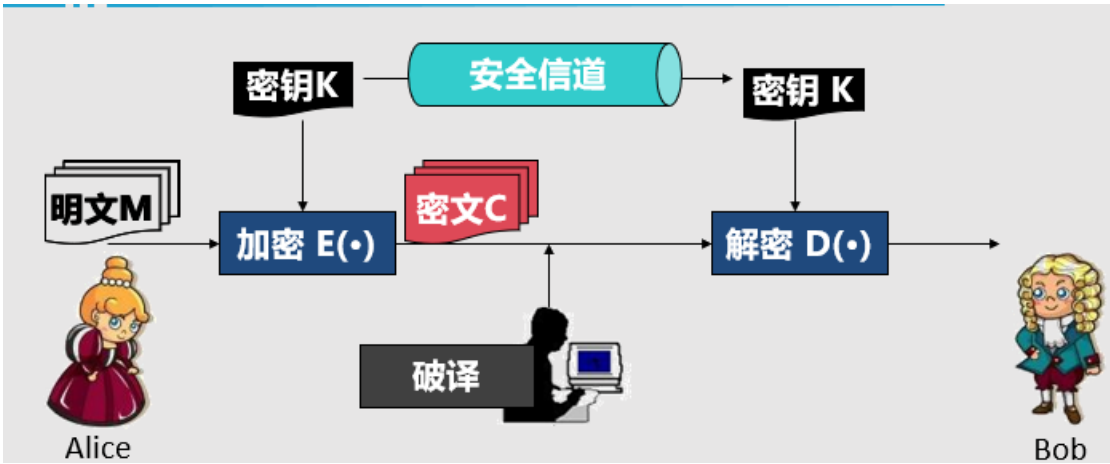
密码学的地位：密码学是信息安全的基础（提供理论基础/技术支持）

信息安全三要素：机密性，完整性，可用性
攻击形式：被动攻击（对机密性的破坏），主动攻击（对完整性、可用性等的破坏）
密码学主要功能：

- 保证机密性
- 保证完整性
- 提供非否认

什么是密码学？（研究内容：保护系统安全）
包括密码编码学和密码分析学
帮助分析算法密码的安全性，帮助破坏受保护信息的安全性

明文：需要加密的信息
加密：隐藏信息的过程
密文：加密后的密文
解密 从密文恢复明文的过程
密码分析： 破译密码的过程



密钥：用于变换：密码算法的辅助输入，是一些随机串
口令：用于身份认证即密码

柯克霍夫斯原则 密码学的基本原则
即使密码系统的任何细节已为人所知只要密钥没有泄漏它也应该是安全的

柯克霍夫斯原则的意义

1.知道算法的人会叛变

2 设计者的个人喜好

3 频繁更换算法不现实（设计算法很难）

加解密是在密钥的控制下进行的

加密算法(函数)必须是一个单射函数

实用的加密体制需满足以下条件：

1 容易性（加密解密算法都应易于计算）

2 安全性（对于任何攻击者难以恢复明文/密钥）

隐写术：

特点：保护的是·信息本身（把信息隐藏起来）

缺点：安全性差

加密术(置换)

