

2019 年上半年信息安全工程师 《案例分析》真题答案及解析

本资料由信管网(www.cnitpm.com)整理发布，供信管网学员使用！

信管网是专业软考中高级与 PMP 考试培训服务网站。提供了考试资讯、考试报名、成绩查询、资料下载、在线答题、考试培训、项目管理人才交流、企业内训等服务。

信管网资料库提供了备考软考的精品学习资料；信管网案例分析频道和论文频道拥有丰富的案例范例和论文范例，信管网考试中心拥有软考中高级历年真题和超过 5000 多道试题免费在线测试；信管网每年指导考生超 100000+人。

信管网——专业、专注、专心，成就你的项目管理师梦想！

信管网：www.cnitpm.com

信管网考试中心：www.cnitpm.com/exam/

信管网培训中心：www.cnitpm.com/wx/

注：本资料由信管网整理后提供给学员使用，未经许可，严禁商业使用。

信管网微信公众号



信管网客服微信号





试题一、

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】

访问控制是保障信息系统安全的主要策略之一，其主要任务是保证系统资源不被非法使用和非常规访问。访问控制规定了主体对客体访问的限制，并在身份认证的基础上，对用户提出的资源访问请求加以控制。当前，主要的访问控制模型包括：自主访问控制 (DAC) 模型和强制访问控制 (MAC) 模型。

【问题 1】(6 分)

针对信息系统的访问控制包含哪三个基本要素？

【问题 2】(4 分)

BLP 模型是一种强制访问控制模型，请问：

- (1) BLP 模型保证了信息的机密性还是完整性？
- (2) BLP 模型采用的访问控制策略是上读下写还是下读上写？

【问题 3】(4 分)

Linux 系统中可以通过 `ls•` 命令查看文件的权限，例如：文件 `net.txt` 的权限属性如下所示：

```
-rwx-----1 root root 5025 May 25 2019 /home/abc/net.txt
```

请问：

- (1) 文件 `net.txt` 属于系统的哪个用户？
- (2) 文件 `net.txt` 权限的数字表示是什么？

信管网参考答案：

【问题 1】

主体、客体、授权访问

【问题 2】

- (1) 机密性
- (2) 下读上写

【问题 3】

- (1) root
- (2) 700

查看解析：www.cnitpm.com/st/411607694.html



联系我们



往期真题下载 ↓ ↓



更多精品资料 ↓ ↓



在线考试题库 ↓ ↓



信管网
www.cnitpm.com

**试题二、**

阅读下列说明和表，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。密码学中，根据加密和解密过程所采用密钥的特点可以将密码算法分为两类：对称密码算法和非对称密码算法。此外，密码技术还用于信息鉴别、数据完整性检验、数字签名等。

【问题 1】(6 分)

信息安全的基本目标包括真实性、保密性、完整性、不可否认性、可控性、可用性、可审查性等。密码学的三大安全目标 C. I. A 分别表示什么？

【问题 2】(5 分)

仿射密码是一种典型的对称密码算法。仿射密码体制的定义如下：

令明文和密文空间 $M = C = Z_{26}$ ，密钥空间 $K = \{(k_1, k_2) \in Z_{26} \times Z_{26} : \gcd(k_1, 26) = 1\}$ 。
对任意的密钥 $key = (k_1, k_2) \in K$ ， $x \in M$ ， $y \in C$ ，定义加密和解密的过程如下：
加密： $e_{key}(x) = (k_1x + k_2) \bmod 26$
解密： $d_{key}(y) = k_1^{-1}(y - k_2) \bmod 26$
其中 k_1^{-1} 表示 k_1 在 Z_{26} 中的乘法逆元，即 k_1^{-1} 乘以 k_1 对 26 取模等于 1， $\gcd(k_1, 26) = 1$ 表示 k_1 与 26 互素。
设已知仿射密码的密钥 $key = (11, 3)$ ，英文字符和整数之间的对应关系如表 2.1 所示，则：

表 2.1

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- (1) 整数 11 在 Z_{26} 中的乘法逆元是多少？
- (2) 假设明文消息为“SEC”，相应的密文消息是什么？

【问题 3】(2 分)

