1. 哪些内容可以作为识别垃圾邮件的特征?

① 发件人信息。垃圾邮件常常使用虚假或者不可信的发件人地址，或者是一些看起来随机的字符组合。垃圾邮件的发件人地址通常是免费邮箱或临时邮箱且经常变化，被列入黑名单，发件人 IP 地址来自可疑或恶意来源，与邮件内容无关。电子邮件地址格式奇怪，包含大量随机字符。发件人域名看起来可疑或与内容无关，或则域名与知名品牌相似，但存在细微拼写错误。

② 邮件主题。垃圾邮件的主题内容含糊不清通常涉及到赚钱、促销、降价、诈骗等内容，或者是与收件人无关的词汇组合，例如“重要信息”、“免费赠品”、“快速致富”等，与邮件内容无关或者是包含大量特殊字符或表情符号

③邮件内容。垃圾邮件的内容可能包含大量的广告、链接、诱骗性文字或者是不良内容。同时，垃圾邮件的文本常常包含拼写错误、语法不通或者乱码等问题，邮件内容排版混乱，字体大小或颜色不一致。垃圾邮件内容通常与主题无关，包含大量广告、促销信息、虚假信息或诈骗信息，要求收件人提供银行账号、密码等敏感信息。有的垃圾邮件还包含恶意链接或附件例如可执行文件、压缩文件或脚本文件，这些链接指向非官方或可疑网站，打开这些附件可能会导致计算机感染病毒或恶意软件。

④邮件格式。邮件格式不规范，例如缺少必要的字段或包含错误的语法或者出现如拼写错误、语法错误、文本混乱等错误。邮件中包含大量图片或附件，邮件中包含大量 HTML 代码或 JavaScript 代码等

⑤邮件头和频率。垃圾邮件头中的信息可能揭示出垃圾邮件的真实来源或者特定的邮件传输规则。如果某个发件人频繁发送类似内容的邮件或者是收件人突然收到大量来自同一发件人的邮件，这可能是垃圾邮件的标志。

2. 小明是一个程序员，发明了一个非常好用的软件，把软件做成一个安装光盘，安装在 Windows 系统中就能使用，但是由于他对于安全技术不是很了解，故受到盗版问题的困扰，需要你的帮助。请简述如何设计一个版权保护模块，防止盗版使用软件，方法不限。

①使用 DRM 技术，对于每一份正版软件，都用 NEC 算法为其生成数字水印，并存储于服务端，利用密钥和数字水印对软件进行版权处理，生成被加密的受保护文件，同时生成针对该受版权保护文件的授权许可，加密的软件头部存放着密钥识别码和软件授权中心的 URL 等内容。每次用户启动软件时，都必须进行联网并与服务器进行数字水印比对，比对不成功就无法启动软件。或者使用 SecureBrun、Roxio Media Creator 等软件制作需要刻录的加密文件。这样，刻录后的光盘需要密码才能打开，否则光盘信息无法显示，以此保护光盘数据不被盗用。

②基于硬件锁的验证，将一个硬件锁插入计算机的 USB 端口。硬件锁包含唯一的标识信息。软件会在运行时检查硬件锁的存在和有效性。如果没有检测到硬件锁或硬件锁无效，软件将停止运行或限制功能。将软件与用户的硬件设备（如主板、网卡等）绑定，使得软件只能在特定设备上运行。这样可以防止用户将软件复制到其他设备上使用。

③在安装软件时，用户需要输入由开发者提供的唯一激活码或序列号。软件在运行时验证该激活码的有效性，如果激活码无效或重复使用，则限制软件功能或者直接阻止软件运行。也可以在软件安装过程中，将软件的注册信息写入 Windows 注册表。软件会在运行时读取注册表信息，验证软件是否已注册。如果没有注册或注册信息无效，软件将停止运行或限制功能。

④添加支持运行认证的功能。软件安装程序加密存放在光盘安全区内，只有输入正确的密码才能打开安全区，运行安装程序；程序正确安装

后，安装光盘转换为运行认证工具，和主程序保持双向通信认证，在光盘处于工作状态时，主程序才能正常运行，从而确保一套软件对应一个光盘，杜绝盗版。

⑤加密存储, 防止拷贝，实际使用时可以使用 CD-protector 等光盘加密软件，其工作原理是在可执行文件上加一个壳，通过这个壳来判断光盘是有没有加密后所产生的对应音频轨道，如果有则运行，没有则拒绝运行。使用该软件加密后，别人无法通过拷贝的方法直接得到光盘中的文件，即使将所有文件复制到硬盘上也无法直接使用。