作系统一定要有好的安全性。一种保证信息机密的方法是把它加密并妥善地保管密钥。有时候提供数字信息的验证是很重要的，在这种情况下，可以使用加密散列表、数字签名，以及被一个可信的证书验证机构所签名的证书。

对信息的访问权限可以模型化为一个大矩阵，行表示域（用户），列表示对象（文件）。每一个元素表示相应的域对相应对象的访问权限。因为这个矩阵是稀疏的，所以它可以按行存储，这样就成了一个能力链表，表示某一域能够做什么；或者稀疏矩阵也可以按列存储，这样就成了一个访问控制链表，表示谁并且如何访问这个对象。使用正式的建模技术，系统里的信息流可以被模型化并受到限制。但是，有时利用隐秘的通道还是可以泄露出去的，比如调整CPU的利用率。

在任何一个安全的系统一定要认证用户。这可以通过用户知道的、用户拥有的，或者用户的身份（生物测定）来完成。使用双因素的身份认证，比如虹膜扫描和口令，可以加强安全性。

代码中有很多bug可以被利用来控制程序和系统。这些包括缓冲区溢出、格式串攻击、返回libc攻击、整数溢出攻击、代码注入攻击和特权扩大攻击。

Internet上遍布恶意软件，有特洛伊木马、病毒、蠕虫、间谍软件和rookit。每一个都对数据机密性和一致性产生着威胁。更糟糕的是，恶意软件攻击可能会控制一台机器，并把这台机器变成一台僵尸机器用来发送垃圾邮件或者发起其他的攻击。

幸运的是，系统有很多种方法来保护自己。最好的策略就是全面防御，使用多种技术一起防御。这些技术有防火墙、病毒扫描、代码签名、囚禁、入侵检测，以及封装移动代码。

习题

1. 破译下列的单一字符替换密文。明文包含的仅仅是字母，并且是Lewis Carroll的著名诗歌。

   kfd ktbd fzm eubd kfd pzyiom mztx ku kzyg ur bzha kfthcm

   ur mfudm zhx mftnm zhx mdzythc pzq ur ezsszcdm zhx gthcm

   zhx pfa kfd mdz tm sutythc fuk zhx pfdkfdi ntcm fzld pthcm

   sok pztk z stk kfd uamkdim eitdx sdruid pd fzld uoi efzk

   rui mubd ur om zid uok ur sidzkf zhx zyy ur om zid rzk

   hu foiia mztx kfd ezindhkdi kfda kfzhgdx ftb boef rui kfzk

2. 假设有一个私密密钥使用了26×26矩阵，行与列都以ABC...Z开头。明文每次用两个字符加密。第一个字符是列，第二个字符是行。每个单元由包含两个密文字符的行和列交叉组成。这样的矩阵必须有些什么限制？共有多少个密钥？
3. 私密密钥机制比公钥机制更有效，但需要发送者和接收者事先共用一个密钥。假设发送者和接收者从未碰到过，但有可信的第三方与发送方共享密钥与接收方也共享密钥（另一个）。那么发送方和接收方如何在这种环境下建立一个新的共享密码体制？
4. 举一个简单例子说明一个数学函数，对一级近似来说这一函数是单向函数。
5. 假设有A和B两个陌生人想使用对称密钥加密和对方交流，但是没有共享对称钥匙。假设他们俩都信任第三方C，C的公钥是大家都知道的。在这种情况下两个陌生人如何建立一个新的对称密钥？
6. 假设一个系统在某时有1000个对象和100个域。在所有域中1%的对象是可访问的（r、w和x的某种组合），两个域中有10%的对象是可访问的，剩下89%的对象只在惟一一个域中才可访问。假设需要一个单位的空间存储访问权（r、w和x的某种组合）、对象ID或一个域ID。分别需要多少空间存储全部的保护矩阵、作为访问控制表的保护矩阵和作为能力表的保护矩阵？
7. 我们讨论过的两种保护机制有能力表和访问控制表。对于下面每个保护问题，请问应该使用哪个机制。

   a) Ken希望除了他的某位办公室的同事之外，其他所有人都可以读到他的文件。

   b) Mitch和Steve想要共享一些秘密文件。

   c) Linda想要她一部分的文件是公开的。
8. 说出在这个UNIX目录里所列保护矩阵的所有者和操作权限。请注意，asw属于两个组：users和devel；gmw仅仅是users组的成员。把两个成员和两个组当作域，矩阵就有四行（每个域一行）和四列（每个文件一列）。