第一章：

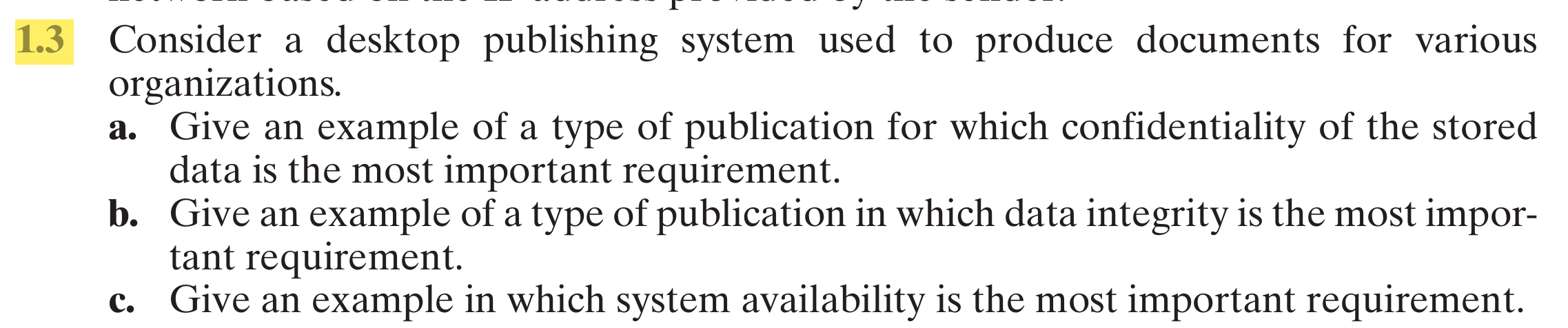


（该题没有找到答案，仿照的是有答案的那一版写的）

机密性：如果有敏感数据，要求较高，否则比较低

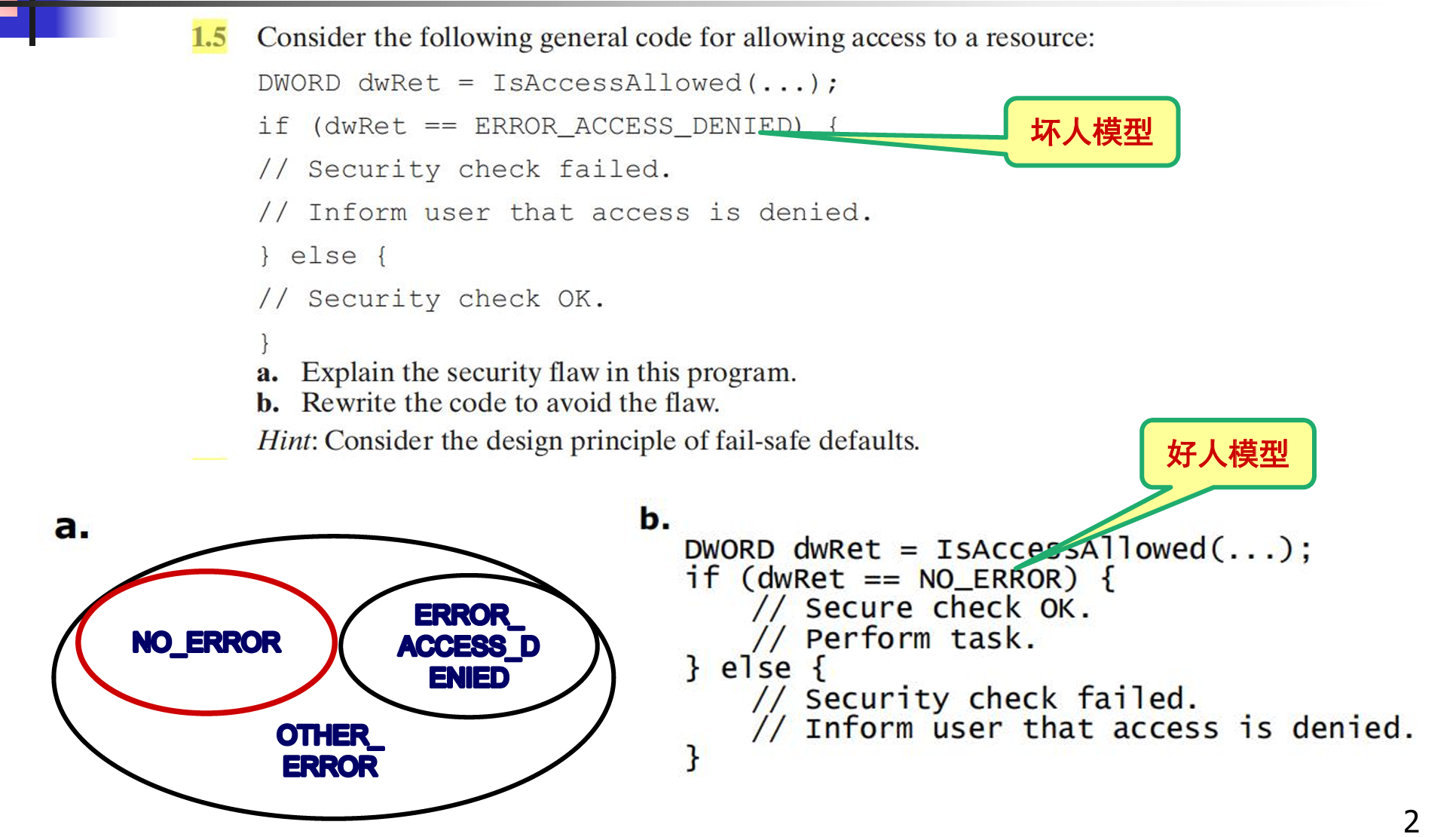
完整性：对于主机之间，要求中等，错误包只需要重发即可，对于整个系统，要求较高，如系统的初始化配置等。