根据表 2.1 的对应关系，仿射密码中，如果已知明文“E”对应密文“C”，明文“T”对应密文“F”，则相应的 $key = (k_1, k_2)$ 等于多少？

信管网参考答案：

【问题 1】



联系我们



保密性、完整性、可用性。

【问题 2】

(1) 19

(2) TVZ

【问题 3】

21; 22

查看解析: www.cnitpm.com/st/4116124940.html

往期真题下载 ↓ ↓



更多精品资料 ↓ ↓



在线考试题库 ↓ ↓



**试题三、**

阅读下列说明，回答问题 1 至问题 5，将解答填入答题纸的对应栏内。

【说明】

假设用户 A 和用户 B 为了互相验证对方的身份，设计了如下通信协议：

1. $A \rightarrow B: R_A$

2. $B \rightarrow A: f(P_{AB} || R_A) || R_B$

3. $A \rightarrow B: f(P_{AB} || \underline{\hspace{2cm}})$

其中： R_A 、 R_B 是随机数， P_{AB} 是双方事先约定并共享的口令，“||”表示连接操作。 f 是哈希函数。

【问题 1】 (2 分)

身份认证可以通过用户知道什么、用户拥有什么和用户的生理特征等方法来验证。请问上述通信协议是采用哪种方法实现的？

【问题 2】 (2 分)

根据身份的互相验证需求，补充协议第 3 步的空白内容。

【问题 3】 (2 分)

通常哈希函数 f 需要满足下列性质：单向性、抗弱碰撞性、抗强碰撞性。如果某哈希函数 f 具备：找到任何满足 $f(x)=f(y)$ 的偶对 (x, y) 在计算上是不可行的，请说明其满足哪条性质。

【问题 4】 (2 分)

上述协议不能防止重放攻击，以下哪种改进方式能使其防止重放攻击？

(1) 在发送消息加上时间参量。

(2) 在发送消息加上随机数。

【问题 5】 (4 分)

如果将哈希函数替换成对称加密函数，是否可以提高该协议的安全性？为什么？

信管网参考答案：

【问题 1】

基于用户知道什么实现身份验证。

【问题 2】

R_B 或者 $R_B || R_A$

【问题 3】

抗强碰撞性



联系我们



【问题 4】

(1)或者“加入时间参量”

【问题 5】

不能。尽管加密函数也可以实现认证功能，但是从单向性要求上，加密函数显然没有哈希函数的安全性高。

查看解析：www.cnitpm.com/st/411623791.html

往期真题下载↓↓



更多精品资料↓↓



在线考试题库↓↓



**试题四、**

阅读下列说明和表，回答问题 1 至问题 4，将解答填入答题纸的对应栏内。

【说明】

防火墙类似于我国古代的护城河，可以阻挡敌人的进攻。在网络安全中，防火墙主要用于逻辑隔离外部网络与受保护的内部网络。防火墙通过使用各种安全规则来实现网络的安全策略。

防火墙的安全规则由匹配条件和处理方式两个部分共同构成。网络流量通过防火墙时，根据数据包中的某些特定字段进行计算以后如果满足匹配条件，就必须采用规则中的处理方式进行处理。

【问题 1】(5 分)

假设某企业内部网(202.114.63.0/24)需要通过防火墙与外部网络互连，其防火墙的过滤规则实例如表 4.1 所示。

表 4.1

序号	源地址	源端口	目的地址	目的端口	协议	ACK	动作 (处理方式)
A	202.114.63.0/24	>1024	*	80	TCP	*	accept
B	*	80	202.114.63.0/24	>1024	TCP	Yes	accept
C	*	>1024	202.114.64.125	80	TCP	*	accept
D	202.114.64.125	80	*	>1024	TCP	Yes	accept
E	202.114.63.0/24	>1024	*	(1)	UDP	*	accept
F	*	53	202.114.63.0/24	>1024	UDP	*	accept
G	*	*	*	*	*	*	(2)

注：表中“*”表示通配符，任意服务端口都有两条规则。

请补充表 4.1 中的内容 (1) 和 (2)，并根据上述规则表给出该企业对应的安全需求。

【问题 2】(4 分)

一般来说，安全规则无法覆盖所有的网络流量。因此防火墙都有一条缺省(默认)规则，该规则能覆盖事先无法预料的网络流量。请问缺省规则的两种选择是什么？

【问题 3】(6 分)

请给出防火墙规则中的三种数据包处理方式。

【问题 4】(4 分)

