1.有哪些常见的密码分析攻击方法？各自有什么特点

1. 唯密文攻击：攻击者在仅已知密文的情况下企图对密文进行解密，这种最容易防范。
2. 已知明文攻击：攻击者获得了一些密文信息及其对应的明文,也可能知道某段明文信息的格式等
3. 选择明文攻击：攻击者可以选择某些他认为对攻击有利的明文并获取其相应的密文
4. 选择密文攻击：密码攻击者事先搜集一定数量的密文,让这些密文通过被攻击的。更有加密算法解密,从而获得解密后的明文。

以上几种攻击的强度依次增强。如果一个密码体制能够抵抗选择密文攻击,则它能抵抗其余3种攻击

2.古典密码常用的两个技术是什么？各自有什么特点？

代换和置换是古典密码学中两种主要的技术

代替技术就是将明文中每一个字符替换成另外一个字符从而形成密文

置换技术则是通过重新排列明文消息中元素的位置而不改变元素本身从而形成密文