全国计算机技术与软件专业技术资格（水平）考试

2016 年下半年 信息安全工程师 下午试卷 I

（考试时间 14:00～16:30 共 150 分钟）

请按下述要求正确填写答题纸

1. 本试卷共五道题，全部为必答题，每题 25 分，满分 75 分。
2. 在答题纸的指定位置填写你所在的省、自治区、直辖市、计划单列市的名称。
3. 在答题纸的指定位置填写准考证号、出生年月日和姓名。
4. 答题纸上除填写上述内容外只能写解答。
5. 解答时字迹务必清楚，字迹不清时，将不评分。

试题一（共 20 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】

研究密码编码的科学称为密码编码学，研究密码破译的科学称为密码分析学，密码编码学和密码分析学共同组成密码学。密码学作为信息安全的关键技术，在信息安全领域有着广泛的应用。

【问题 1】（9 分）

密码学的安全目标至少包括哪三个方面？具体内涵是什么？

【问题 2】（3 分）

对下列违规安全事件，指出各个事件分别违反了安全目标中的哪些项？

（1）小明抄袭了小丽的家庭作业。

（2）小明私自修改了自己的成绩。（3）小李窃取了小刘的学位证号码、登录口令信息、并通过学位信息系统更改了小刘的学位信息记录和登陆口令，将系统中小刘的学位信息用一份伪造的信息替代，造成小刘无法访问学位信息系统。

【问题 3】（3 分）

现代密码体制的安全性通常取决于密钥的安全，为了保证密钥的安全，密钥管理包括哪些技术问题？

【问题 4】（5 分）

在图 1-1 给出的加密过程中，M_i，i=1，2，…，n 表示明文分组，C_i，i=1,2，…，n 表示密文分组，Z 表示初始序列，K 表示密钥，E 表示分组加密过程。该分组加密过程属于哪种工作模式？这种分组密码的工作模式有什么缺点？

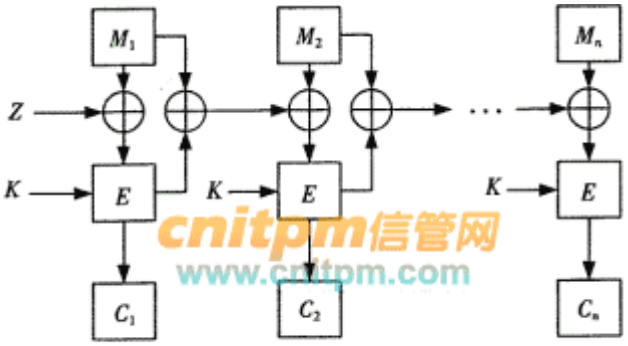

图1-1

信管网参考答案：

参考答案：

【问题一】

（1）保密性：保密性是确保信息仅被合法用户访问，而不被地露给非授权的用户、实体或过程，或供其利用的特性。即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。

（2）完整性：完整性是指所有资源只能由授权方或以授权的方式进行修改，即信息未经授权不能进行改变的特性。信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

（3）不可抵赖性：不可抵赖性也称作不可否认性，在网络信息系统的信息交互过程中，确信参与者的真实同一性。即，所有参与者都不可能否认或抵赖曾经完成的操作和承诺。

（3）可用性：可用性是指所有资源在适当的时候可以由授权方访问，即信息可被授权实体访问并按需求使用的特性。信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

【问题二】

（1）保密性

（2）完整性
（3）可用性
【问题三】
答：密钥管理包括密钥的产生、存储、分配、组织、使用、停用、更换、销毁等一系列技术问题。
【问题四】
明密文链接模式。**密码分组链接模式**

优点：

1.不容易主动攻击,安全性好于 ECB,适合传输长度长的报文,是 SSL、IPSec 的标准。

缺点：

1.不利于并行计算；
2.误差传递；
3.需要初始化向量 IV

缺点：当 Mi 或 Ci 中发生一位错误时，自此以后的密文全都发生错误，即具有错误传播无界的特性，不利于磁盘文件加密。并且要求数据的长度是密码分组长度的整数倍，否则最后一个数据块将是短块，这时需要特殊处理。

