腾讯课堂

1. 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】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】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】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？

送出小花

我也要缓考

送出小花

腾讯课堂

【问题4】

在图1-1给出的加密过程中，Mi，i=1，2，…，n表示明文分组，Ci，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？

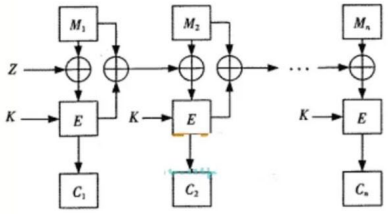


图1-1

送出小花

我也要缓考

送出小花

腾讯课堂

2. 阅读下列说明，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向的限制，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】

简述访问控制的原理？针对信息系统的访问控制包含哪三个基本要素？

【问题2】

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？

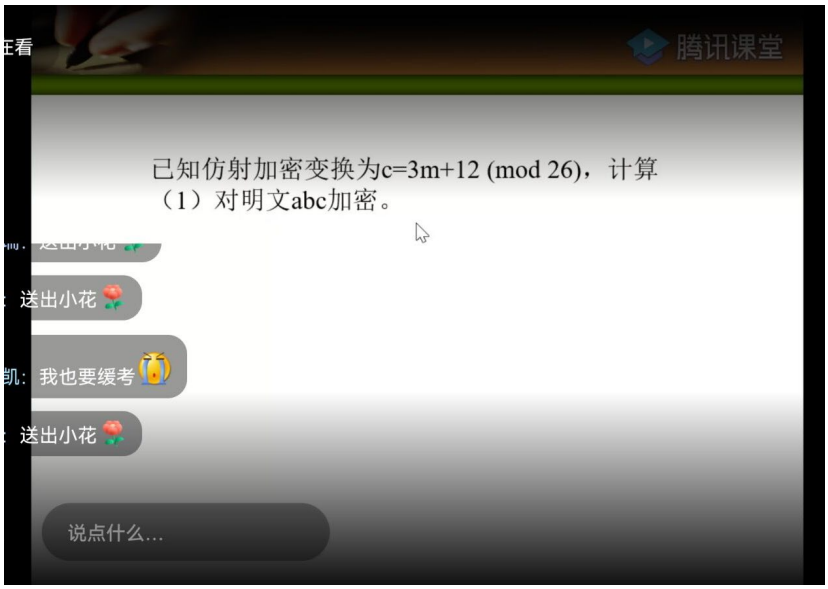
（2）BLP模型采用的访问控制策略是上读下写还是下读上写？

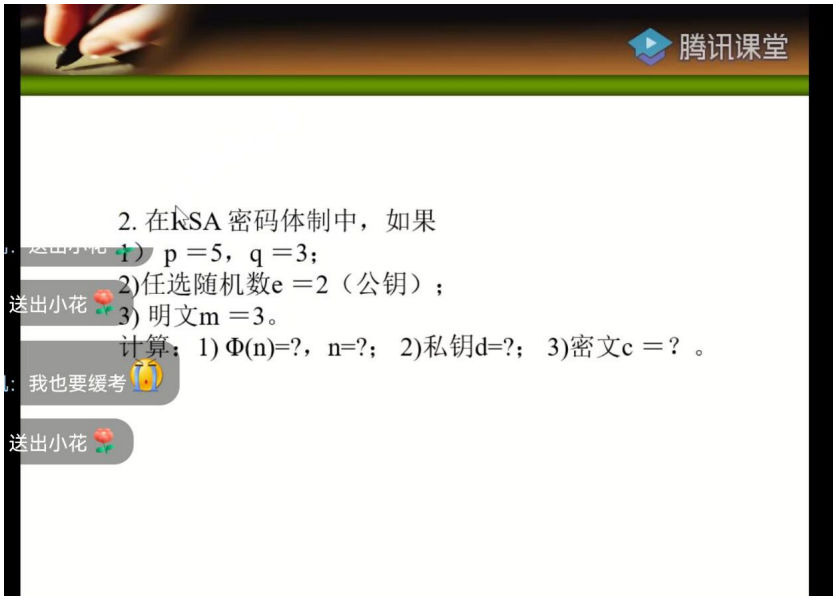
送出小花

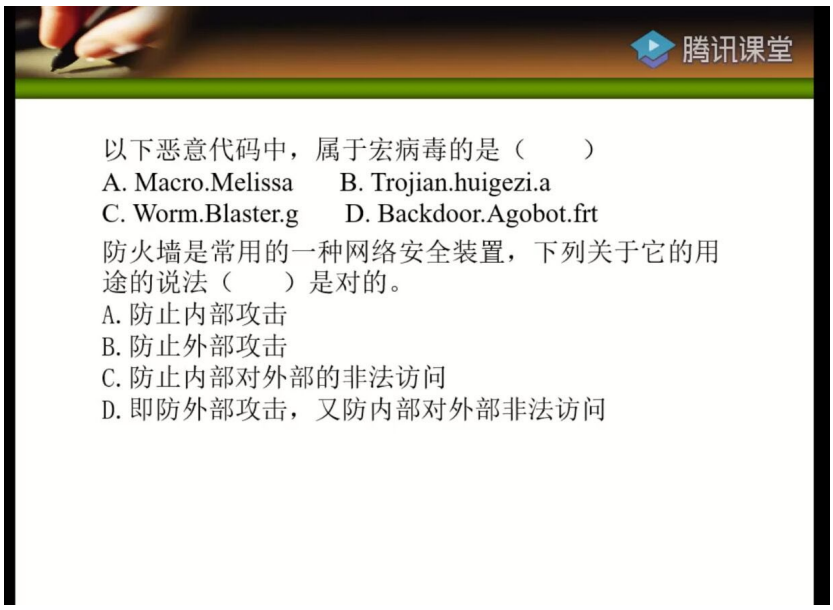
我也要缓考

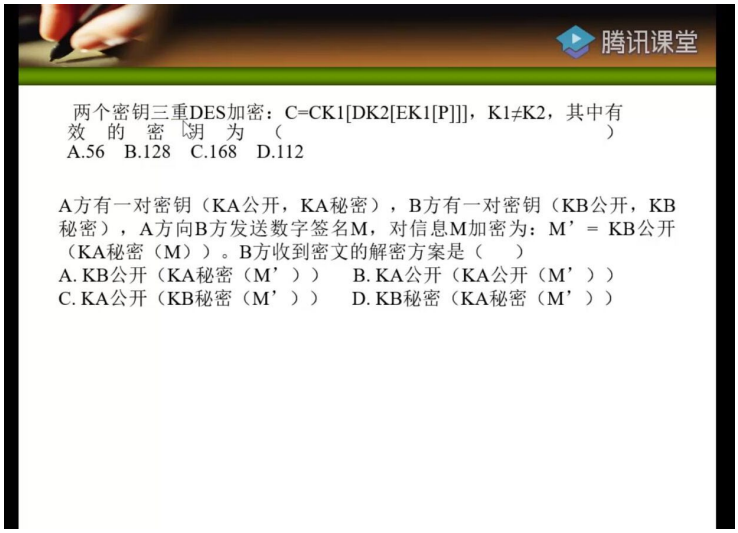
送出小花

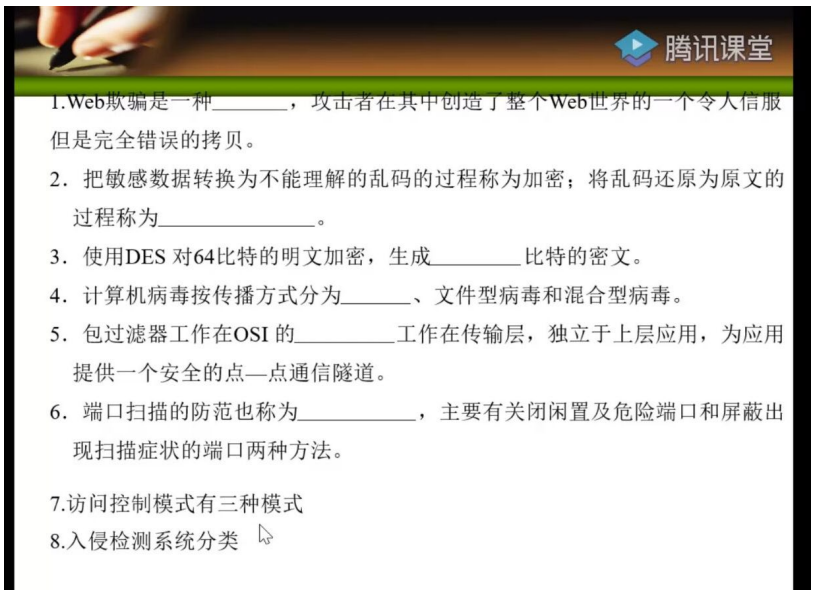
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	(1)	1	2	8	5	11	12	4	15
1	13	8	11	5	(2)	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	(3)	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	(4)	12	7	2	14






