来自黑客的攻击

C．非授权访问是指某一资源被某个非授权的人，或以非授权的方式使用

D．重放攻击是指出于非法目的，将所截获的某次合法的通信数据进行拷贝而重新发送

试题（23）分析

本题考查常规网络攻击和网络安全的基本概念。

抵赖是事后否认某些网络行为，与黑客没有关系。

参考答案

（23）B

试题（24）

Linux 系统的运行日志存储的目录是__（24）__。

（24）A．/var/log　　B．/usr/log　　C．/etc/log　　D．/tmp/log

试题（24）分析

本题考查主机安全和日志安全。

Linux 系统默认配置下，日志文件通常都保存在“/var/log”目录下。

参考答案

（24）A

试题（25）

电子邮件已经成为传播恶意代码的重要途径之一，为了有效防止电子邮件中的恶意代码，应该用__（25）__的方式阅读电子邮件。

（25）A．应用软件　　B．纯文本　　C．网页　　D．在线

试题（25）分析

本题考查电子邮件传播恶意代码的载体。

根据恶意代码的形式和执行方法，通过纯文本方式打开邮件可以防止恶意代码被执行，从而避免中毒。

参考答案

（25）B

试题（26）

已知 DES 算法 S 盒如下：

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

如果该 S 盒的输入为 100010，则其二进制输出为__（26）__。

（26）A．0110　　B．1001　　C．0100　　D．0101

试题（26）分析

本题考查 DES 加密算法的 S 盒替换运算。

根据 S 盒运算规则，第一、六位确定行：10=2，第二、三、四、五确定列：0001=1，从而唯一确定元素 6，再转换成二进制。

参考答案

（26）A

试题（27）

以下关于 TCP 协议的描述，错误的是__（27）__。

（27）A．TCP 是 Internet 传输层的协议，可以为应用层的不同协议提供服务

B．TCP 是面向连接的协议，提供可靠、全双工的、面向字节流的端到端的服务

C．TCP 使用二次握手来建立连接，具有很好的可靠性

D．TCP 每发送一个报文段，就对这个报文段设置一次计时器

试题（27）分析

本题考查计算机网络协议的基础知识。

TCP 作为可靠的传输协议，在真正开始数据传输之前需要三次握手建立连接，而不是二次握手。

参考答案

（27）C

试题（28）

Kerberos 是一种常用的身份认证协议，它采用的加密算法是__（28）__。

（28）A．Elgamal　　B．DES　　C．MD5　　D．RSA

第 2 章　2018 上半年信息安全工程师下午试题分析与解答

试题一（共 15 分）

阅读下列说明，回答问题 1 至问题 4，将解答填入答题纸的对应栏内。

【说明】

恶意代码是指为达到恶意目的而专门设计的程序或者代码。常见的恶意代码类型有：特洛伊木马、蠕虫、病毒、后门、Rootkit、僵尸程序、广告软件。

2017 年 5 月，勒索软件 WannaCry 席卷全球，国内大量高校及企事业单位的计算机被攻击，文件及数据被加密后无法使用，系统或服务无法正常运行，损失巨大。

【问题 1】（2 分）

按照恶意代码的分类，此次爆发的恶意软件属于哪种类型？

【问题 2】（2 分）

此次勒索软件针对的攻击目标是 Windows 还是 Linux 类系统？

【问题 3】（6 分）

恶意代码具有的共同特征是什么？

【问题 4】（5 分）

由于此次勒索软件需要利用系统的 SMB 服务漏洞（端口号 445）进行传播，我们可以配置防火墙过滤规则来阻止勒索软件的攻击，请填写表 1-1 中的空（1）～（5），使该过滤规则完整。

表 1-1　防火墙过滤规则表

规则号	源地址	目的地址	源端口	目的端口	协议	ACK	动作
1	（1）	1.2.3.4	（2）	（3）	（4）	（5）	拒绝
…	…	…	…	…	…	…	…
…	*	*	*	*	*	*	拒绝