最终答案以信管网题库为准：http://www.cnitpm.com/zt/2016xaqcf/

试题二（共 10 分）

阅读下列说明和图，回答问题 1 至问题 2，将解答填入答题纸的对应栏内。

【说明】

访问控制是对信息系统资源进行保护的重要措施，适当的访问控制能够阻止未经授权的用户有意或者无意地获取资源。访问控制一般是在操作系统的控制下，按照事先确定的规则决定是否允许用户对资源的访问。图 2-1 给出了某系统对客体 traceroute.mpg 实施的访问控制规则。

图 2-1

【问题 1】（3 分）

针对信息系统的访问控制包含哪些基本要素？

【问题 2】（7 分）

分别写出图 2-1 中用户 Administrator 对应三种访问控制实现方法，即能力表、访问控制表、访问控制矩阵下的访问控制规则。

信管网参考答案：

【问题 1】

主体、客体、授权访问

【问题二】

能力表：

（主体）Administrator <（客体）traceroute.mpg：读取，运行>

访问控制表：

（客体）traceroute.mpg<（主体）Administrator ：读取，运行>

访问控制矩阵：

	（客体）traceroute.mpg
（主体）Administrator	读取，运行

最终答案以信管网为准：http://www.cnitpm.com/zt/2016xaqcf/

试题三（共 19 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】

防火墙是一种广泛应用的网络安全防御技术，它阻挡对网络的非法访问和不安全的数据传递，保护本地系统和网络免于受到安全威胁。

图 3-1 给出了一种防火墙的体系结构。

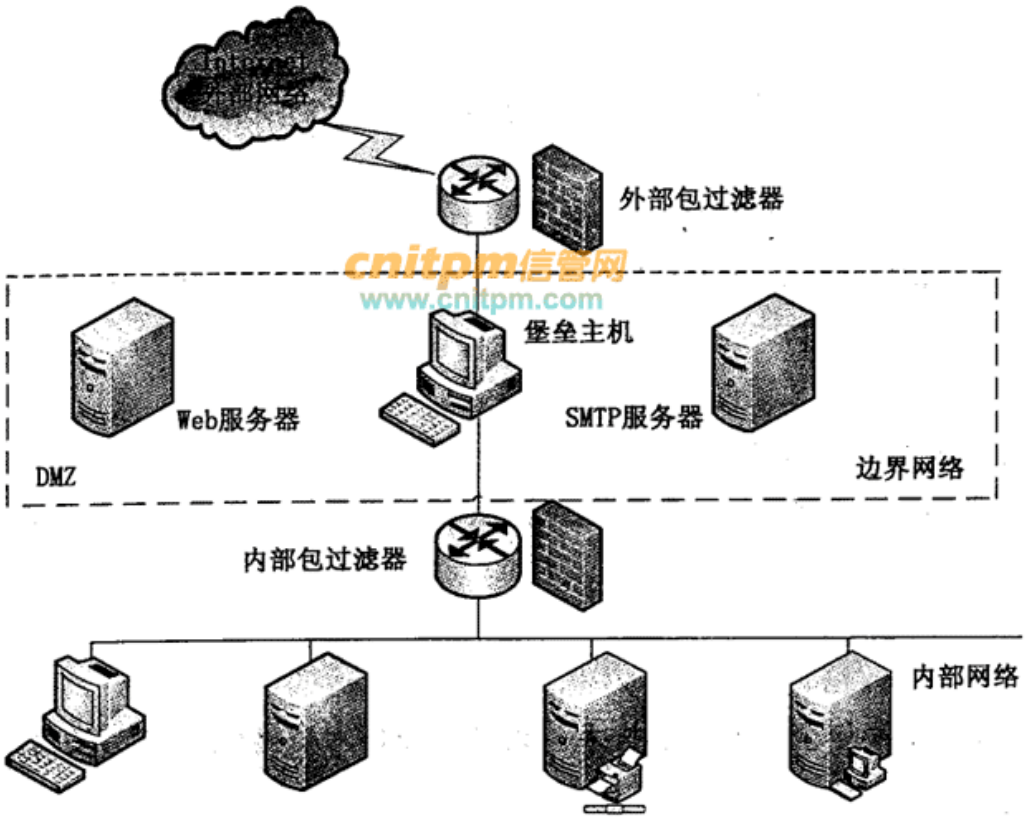

图 3-1

【问题 1】（6 分）

防火墙的体系结构主要有：

（1）双重宿主主机体系结构；

（2）（被）屏蔽主机体系结构；

（3）（被）屏蔽子网体系结构；

请简要说明这三种体系结构的特点。

【问题 2】（5 分）

（1）图 3-1 描述的是哪一种防火墙的体系结构？

（2）其中内部包过滤器和外部包过滤器的作用分别是什么？

【问题 3】（8 分）

设图 3-1 中外部包过滤器的外部 IP 地址为 10.20.100.1，内部 IP 地址为 10.20.100.2，内部包过滤器的外部 IP 地址为 10.20.100.3，内部 IP 地址为 192.168.0.1，DMZ 中 Web 服务器 IP 为 10.20.100.6，SMTP 服务器 IP 为 10.20.100.8.