特点:明文中字符与密文中相同，只是出现的位置发生变化

密钥是什么？改变位置的规则

加密术（代换）

明文中出现的字符不一定出现在密文中，但位置保持不变

此时密钥是：代换规则

隐写术与加密术的区别

隐写术：　　保护的是信息本身，传递的仍是原来的信息，只是被藏了起来

　　一旦发现隐藏的方法，信息就会暴露

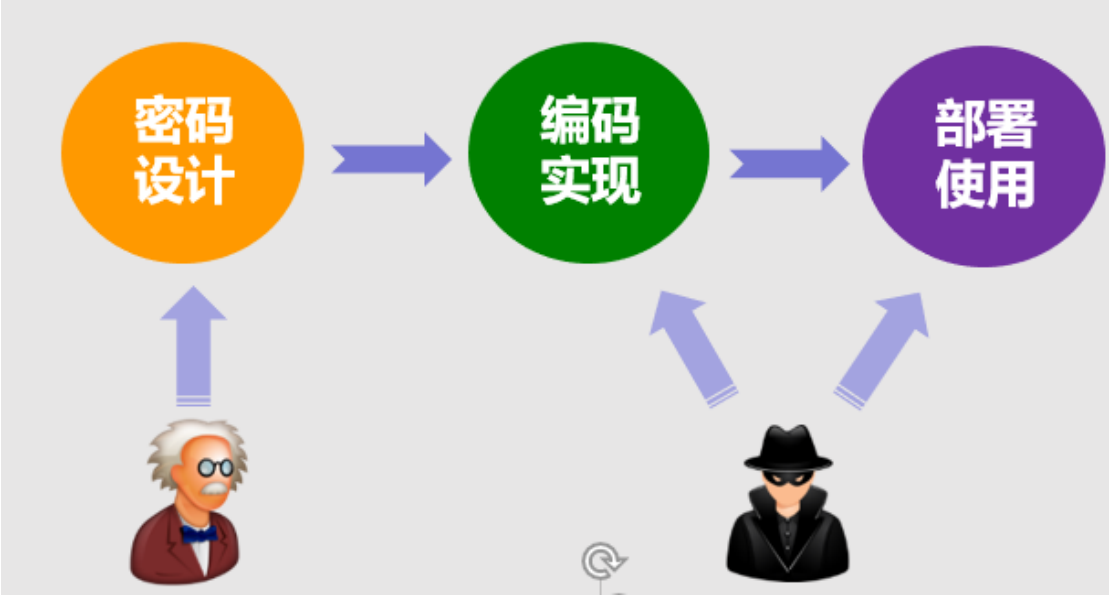
加密术：　　保护的是信息内容，传递的是变换后的密文，而不是原来的明文

　　不知道密钥，很难恢复信息

对加密体制进行攻击的分类

1.唯密文攻击　只有一些密文，好的现代密码系统对此通常是免疫的
2 已知密文攻击　已经有很多对密文/明文对
3 选择明文攻击　可以任意选择明文，并可获得相应密文
4 选择密文攻击　可以任意选择密文，并可获得相应明文

密码设计 vs 密码实现



设计上安全的密码算法，由于实现或使用不当，可能引入安全漏洞

恢复明文和恢复密钥
破译的主要目的：恢复密钥
　　因为知道了密钥，便可恢复出该密钥加密的所有明文
　　（当然有些时候，破译的目的也在于恢复特定的明文）
通过密文推导密钥，至少要和推导明文一样困难

同等对待所有密钥，不要根据自己的偏好选择密钥
（以防攻击者根据你的偏好缩小密钥范围）即密钥应随机选择

全部破译和部分破译
　恢复出明文的部分信息，甚至几个关键单词，也算成功破译

穷举攻击 vs 其他攻击
穷举攻击（暴力攻击，蛮力攻击）

目的： 穷举搜索密钥
方法： 依次测试密钥空间中的所有密钥
密钥空间要足够大，以抵抗密钥穷举攻击

保密密钥 vs 保密算法
根据柯克霍夫斯原则，对密码进行分析的前提是，在不知道密钥的条件下，对公开的密码算法进行分析。
但在政府或军事应用中，也存在保密算法的情况。
不过前提是，算法必须是安全的。通过保密算法进一步加强安全性。

对密码安全性的一些直观认识

- 密钥空间要足够大
- 密钥应该随机选择
- 通过密文推导密钥，至少要和推导明文一样困难

明文与密文之间的统计关系要尽量小
密钥与密文之间的统计关系要尽量小
……

1. 信息安全三要素是 （**机密性、完整性、可用性**）
2. 密码学由(**密码编码学、密码分析学**)两部分组成?
3. 加密的两种基本技术是（ **置换、代换** ）
4. 按照攻击者知道信息的多少，密码分析
   （**唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击**）
   四种类型

5. 加密和解密都是在（ **B** ）控制下进行的
   A.口令 B.密钥 C.字符串 D.算法
6. 以下哪种攻击破坏数据的机密性（ **B** ）
   A. 篡改 B.窃听 C.冒充 D.匿名
7. 以下哪种属于被动攻击（ **B** ）
   A. 篡改 B.窃听 C.冒充 D.以上答案都不对