注：假设本机 IP 地址为：1.2.3.4 ，“*”表示通配符。

试题一分析

本题综合了恶意代码的基本知识以及如何同防火墙联动阻止恶意代码的攻击行为，考查考生对恶意代码基本概念的理解程度以及防火墙过滤规则的设置能力。

【问题 1】

病毒、蠕虫和特洛伊木马是可导致用户计算机和计算机上的信息损坏的恶意程序。

病毒的明确定义是“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影

响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。病毒必须满足两个条件。

（1）它必须能自行执行。它通常将自己的代码置于另一个程序的执行路径中。

（2）它必须能自我复制。例如，它可能用受病毒感染的文件副本替换其他可执行文件。病毒既可以感染桌面计算机，也可以感染网络服务器。

蠕虫是一种通过网络传播的恶性病毒，它具有病毒的一些共性，如传播性、隐蔽性、破坏性等等，同时具有自己的一些特征，如不利用文件寄生（有的只存在于内存中），对网络造成拒绝服务，以及和黑客技术相结合，等等。

木马是指那些表面上是有用的软件、实际目的却是危害计算机安全并导致严重破坏的计算机程序。它是具有欺骗性的文件（宣称是良性的，但事实上是恶意的），是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。

此次勒索软件是通过系统漏洞实现网络的自动传播，并完成其各种恶意功能。

【问题 2】

该勒索软件利用的 Windows 系统的安全漏洞，因此其攻击目标也是 Windows 类系统。

【问题 3】

总地来说，恶意代码首先就是具有恶意目的，不管是造成网络瘫痪还是窃取个人隐私目的是恶意的；其次这些恶意代码通常都是完整的计算机程序，可以实现自我传播或者感染其他程序；最后恶意代码需要被执行才能发挥其恶意的功能，恶意代码如果没有执行的可能，就无法达到其恶意目的。

【问题 4】

针对该勒索软件的攻击和传播特点，需要对 SMB 服务所在的 445 端口进行过滤，只要网外对网内 445 端口的所有连接请求予以过滤。需要注意的是 SMB 服务是基于 TCP 协议的。

参考答案

【问题 1】

蠕虫。

【问题 2】

Windows。

【问题 3】

具有恶意的目的；自身是计算机程序；通过执行发生作用。

【问题 4】

（1）*.*.*.*

（2）*

（3）445

（4）TCP

（5）*

试题二（共 15 分）

阅读下列说明和图，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。

【说明】

密码学的基本目标是在有攻击者存在的环境下，保证通信双方（A 和 B）之间能够使用不安全的通信信道实现安全通信。密码技术能够实现信息的保密性、完整性、可用性和不可否认性等安全目标。一种实用的保密通信模型往往涉及对称加密、公钥密码、Hash 函数、数字签名等多种密码技术。

在以下描述中，M 表示消息，H 表示 Hash 函数，E 表示加密算法，D 表示解密算法，K 表示密钥，SK_A 表示 A 的私钥，PK_A 表示 A 的公钥，SK_B 表示 B 的私钥，PK_B 表示 B 的公钥，||表示连接操作。

【问题 1】（6 分）

用户 AB 双方采用的保密通信的基本过程如图 2-1 所示。

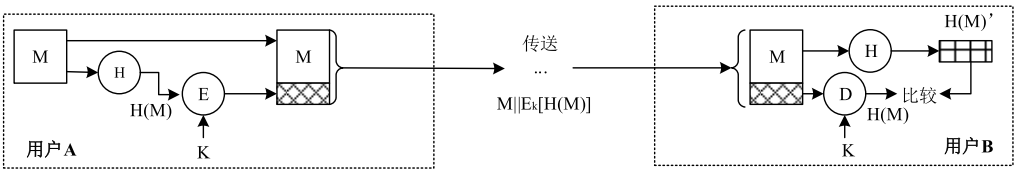

图 2-1　保密通信模型一

请问图 2-1 所设计的保密通信模型能实现信息的哪些安全目标？图 2-1 中的用户 A 侧的 H 和 E 能否互换计算顺序？如果不能互换请说明原因，如果能互换请说明对安全目标的影响。