关于包过滤器，要求实现以下功能，不允许内部网络用户访问外网和 DMZ，外部网络用户只允许访问 DMZ 中的 Web 服务器和 SMTP 服务器。内部包过滤器规则如表 3-1 所示。请完成外部包过滤器规则表 3-2，将对应空缺表项的答案填入答题纸对应栏内。

表3-1内部包过滤器规则表

规则号	协议	源地址	目的地址	源端口	目的端口	动作	方向
1	*	*	*	*	*	拒绝	*

表3-2外部包过滤器规则表

规则号	协议	源地址	目的地址	源端口	目的端口	动作	方向
1	TCP	*	10.20.100.6	〉1024	80	允许	入
2	TCP	10.20.100.6	*	80	〉1024	允许	出
3	TCP	(1)	(2)	〉1024	25	允许	入
4	TCP	(3)	(4)	25	〉1024	允许	出
5	(5)	(6)	*	〉1024	53	允许	入
6	(7)	*	(8)	53	〉1024	允许	出
7	*	*	*	*	*	拒绝	*

信管网参考答案：

【问题一】

双重宿主主机体系结构：双重宿主主机体系结构是指以一台双重宿主主机作为防火墙系统的主体，执行分离外部网络与内部网络的任务。双宿主机网关是用一台装有两块网卡的堡垒主机做防火墙。双宿主机的两块网卡分别与受保护的内部子网及 Internet 网络连接，起着监视和隔离应用层信息流的作用，彻底隔离了所有的内部主机与外部主机的可能连接。

被屏蔽主机体系结构：被屏蔽主机体系结构是指通过一个单独的路由器和内部网络上的堡垒主机共同构成防火墙，主要通过数据包过滤实现内外网络的隔离和对内网的保护。

屏蔽主机型防火墙也叫主机过滤防火墙，由堡垒主机和包过滤路由器组成，所有的外部主机与一个堡垒主机相连接而不让它们与内部主机直接相连。

通常在路由器上设立过滤规则，并使这个堡垒主机成为唯一可以从外部网络直接到达的主机，符合规则的数据包被传送到堡垒主机。堡垒主机的代理服务软件将允许通过的信息传输到受保护的内部网络，这就确保了内部网络不受未被授权的外部用户的攻击。

被屏蔽子网体系结构：被屏蔽子网体系结构将防火墙的概念扩充至一个由两台路由器包围起来的周边网络，并且将容易受到攻击的堡垒主机都置于这个周边网络中。其主要由四个部件构成，分别为:周边网络、外部路由器、内部路由器以及堡垒主机。

子网过滤结构是在主机过滤结构中又增加一个额外的安全层次而构成的。在内部网络和外部网络之间建立一个被隔离的子网，用两台过滤路由器将这一子网分别与内部网络和外部网络分开。增加的安全层次包括一台堡垒主机和一套路由器。两台路由器之间是一个被称为周边网络或参数网络的安全子网，也叫 DMZ（隔离区或非军事区）。使得内部网络和外部网络之间有了两层隔断。

【问题二】

（1） 屏蔽子网体系结构。

（2） 内部路由器：内部路由器用于隔离周边网络和内部网络，是屏蔽子网体系结构的第二道屏障。在其上设置了针对内部用户的访问过滤规划，对内部用户访问周边网络和外部网络进行限制。

外部路由器：外部路由器的主要作用在于保护周边网络和内部网络，是屏蔽子网体系结构的第一道屏障。在其上设置了对周边网络和内部网络进行访问的过滤规则，该规则主要针对外网用户。