可用性：最高，路由系统如果不能转发数据包就没有存在的意义。

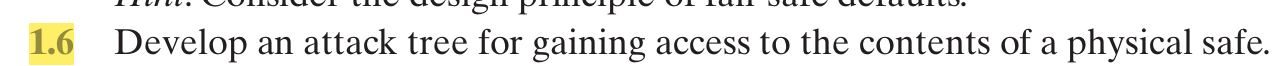
a. 公司的机密资料

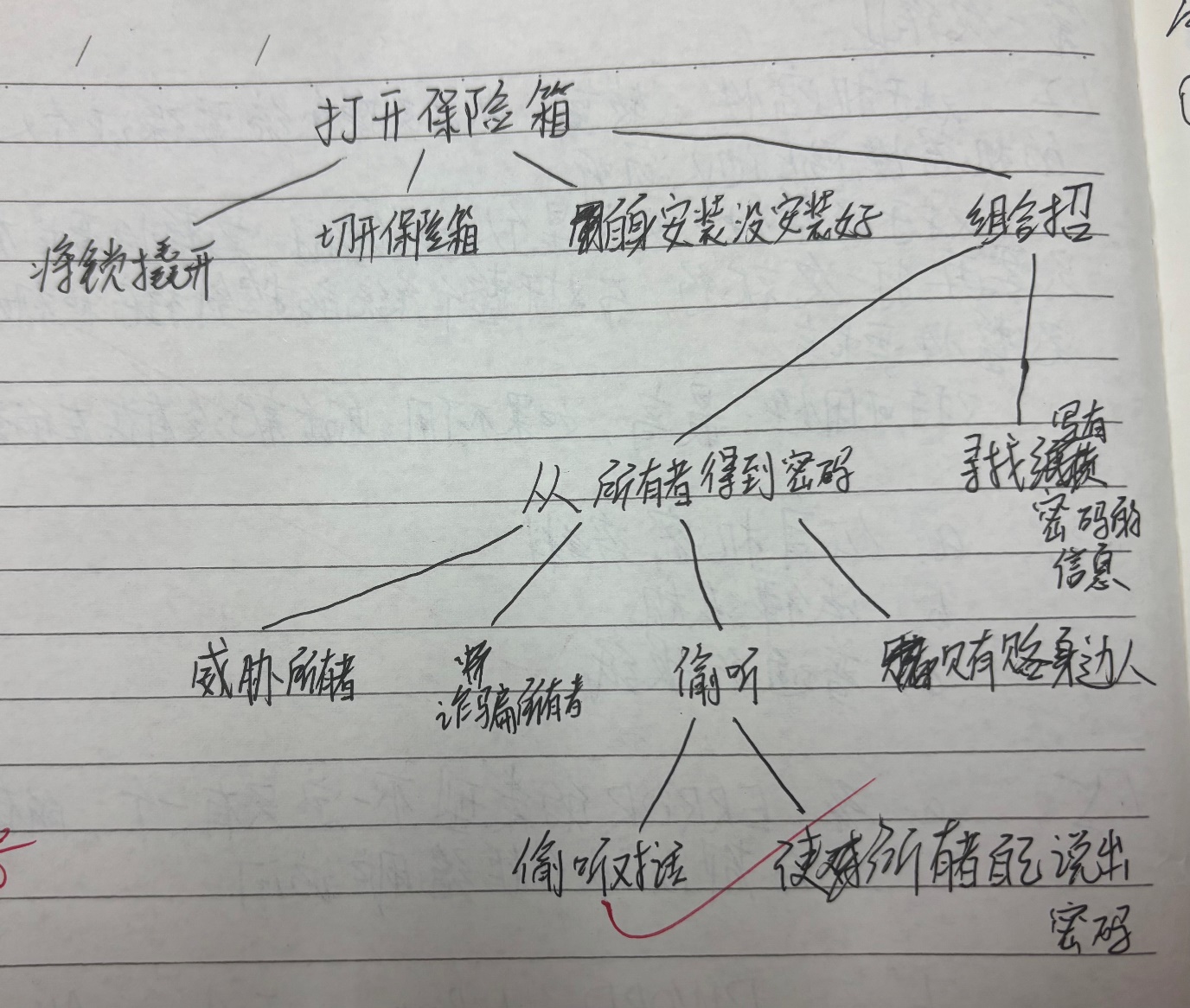
b. 法律法规

c. 普通的日报

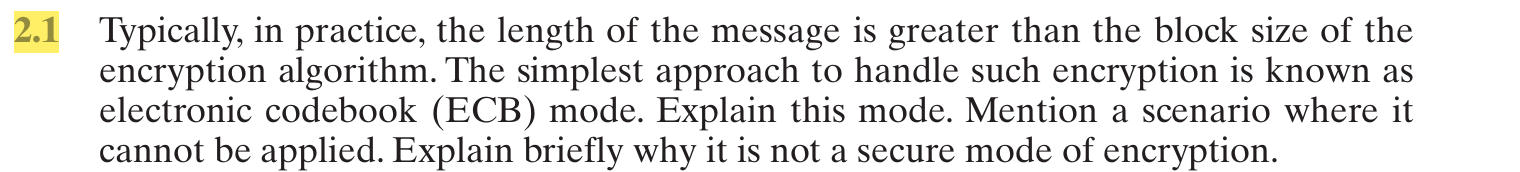


1.5：利用安全缺省原则，当且仅当没有错误时给通过（好人模型）



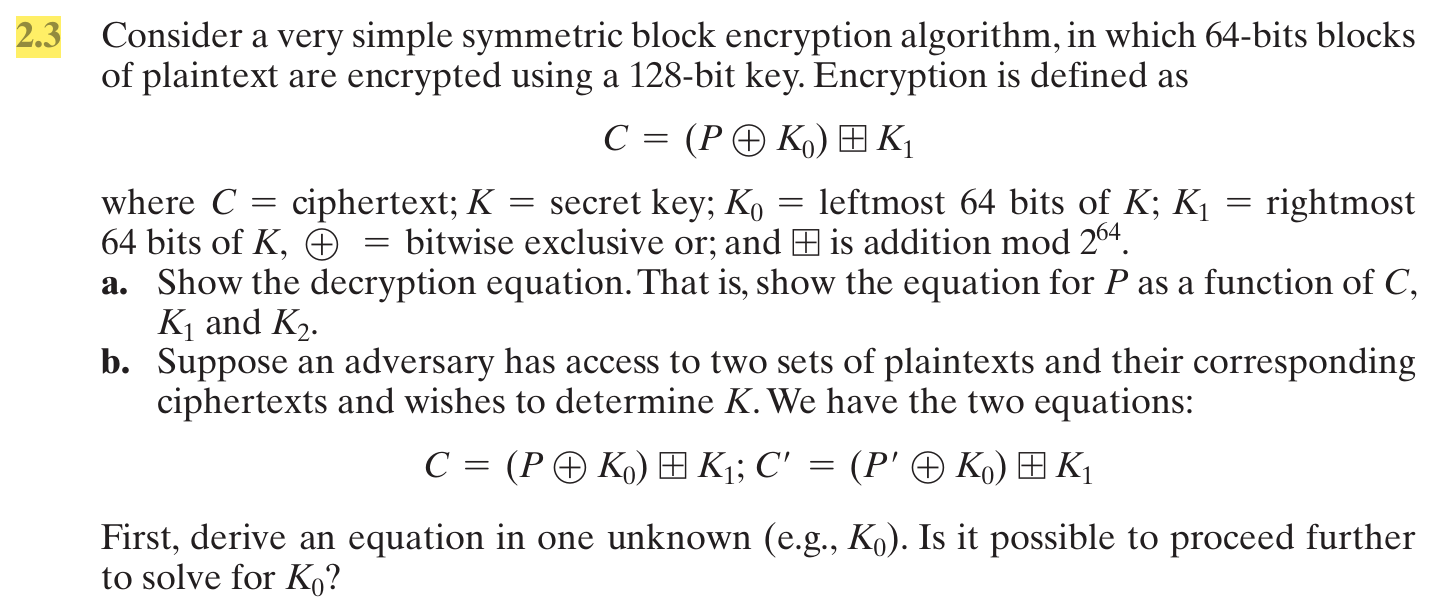


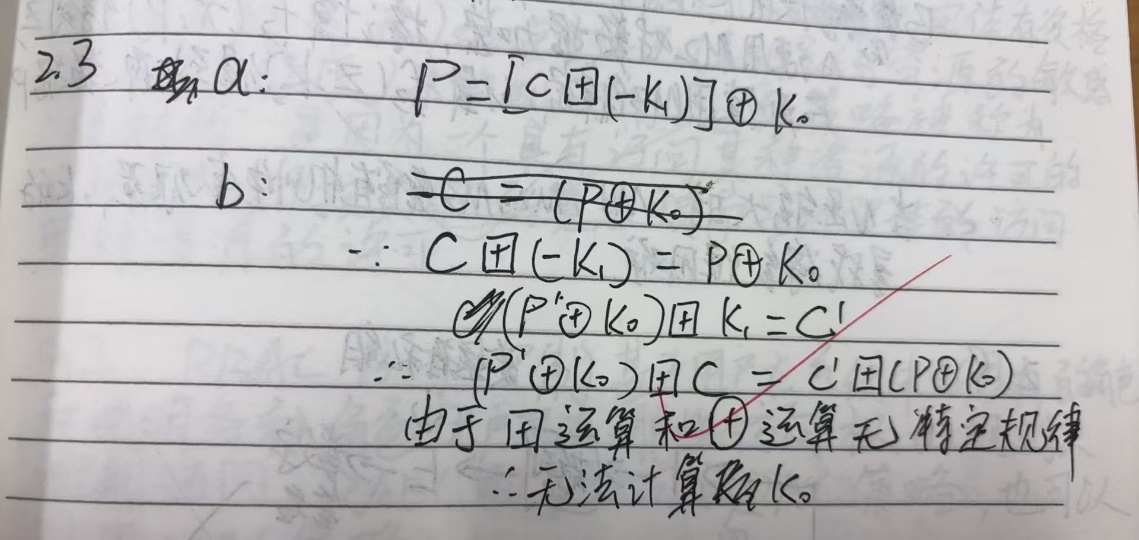
第二章：



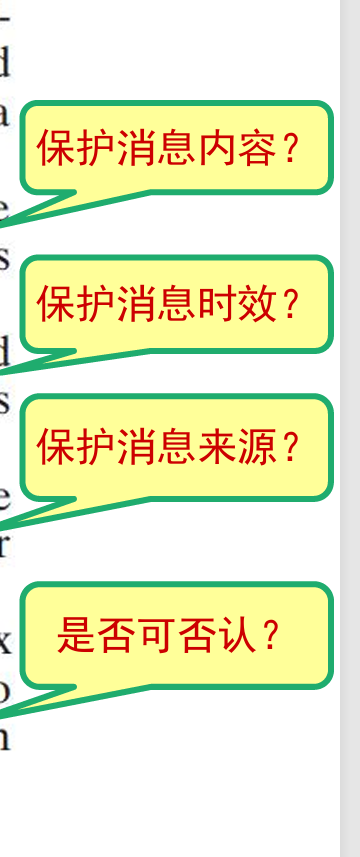
