密码学发展大致分为哪几个阶段及各阶段特点
现代密码的两次飞跃和两个里程碑事件
密码算法公开的意义
DES 加密算法的要素及安全性
DES 的设计思想及其含义
密钥序列产生器的基本要求
现代密码体制的分类以及对称密码的分类

密码学发展历程:
三个阶段：古典密码时期（传统），　特点：　手工，信使，　代换及置换
近代密码时期（传统），　特点：机械设备，电报，　较复杂（如轮转密码）
现代密码时期：　特点：计算机　通信手段：无线有线通信、计算机网络
密码体制：对称密码和非对称密码（公钥密码）
现代密码时期才是一门科学
举例：DES\AES\SHA\RSA

两次飞跃，里程碑事件
第一次飞跃 Shannon《保密系统的通信理论》 从此密码学成为科学
里程碑事件：DES：美国数据加密标准，其主要贡献在密码算法公开（分组密码的典型代表
第二次飞跃：D\H 发表《密码学的新方向》提出新的密码设计思想，开创公钥密码学
里程碑事件：RSA 公钥密码体制，实用，使公钥密码的研究快速发展

密码算法公开的意义
1. 安全性，接受大众检验
2. 利于推广应用：相同算法才能实现保密通信
3. 增加用户信心，不会泄露给算法设计者因为他没有密钥
4. 利于发展，公开设计思想，密码设计者可以取长补短

DES 设计思想（分组密码）
1. 扩散：p 盒
   雪崩效应，密文任意比特尽可能与明文、密钥相关联，明文和密文任何一比特值发生改变时密文都要尽可能地被影响

2. 混乱：s 盒
   关系尽可能地复杂化，防止破译者采用解析法进行破译攻击
   混乱的每步必须是可逆的，按照混乱原则，分组密码算法应有复杂的非线性因素

DES 加密系统的基本要素:
明文分组，密钥，密钥根据子密钥生成算法生成子密钥 K1…Kn,通过轮函数 F 经过 n 次迭代次数加密生成密文分组。
DES 加密算法的要素：子密钥生成算法，轮函数 F，迭代次数
轮函数：分组密码的核心，基本准则：扩散（雪崩效应）混乱（非线性、可逆性）

DES 算法的优点是加解密算法相同，但并不是所有的分组密码都有这个优点，如 AES 算法加解密算法不同
DES 的安全性：
密钥长度 des 密码长度是 56 位

AES 的基本要求是比三重 DES 快、安全

分组密码应用：构造伪随机数生成器、序列密码、认证码、哈希函数，习惯上是对称分组密码

序列密码：对称密码体制，又称流密码，基于伪随机序列，密钥序列是随机的，所以序列密码是“一次一密”密码体制（在理论上不可破译）
过程：明文按一定长度分组，一般是一位，对各组用“随机”的密钥序列加密，解密时也用相同的密钥序列分组解密
序列密码特点：1.加解密是异或运算 2.密码安全度依赖于密钥序列的安全性 3.加解密没有分组限制

序列密码是逐位进行加密，序列密码的扩散性不强，序列密码中篡改一位明文只会影响到一位密文
密钥序列产生器（KG）的基本要求：
1. 密钥长度在 128 位以上，因为密钥序列生成器的算法是公开的，需要抵御穷举攻击
2. 极大周期，密钥序列周期应大于使用密钥序列的长度
3. 随机性 要具有均匀的 n 元分布
4. 不可逆性：不能根据 Ki 提取种子密钥
5. 雪崩效应：种子密钥 K 改变引起 Ki 全貌上的变化
6. ki 不可预测：知道前面也不能确定后续的

现代密码体制的分类：
1. 对称密码体制（又称传统密码体制，私秘秘钥体制，但密钥体制）加解密密钥相同或则不同但容易推出另一个。
   从密钥使用方式上分为分组密码和序列密码
2.非对称密码体制（公钥密码体制）
加解密密钥不同且难相互推出，其中一个可以公开，公钥，另一个要私密保存，私钥