防火墙的目的是实施访问控制和加强站点安全策略，其访问控制包含四个方面的内容：服务控制、方向控制、用户控制和行为控制。请问表 4.1 中，规则 A 涉及访问控制的哪几个方面的内容？

信管网参考答案：

**【问题 1】**

1、53

2、丢弃或者 Drop 企业对应的安全需求有：

- (1) 允许内部用户访问外部网络的网页服务器；
- (2) 允许外部用户访问内部网络的网页服务器；
- (3) 除 1 和 2 外，禁止其他任何网络流量通过该服务器。

【问题 2】

默认拒绝:默认拒绝指的是一切没有被允许的就是禁止的。默认允许:默认允许指的是一切没有被禁止的就是允许的。

【问题 3】

接受(Accept) :允许数据包或者信息通过。

拒绝 (Reject) :拒绝数据包或者信息通过，并且通知信息源该信息被禁止。

丢弃(Drop):直接将数据包或者信息丢弃，并且不通知信息源。

【问题 4】

服务控制和方向控制。

查看解析: www.cnitpm.com/st/4116311229.html

往期真题下载 ↓ ↓



更多精品资料 ↓ ↓



在线考试题库 ↓ ↓



**试题五、**

阅读下列说明和图，回答问题 1 至问题 4，将解答填入答题纸的对应栏内。

【说明】

信息系统安全开发生命周期(Security Development Life Cycle(SDLC))是微软提出的从安全角度指导软件开发过程的管理模式，它将安全纳入信息系统开发生命周期的所有阶段，各阶段的安全措施与步骤如下图 5.1 所示。

**【问题 1】** (4 分)

在培训阶段，需要对员工进行安全意识培训，要求员工向弱口令说不！针对弱口令最有效的攻击方式是什么？以下口令中，密码强度最高的是()。

- A. security2019
- B. 2019Security
- C. Security@2019
- D. Security2019

【问题 2】 (6 分)

在大数据时代，个人数据正被动地被企业搜集并利用。在需求分析阶段，需要考虑采用隐私保护技术防止隐私泄露。从数据挖掘的角度，隐私保护技术主要有：基于数据失真的隐私保护技术、基于数据加密的隐私保护技术、基于数据匿名隐私保护技术。

请问以下隐私保护技术分别属于上述三种隐私保护技术的哪一种？

- (1) 随机化过程修改敏感数据
- (2) 基于泛化的隐私保护技术
- (3) 安全多方计算隐私保护技术

【问题 3】 (4 分)

有下述口令验证代码：



```

#define PASSWORD "1234567"
int verify_password(char *password)
{
    int authenticated;
    char buffer[8];
    authenticated=strcmp(password,PASSWORD);
    strcpy(buffer,password);
    return authenticated;
}

int main(int argc, char* argv[])
{
    int valid_flag=0;
    char password[1024];
    while(1)
    {
        printf("please input password: ");
        scanf("%s",password);
        valid_flag = verify_password(password); //验证口令
        if(valid_flag) //口令无效
        {
            printf("incorrect password!\n\n");
        }
        else //口令有效
        {
            printf("Congratulation! You have passed the verification!\n");
            break;
        }
    }
}

```

其中 main 函数在调用 verify_password 函数进行口令验证时,堆栈的布局如图 5.2 所示。



图 5.2

请问调用 verify_password 函数的参数满足什么条件,就可以在不知道真实口令的情况下绕过口令验证功能?

【问题 4】(3 分)

SDLC 安全开发模型的实现阶段给出了 3 种可以采取的安全措施,请结合问题 3 的代码举例说明?

信管网参考答案:

【问题 1】

口令爆破或穷举攻击。

C

【问题 2】



- (1) 基于数据失真的隐私保护技术
- (2) 基于数据匿名的隐私保护技术
- (3) 基于数据加密的隐私保护技术

【问题 3】

完整 8 个字符即可。

【问题 4】

- (1) 使用批准工具(安全编译工具)。
- (2) 禁用危险函数(例如代码中的 `strcpy`, `scanf`)。
- (3) 静态分析工具。

查看解析: www.cnitpm.com/st/411642133.html

<p>往期真题下载 ↓ ↓</p> 	<p>更多精品资料 ↓ ↓</p> 	<p>在线考试题库 ↓ ↓</p> 
--	--	--