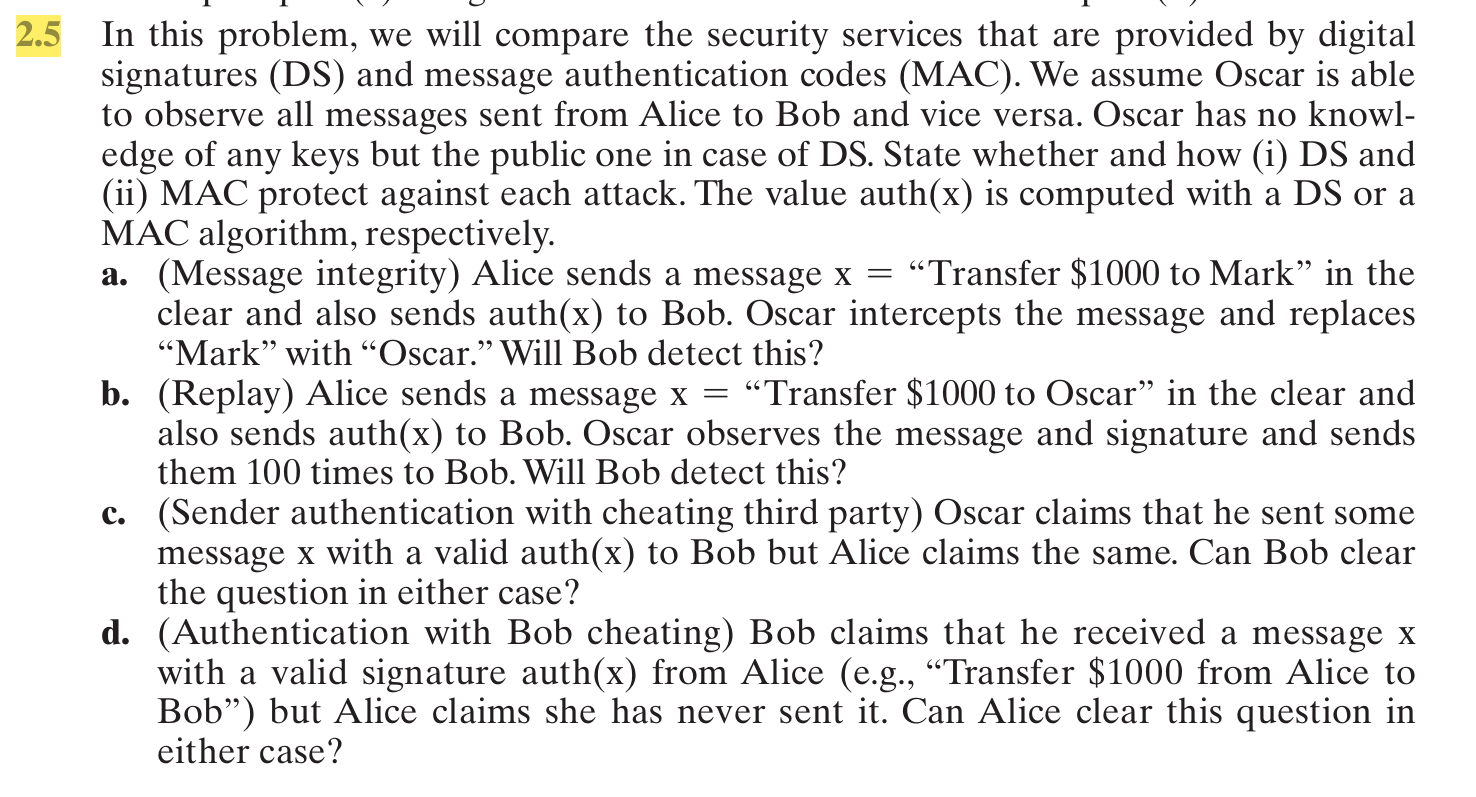
Ecb模式下，明文每次被提交b位（通常，b=64或128）并且每组明文用相同的密匙进行加密。 长度为nb的明文被分成n个b位的分组，每个分组用相同的算法和相同的密匙加密，产生出由n个b位分组组成的密文序列。

对于很长的消息，ecb模式可能不安全。密码分析者可能利用明文中的一些规律进行破解。例如，若这段消息总是以某些固定的字符开头，密码分析者就可以拥有大量的明文-密文对，进而展开攻击。





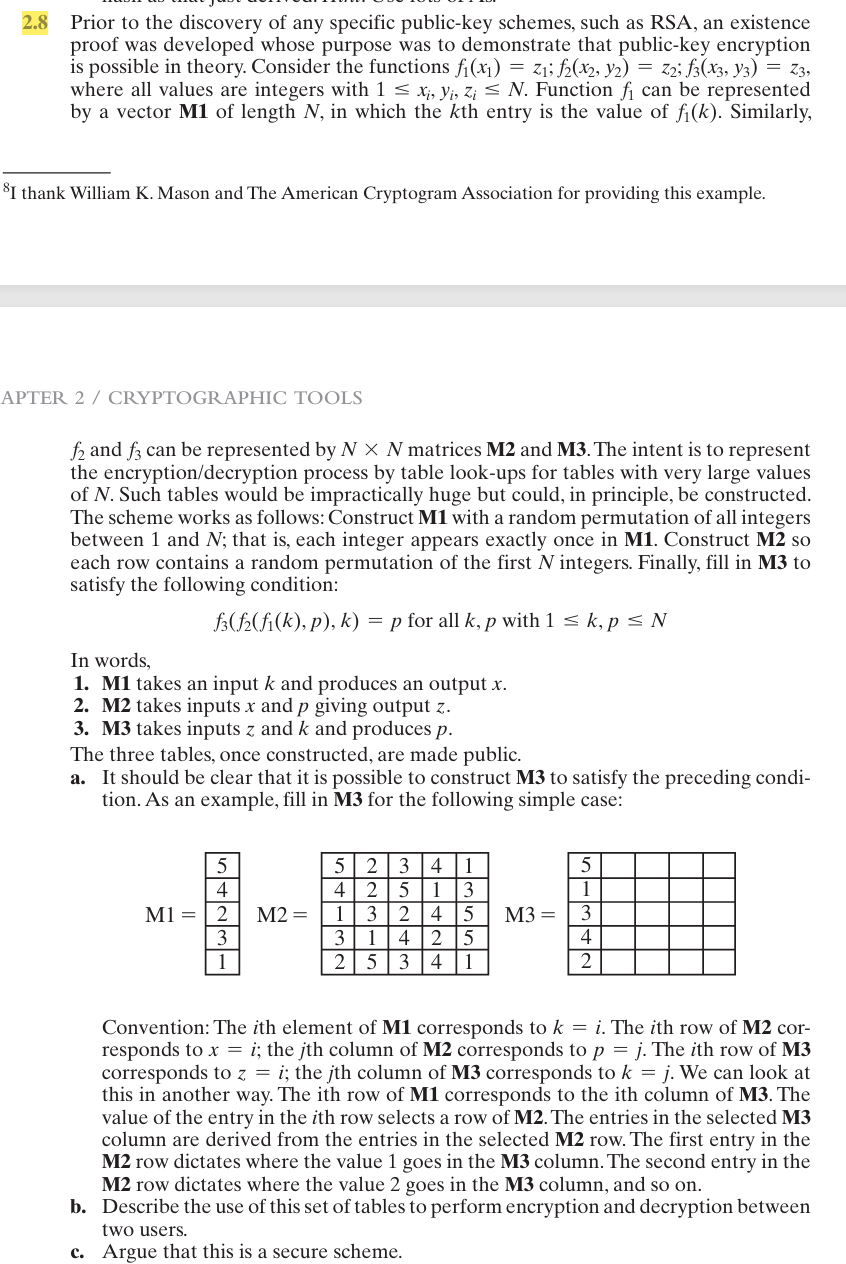
实际上就是等式两边变量的左移右移，唯一要注意的是加法取模运算移到另一边后还是加法取模，但是原数值要取反。