腾讯课堂
以下恶意代码中，属于宏病毒的是（　　）
A. Macro.Melissa　　B. Trojian.huigezi.a
C. Worm.Blaster.g　　D. Backdoor.Agobot.frt
防火墙是常用的一种网络安全装置，下列关于它的用途的说法（　　）是对的。
A. 防止内部攻击
B. 防止外部攻击
C. 防止内部对外部的非法访问
D. 即防外部攻击，又防内部对外部非法访问


腾讯课堂
两个密钥三重DES加密：C=CK1[DK2[EK1[P]]]，K1≠K2，其中有效的密钥为（　　）
A.56　B.128　C.168　D.112
A方有一对密钥（KA公开，KA秘密），B方有一对密钥（KB公开，KB秘密），A方向B方发送数字签名M，对信息M加密为：M’ = KB公开（KA秘密（M））。B方收到密文的解密方案是（　　）
A. KB公开（KA秘密（M’））　B. KA公开（KA公开（M’））
C. KA公开（KB秘密（M’））　D. KB秘密（KA秘密（M’））


腾讯课堂
1.Web欺骗是一种_____，攻击者在其中创造了整个Web世界的一个令人信服但是完全错误的拷贝。
2．把敏感数据转换为不能理解的乱码的过程称为加密；将乱码还原为原文的过程称为_____。
3．使用DES 对64比特的明文加密，生成_____比特的密文。
4．计算机病毒按传播方式分为_____、文件型病毒和混合型病毒。
5．包过滤器工作在OSI 的_____工作在传输层，独立于上层应用，为应用提供一个安全的点—点通信隧道。
6．端口扫描的防范也称为_____，主要有关闭闲置及危险端口和屏蔽出现扫描症状的端口两种方法。
7.访问控制模式有三种模式
8.入侵检测系统分类

DES 是一种分组密码，已知 DES 加密算法的某个 S 盒如表 4-1 所示。

表 4-1 S 盒

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

【问题1】（4分）

请补全该 S 盒，填补其中的空(1) - (4），将解答写在答题纸的对应栏内。

【问题 2】（2分）

如果该 S 盒的输入为 110011，请计算其二进制输出。

【问题3】（6分）

DES加密的初始置换表如下：

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

置换时，从左上角的第一个元素开始，表示输入的第58位明文的第58位置换成输出的第1位，输入明文的第50位置换成输出的第2位，从左至右，从上往下，依次类推。

DES加密时，对输入的64位明文首先进行初始置换操作。

若置换输入的明文M=0123456789ABCDEF（16进制），请计算其输出（16进制表示）。

【问题4】（2分）

如果有简化的DES版本，其明文输入为8比特，初始置换表IP如下：

IP：2 6 3 1 4 8 5 7

请给出其逆初始置换表。

【问题5】（2分）

DES加密算法存在一些弱点和不足，主要有密钥和存在弱密钥。请问，弱密钥的定义是什么？

2017年上半年信息安全工程师下午案例分析试题四信管网参考答案

【问题 1】

(1) 10　(2) 6　(3) 1　(4) 11

【问题 2】

0100

【问题 3】

M = (0123456789ABCDEF)16 = (00000001 00100011 01000101 01100111 10001001 10101011 11001101 11101111)2

经过 IP 置换，结果为：

M' = (11001100 00000000 11001100 11111111 11110000 10101010 11110000 10101010) 2

= (CC00CCFFF0AAF0AA) 16

【问题 4】

4 1 3 5 7 2 8 6

【问题 5】

弱密钥不受任何循环移位的影响，并且只能得到相同的子密钥，由全 0 或全 1 组成的密钥显然是弱密钥。生成过程中被分割的两部分分别为全 0 或全 1 时也是弱密钥。