【问题三】

（1）*

（2）10.20.100.8

（3）10.20.100.8

（4）*

（5）UDP

（6）10.20.100.3 **.8**

（7）UDP

（8）10.20.100.3**.8**

最终答案以信管网为准：http://www.cnitpm.com/zt/2016xaqcf/

试题四（共 18 分）

阅读下列说明，回答问题 1 至问题 4，将解答写在答题纸的对应栏内。

【说明】

用户的身份认证是许多应用系统的第一道防线、身份识别对确保系统和数据的安全保密及其重要，以下过程给出了实现用户 B 对用户 A 身份的认证过程。

1.B –> B：A

2.B –> A：{B，Nb}pk（A）

3.A –> B：b（Nb）

此处 A 和 B 是认证实体，Nb 是一个随机值，pk（A）表示实体 A 的公钥、{B，Nb}pk（A）表示用 A 的公钥对消息 BNb 进行加密处理，b（Nb）表示用哈希算法 h 对 Nb 计算哈希值。

【问题 1】（5 分）

认证和加密有哪些区别？

【问题 2】（6 分）

（1）包含在消息 2 中的“Nb”起什么作用？

（2）“Nb”的选择应满足什么条件？

【问题 3】（3 分）

为什么消息 3 中的 Nb 要计算哈希值？

【问题 4】（4 分）

上述协议存在什么安全缺陷？请给出相应的解决思路。

信管网参考答案：

【问题一】

认证和加密的区别在于：加密用以确保数据的保密性，阻止对手的被动攻击，如截取，窃听等；而认证用以确保报文发送者和接收者身份的真实性以及报文的完整性，阻止对手的主动攻击，如冒充、篡改、重播等。

【问题二】

（1） Nb 是一个随机值，只有发送方 B 和 A 知道，起到抗重放攻击作用。（对 A 的身份进行验证）

（2） 应具备随机性，不易被猜测。

【问题三】

哈希算法具有单向性，经过哈希值运算之后的随机数，即使被攻击者截获也无法对该随机数进行还原，获取该随机数 Nb 的产生信息。（我们电脑中的随机数，都是通过数学方法生成的，严格上讲不是真正的随机数，如果知道了当前的随机数，就有可能推测出下一个数）

【问题四】

1、攻击者可以通过截获 h（Nb）冒充用户 A 的身份给用户 B 发送 h（Nb）。

解决思路：用户 A 通过将 A 的标识和随机数 Nb 进行哈希运算，将其哈希值 h（A，Nb）发送给用户 B，用户 B 接收后，利用哈希函数对自己保存的用户标识 A 和随机数 Nb 进行加密，并与接收到的 h（A，Nb）进行比较。若两者相等，则用户 B 确认用户 A 的身份是真实的，否则认为用户 A 的身份是不真实的。

这个题本身描述：B 对用户 A 身份的认证过程。

2、如何保证 pk（A）是准确的，万一 pk（A）是第三方假冒的呢？我们需要使用数字证书，A 把自己的数字证书先发给 B。

最终答案以信管网为准：http://www.cnitpm.com/zt/2016xaqcf/

试题五（共 8 分）

阅读下列说明和代码，回答问题 1 和问题 2，将解答卸载答题纸的对应栏内。

【说明】

某一本地口令验证函数（C 语言环境，X86_32 指令集）包含如下关键代码：某用户的口令保存在字符数组 origPassword 中，用户输入的口令保存在字符数组 userPassword 中，如果两个数组中的内容相同则允许进入系统。

```
[...]
char origPassword[12] = "Secret";
char userPassword[12];
[...]
gets(userPassword);    /* 读取用户输入的口令*/
[...]

if(strncmp(origPassword, userPassword, 12) != 0)
{
printf("Password doesn't match!\n");
exit(-1);
}
[...]
/* 口令认证通过时允许用户访问*/
[...]
```


【问题 1】（4 分）

用户在调用 gets()函数时输入什么样式的字符串，可以在不知道原始口令“Secret”的情况下绕过该口令验证函数的限制？

【问题 2】（4 分）

上述代码存在什么类型的安全隐患？请给出消除该安全隐患的思路。

信管网参考答案：

【问题一】

只要输入长度为 24 的字符串，其前 12 个字符和后 12 个字符一样即可。

【问题二】

gets（）函数必须保证输入长度不会超过缓冲区，一旦输入大于 12 个字符的口令就会造成缓冲区溢出。

解决思路：使用安全函数来代替 gets（）函数，或者对用户输入进行检查和校对，可通过 if 条件语句判断用户输入是否越界。 使用 fgets。

最终答案以信管网为准：http://www.cnitpm.com/zt/2016xaqcf/