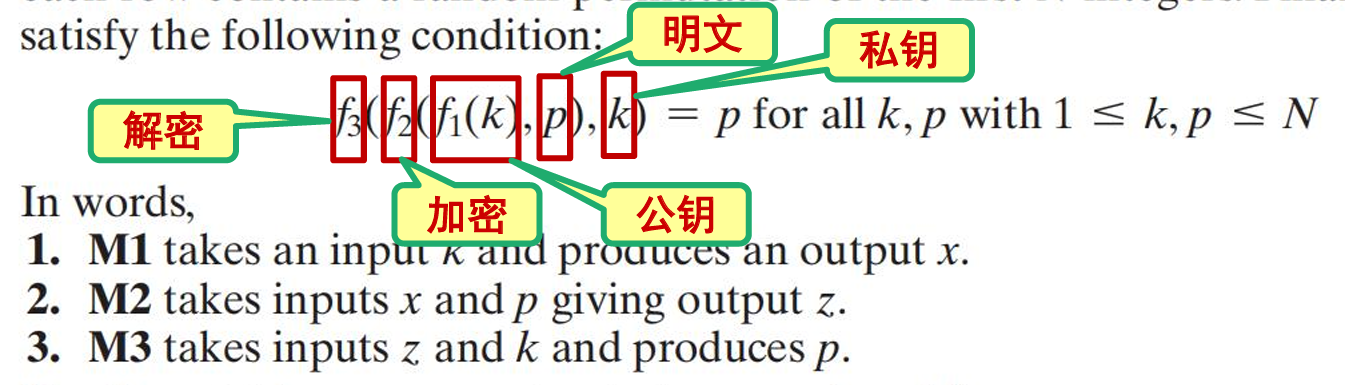
mac（消息认证码，基于对称加密）和DS（数字签名，基于非对称加密）均可保障消息的内容完整性（即可以检测出消息是否被篡改）也可以进行来源验证（谁发的消息），但是，mac并不具有不可抵赖性（即发送消息的一方声称自己没有发送，就像

题d中的alice一样），因为收发双方都有密匙，而DS不会有不可抵赖性的问题，能明确一条消息由谁发出。最后，二者均不具有保护消息时效的能力，无法抵御重放攻击。

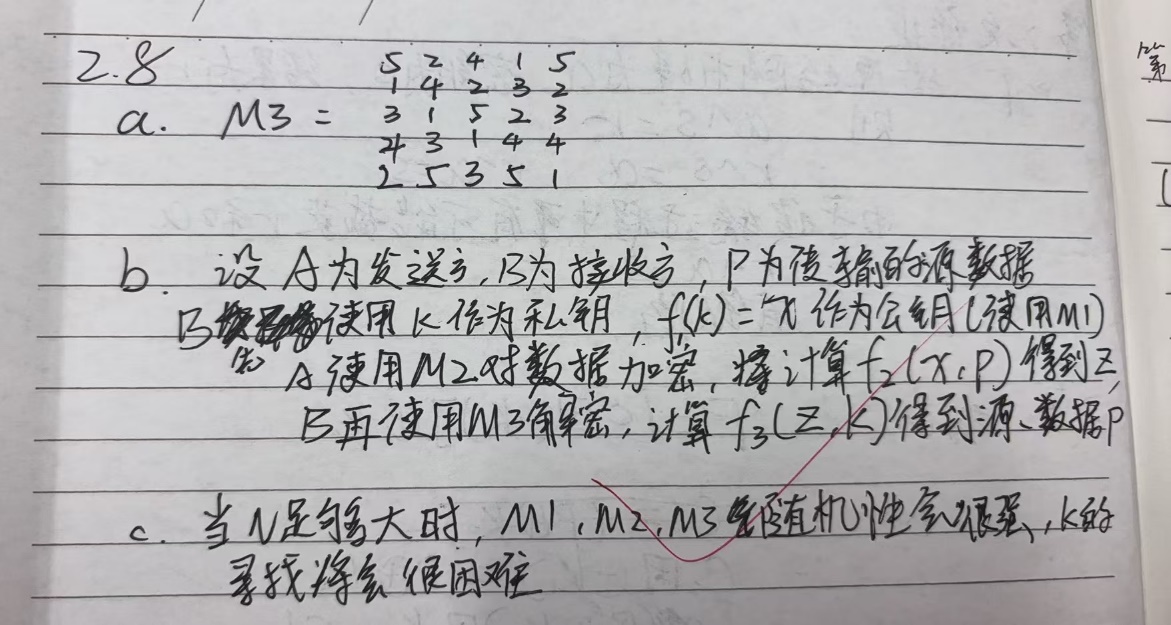
综上，对于题a和c，两种方式均可检测出来，而对于题b，二者均检测不出来，对于题d，只有DS能检测出来。