【问题 2】（4 分）

图 2-2 给出了另一种保密通信的基本过程。

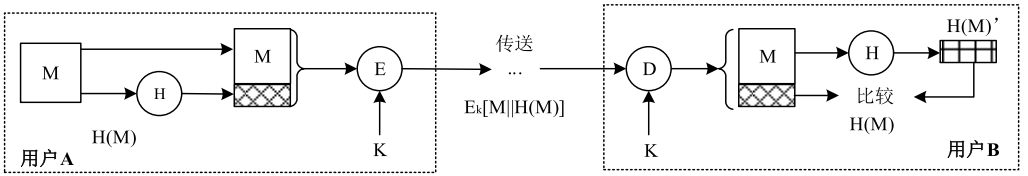

图 2-2　保密通信模型二

请问图 2-2 设计的保密通信模型能实现信息安全的哪些特性？

【问题 3】（5 分）

为了在传输过程中能够保障信息的保密性、完整性和不可否认性，设计了一个安全通信模型结构如图 2-3 所示。

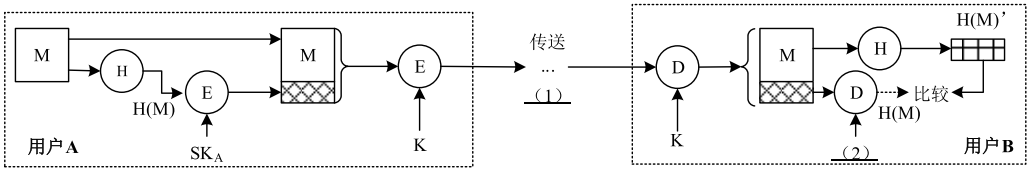

图 2-3　保密通信模型三

请问图 2-3 中__（1）__、__（2）__分别应该填什么内容？

试题二分析

本题主要考查保密通信所涉及的关键技术，信息安全所涉及哈希、加解密、安全通信等之间的关系以及在实际安全通信中的应用。

【问题 1】

在保密通信模型一当中，首先消息 M 是没有加密的，关键是对消息 M 计算哈希值然后对哈希进行了加密，因此重点实现的是对消息 M 的完整性目标。由此可知，先计算哈希值还是先对 M 加密后再计算哈希值，都不会影响该安全目标。