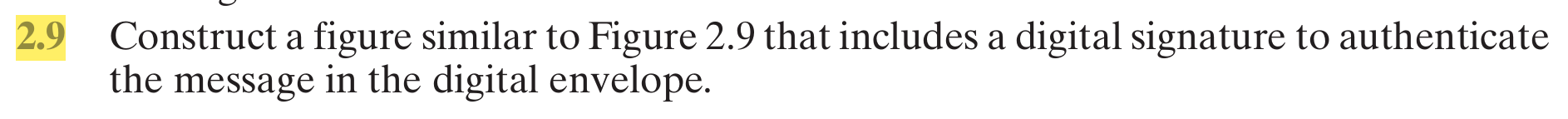
加解密公式解释：

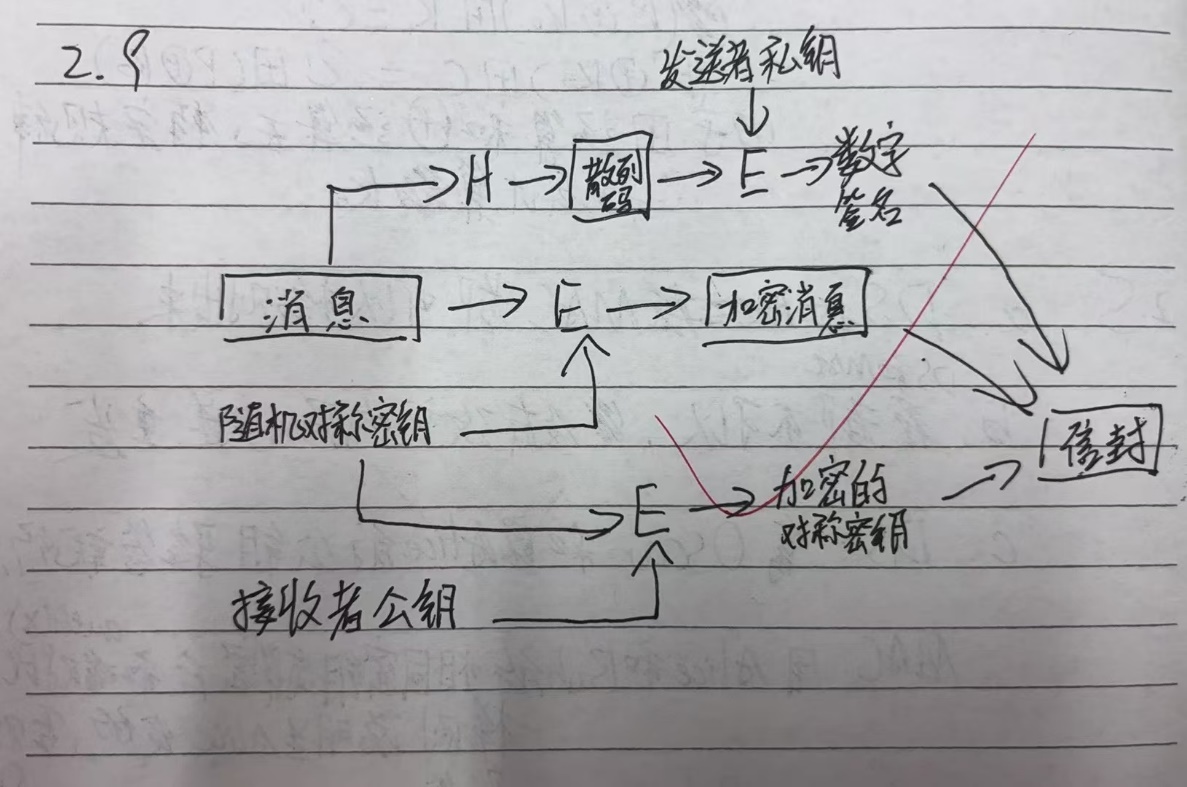


明文使用私钥算出来的公钥进行加密，得到密文**z**，也就是函数f2的值，接收者使用自己的私钥解出明文，这个公式解释了公钥系统的运作原理，题目中的矩阵算法相当于具体的加解密算法

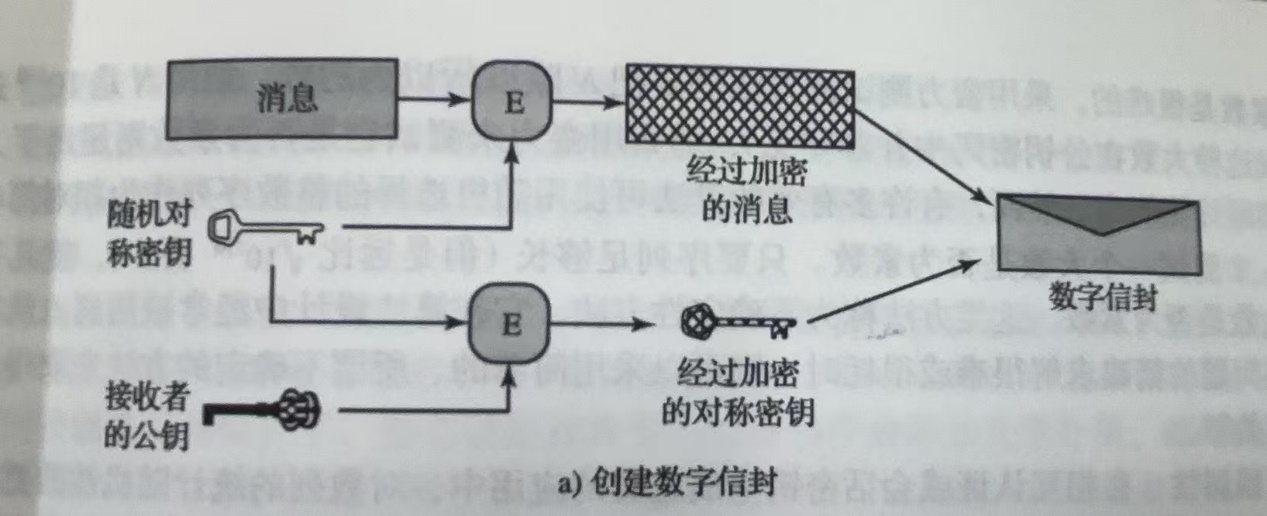


此题的关键是读懂题意，再照着做就很简单了。





数字信封本身包含两个部分，加密消息和加密的密钥，现在要加入数字签名，数字签名是将信息通过单向性的哈希函数生成固定长度的信息摘要，该摘要再使用发送者密钥进行签名，最终形成数字签名，因此，我们只要在原图上加上对消息的数字签名生成过程即可。原图如下：



第三章：

Questions：



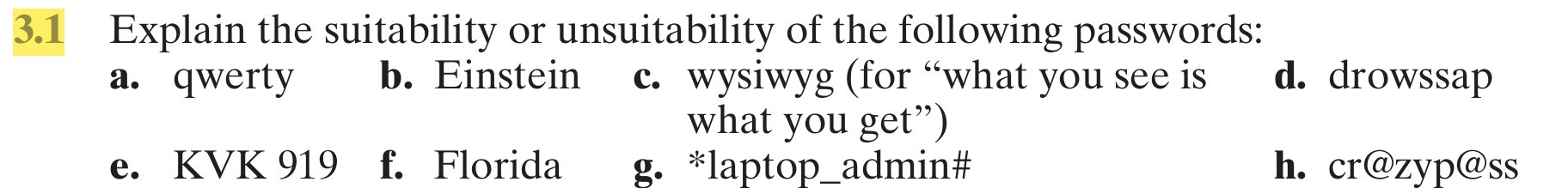
1. 个人所知道的信息（主要是口令验证）
2. 个人所持有的物品（主要是令牌）
3. 个人的生理特征（静态生物特征，如指纹，虹膜等）
4. 个人的行为特征（动态生物特征，如语音，笔迹）



（未找到直接答案，书上唯一和影子口令文件相关的部分在3.2.4的第一段话）：

一种阻止口令攻击的方法就是拒绝对手访问口令文件。如果文件的散列口令部分只能被特权用户访问，那么对手就不能够读取口令文件，除非他拥有特权用户的口令。通常，散列后的口令保存在与用户ID分离的单独文件中，这个文件叫作影子口令文件(shadow password file)对于影子口令文件，需要特别注意保护，防止非授权访问。

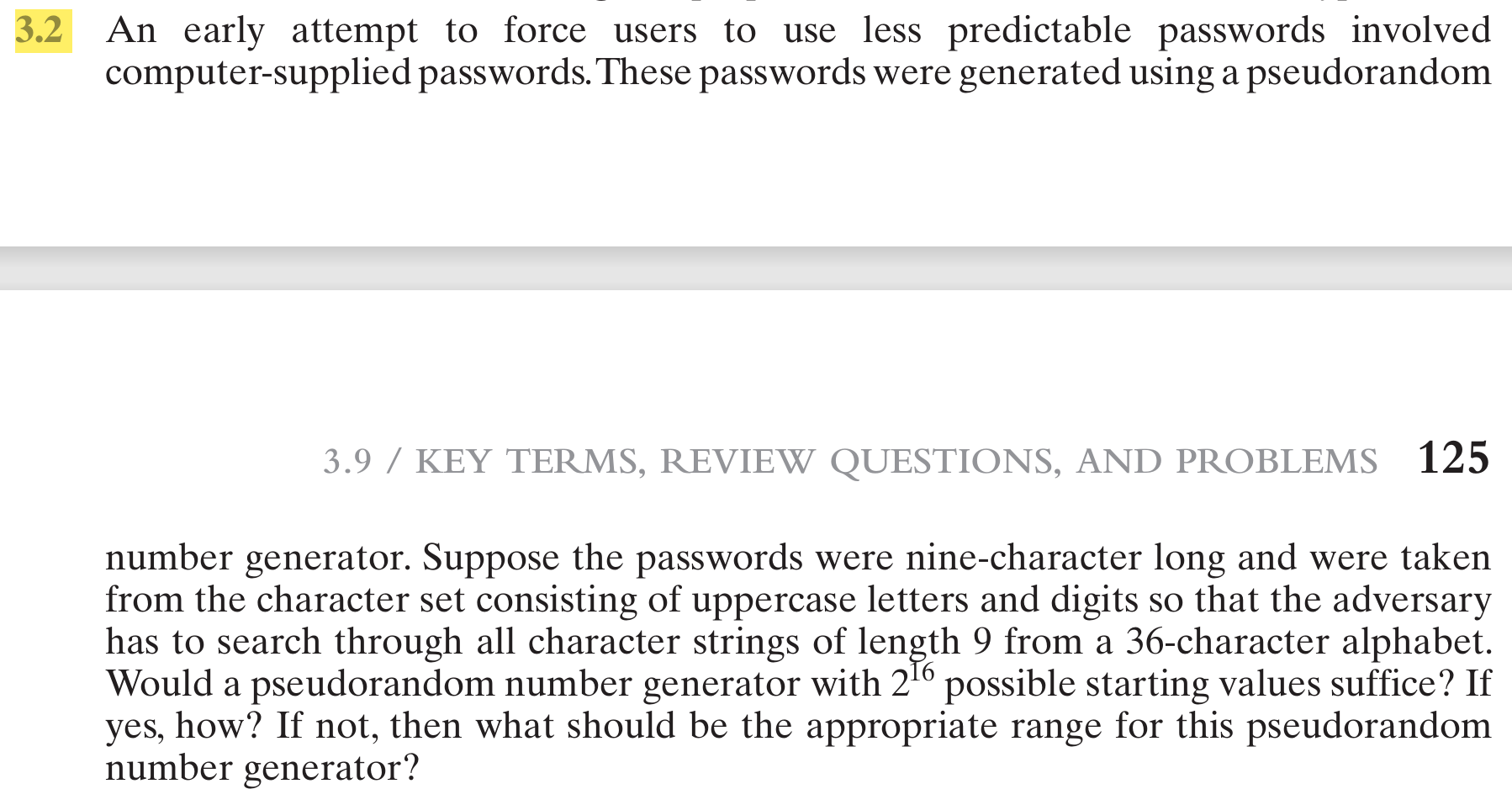
Problems：



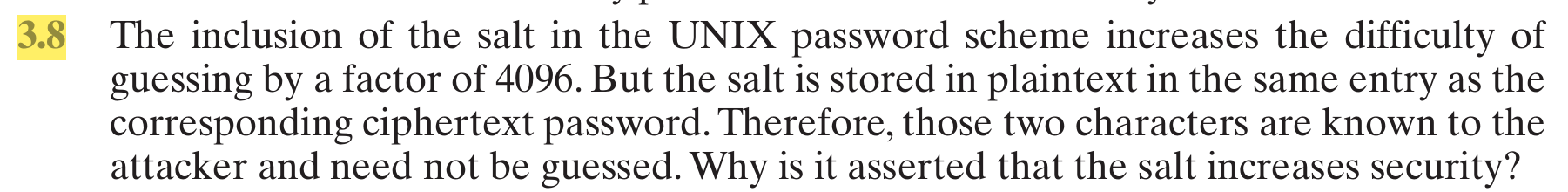
该题也没有直接答案，但是根据有答案的那一版来看，c和h是铁定合适的，d不一定，其他不合适。

这些密码的具体含义：





从题目中可以看出总的密码数为36的9次方，而产生的随机数只有2的16次方，因此只能对应2的16次方个密码，猜测的集合会比较小。

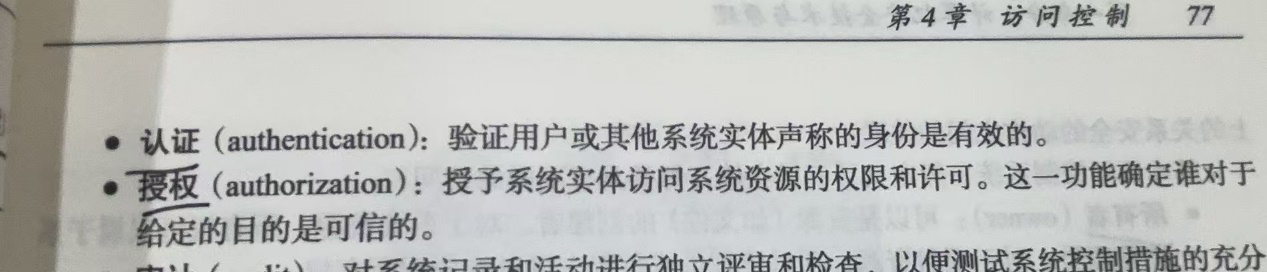


如果没有盐值，攻击者可以随机猜测一个口令并加密（只要加密一次），并用加密结果和所有用户匹配，如果有用户使用这个密码，总会有一个匹配到。而如果有盐值，攻击者要为每一个用户进行一次加密运算（每个用户的盐值不一样），更为麻烦。