【问题 2】

模型二相对模型一的最大区别就是，消息 M 被加密了，因此在模型一的基础上，增加了保密性的目标。

【问题 3】

本问题综合考查各种安全目标的实现技术。在此模型下，增加了不可否认的目标实现。此时需要发送者用私钥签名，接收端用公钥验证签名。

对于空（1），要求考生清楚整个签名过程的细节和各个要素的作用，而空（2）只要用对应的公钥去解密哈希值即可。

参考答案

【问题 1】

完整性；可以互换；不影响完整性安全目标。

【问题 2】

保密性和完整性。

【问题 3】

（1）$E_K[M \| E_{SK_A}[H(M)]]$

（2）PK_A

试题三（共 15 分）

阅读下列说明，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。

【说明】

在 Linux 系统中，用户账号是用户的身份标志，它由用户名和用户口令组成。

【问题 1】（4 分）

Linux 系统将用户名和口令分别保存在哪些文件中？

【问题 2】（7 分）

Linux 系统的用户名文件通常包含如下形式的内容：

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
hujw:x:500:500:hujianwei:/home/hujw:/bin/bash
```

文件中的一行记录对应着一个用户，每行记录又用冒号（:）分隔为 7 个字段，请问第一个冒号（第二列）和第二个冒号（第三列）的含义是什么？

上述用户名文件中，第三列的数字分别代表什么含义？

【问题 3】（4 分）

Linux 系统中用户名文件和口令字文件的默认访问权限分别是什么？

试题三分析

本题考查 Linux 系统安全相关问题，主要是对 Linux 系统中用户和口令的安全管理以及文件的访问权限等知识点进行考察。

【问题 1】

Linux 系统中用户和口令是分开保存的。用户名信息主要保存在/etc/passwd 文件中，而口令信息这是通过哈希加盐处理后保存在/etc/shadow 的影子文件中。

【问题 2】

题目给出的是/etc/passwd 文件中的部分内容，每一行代表一个用户及其信息，每行格式及用冒号分隔的字段含义是：

用户名:口令: 用户标识号:组标识号:注释性描述:主目录:登录 Shell。

其中，口令都是用 x 表示，单独在口令字文件中保存。第三列表示的用户的组别信息。

【问题 3】

通常情况下，用户名文件是系统中所有用户可读的，但只有 root 有修改权限。采用标准的 Linux 系统访问控制来描述就是 rwxr--r--，用数字表示就是 744。而口令字文件只有 root 用户有权读写，其他用户是没有任何权限的，因此其访问权限模式是：400 或者 600。

参考答案

【问题 1】

/etc/passwd　　/etc/shadow

【问题 2】

用户名:口令: 用户标识号:组标识号:注释性描述:主目录:登录 Shell。

超级用户（0），系统管理账号（1-99），普通账号（500）。

【问题 3】

数字形式：744（2 分），400（600）

或

文字形式：用户名文件全局可读（2 分），口令字文件只有超级用户可读（写）。

试题四（共 15 分）

阅读下列说明和 C 语言代码，回答问题 1 至问题 4，将解答写在答题纸的对应栏内。

【说明】

在客户服务器通信模型中，客户端需要每隔一定时间向服务器发送数据包，以确定服务器是否掉线，服务器也能以此判断客户端是否存活。这种每隔固定时间发一次的数据包也称为心跳包。心跳包的内容没有什么特别的规定，一般都是很小的包。

某系统采用的请求和应答两种类型的心跳包格式如图 4-1 所示。

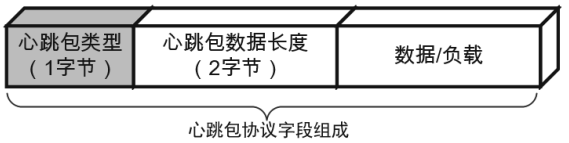

图 4-1 协议包格式

心跳包类型占 1 个字节，主要是请求和响应两种类型；心跳包数据长度字段占 2 个字节，表示后续数据或者负载的长度。

接收端收到该心跳包后的处理函数是 process_heartbeat()，其中参数 p 指向心跳包的报文数据，s 是对应客户端的 socket 网络通信套接字。

```
void process_heartbeat(unsigned char *p, SOCKET s)
{
    unsigned short hbtype;
    unsigned int payload;
    hbtype=*p++;              //心跳包类型
    n2s(p, payload);          //心跳包数据长度
    pl=p;                     //pl 指向心跳包数据
    if (hbtype==HB_REQUEST) {
        unsigned char *buffer, *bp;
        buffer=malloc(1+2+payload);
        bp=buffer;            //bp 指向刚分配的内存
        *bp++=HB_RESPONSE;  //填充 1 byte 的心跳包类型
        s2n(payload, bp);   //填充 2 bytes 的数据长度
        memcpy(bp, pl, payload);
        /* 将构造好的心跳响应包通过 socket s 返回给客户端 */
        r=write_bytes(s, buffer, 3+payload);
    }
}
```

【问题 1】（4 分）

（1）心跳包数据长度字段的最大取值是多少？

（2）心跳包中的数据长度字段给出的长度值是否必须和后续的数据字段的实际长度一致？

【问题 2】（5 分）

（1）上述接收代码存在什么样的安全漏洞？