第四章：

Questions：





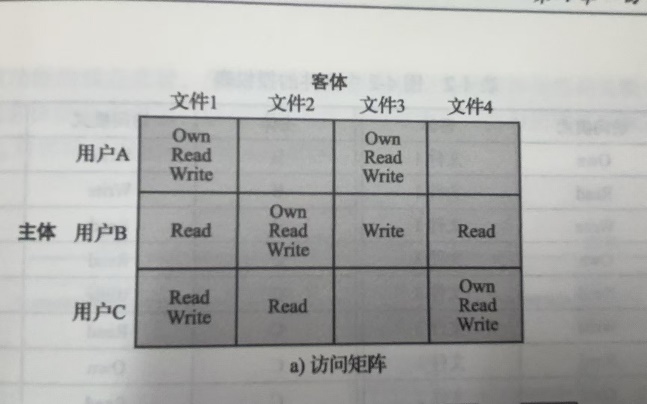


RBAC基于用户在系统中具有的角色和说明各种角色享有哪些访问权的规则来控制访问。RBAC既可使用DAC策略，也可使用MAC策略

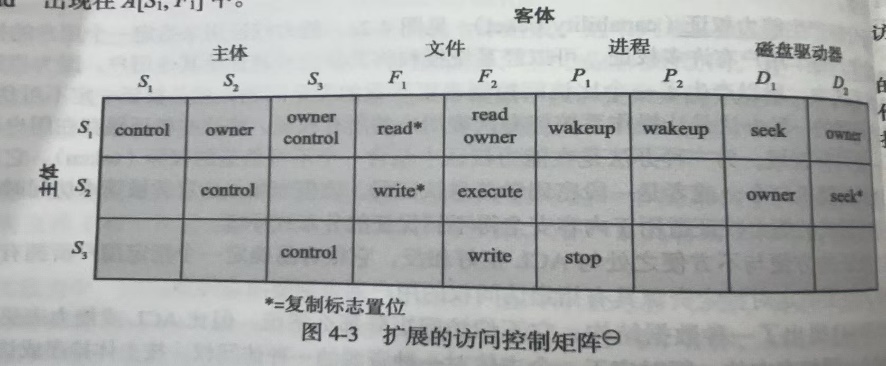
Problems：



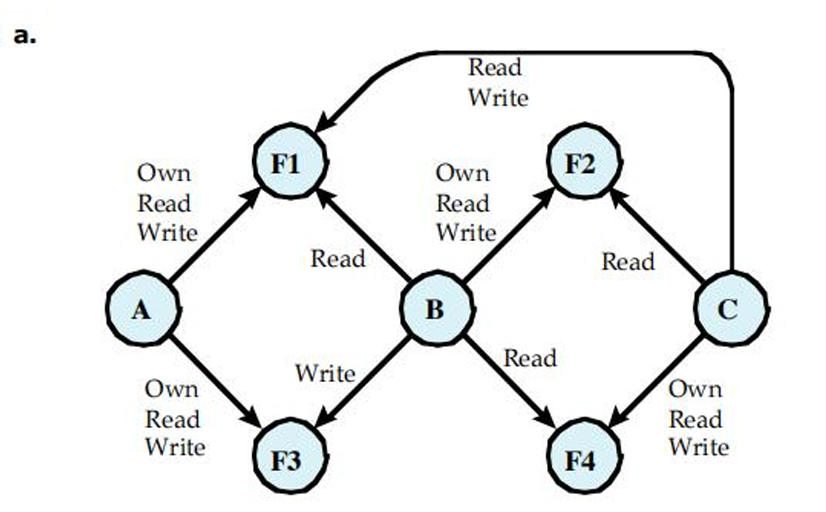
4.2a的图：

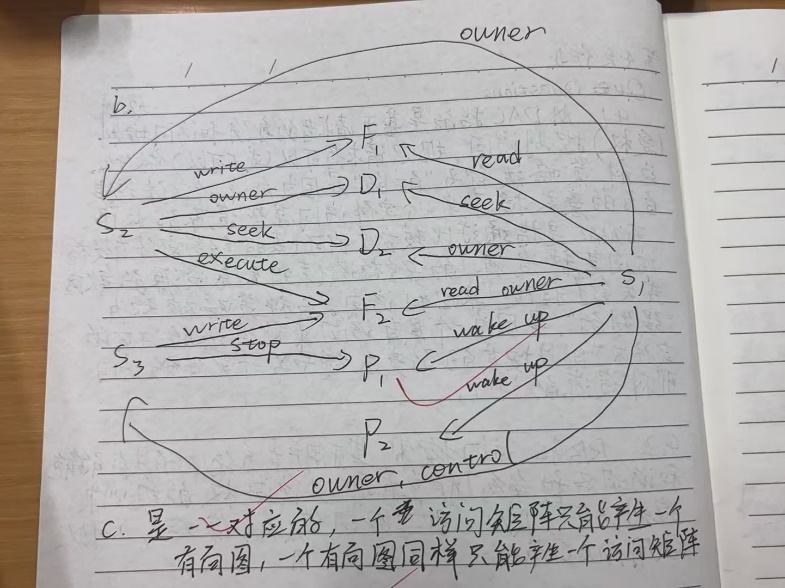


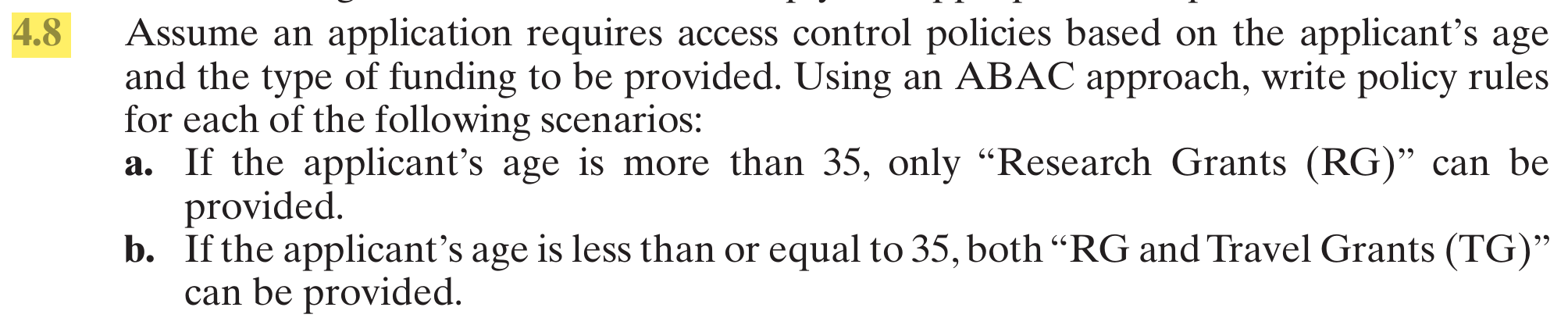
4.3的图：



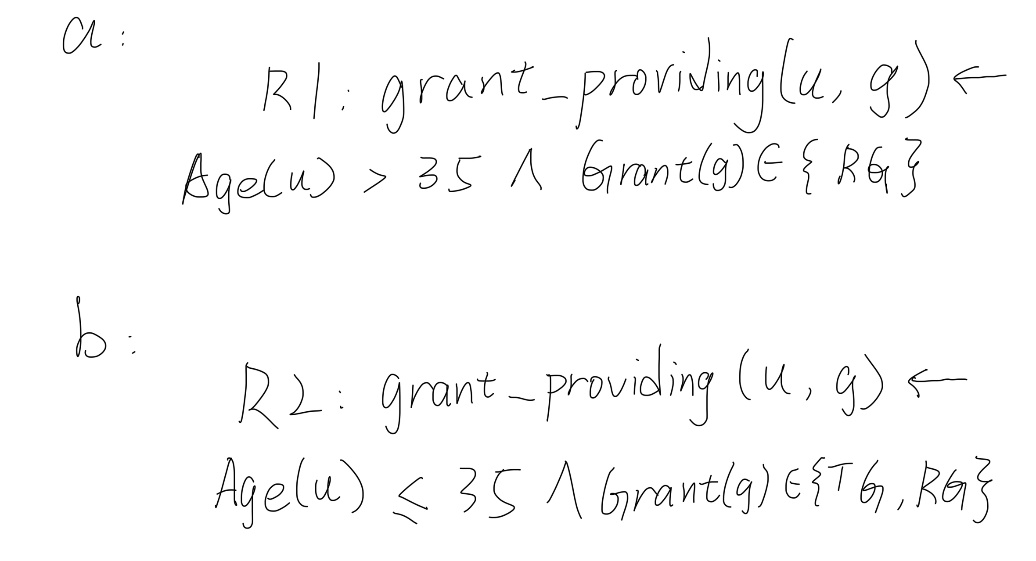
答案：

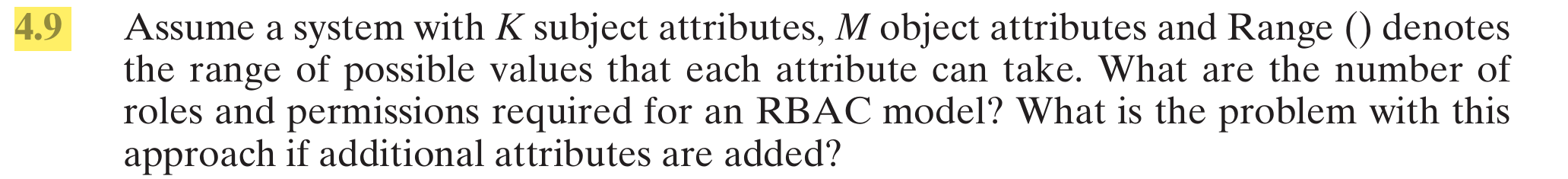




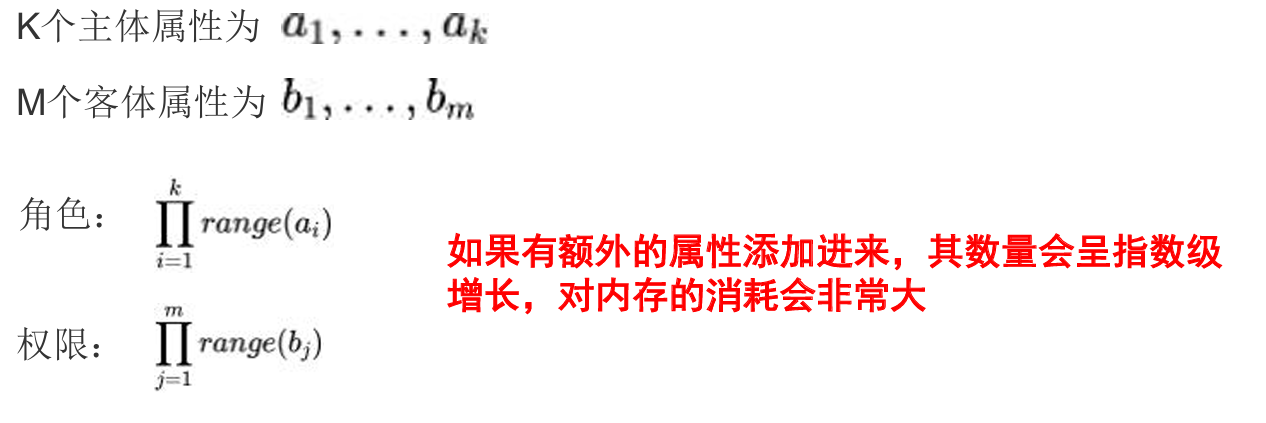


（本题我是仿照书上4.6.3现做的，我不知道正确答案，如果觉得不对，请指正）





书上4.6.3节有，答案为：



第五章

Questions：



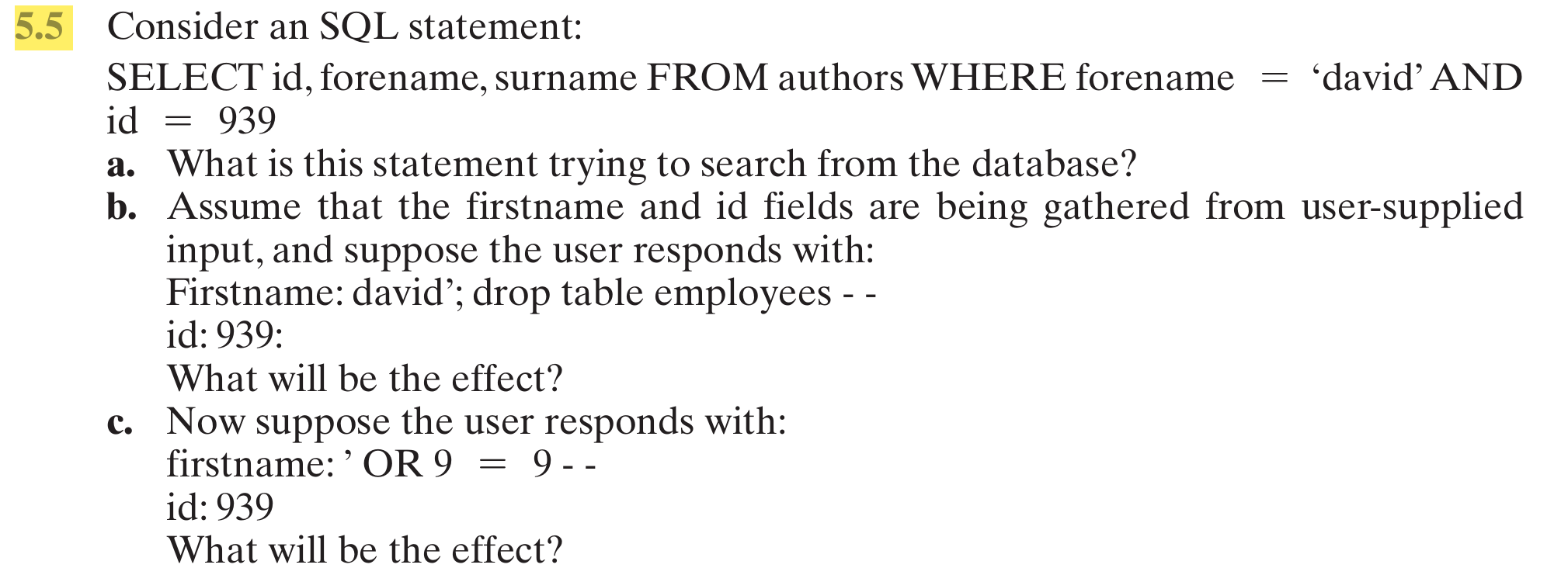
关系数据库是一个关系的集合，使用各种表格来表示关系，表中的唯一标识符可以用来连接多个表。



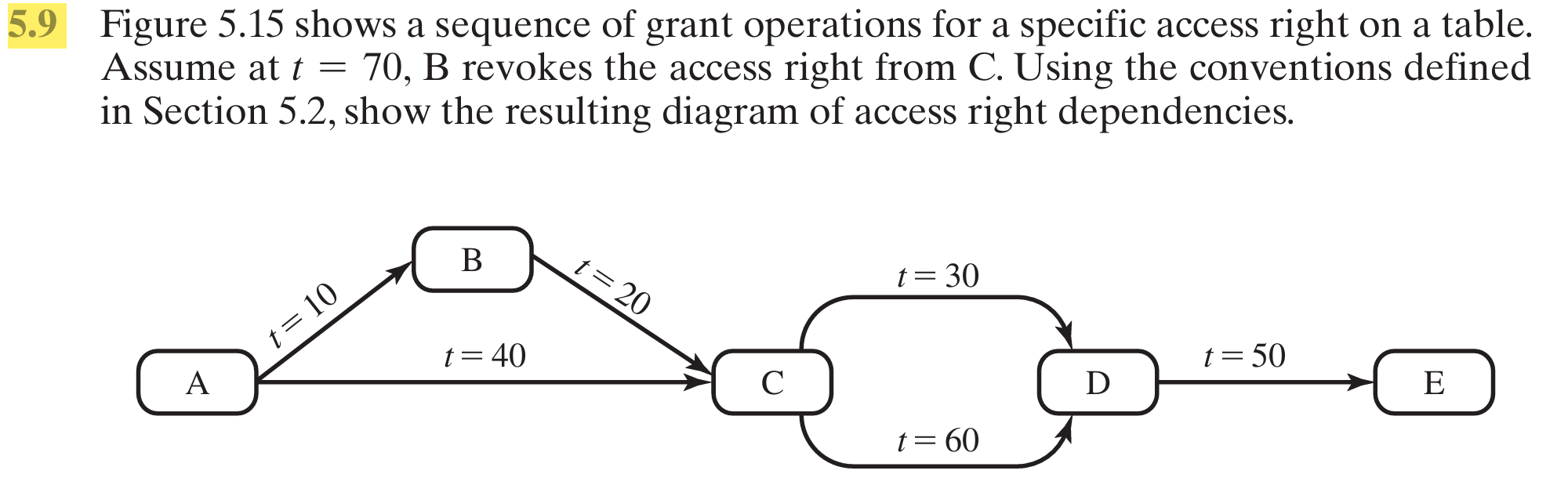
（未在书上找到，但是在ppt上找到了）

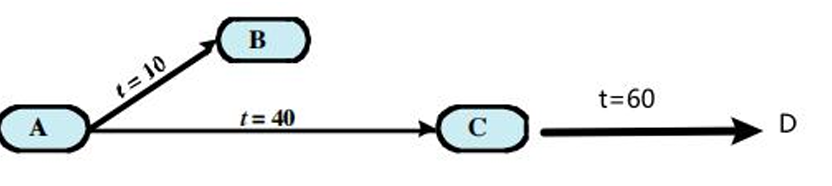
Can be applied to the entire database, at the record level, the attribute level, or level of the individual field

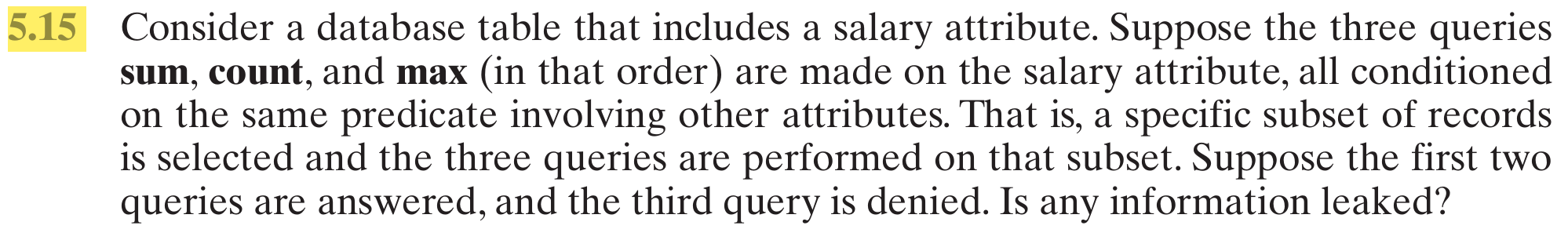
Problems：



1. 找到author表所有中名（forename）为david且id为939的项
2. 先查找author表中所有名为david的表项，然后删除employees表。
3. 列出author表的所有表项







这道题的意思是使用推理攻击反推出max = sum/count，理论上数据库应该返回给我max（如果sum/count不等于max的话，给个max是不会泄露什么信息的），但是现在没有返回给我，说明了max = sum/count。