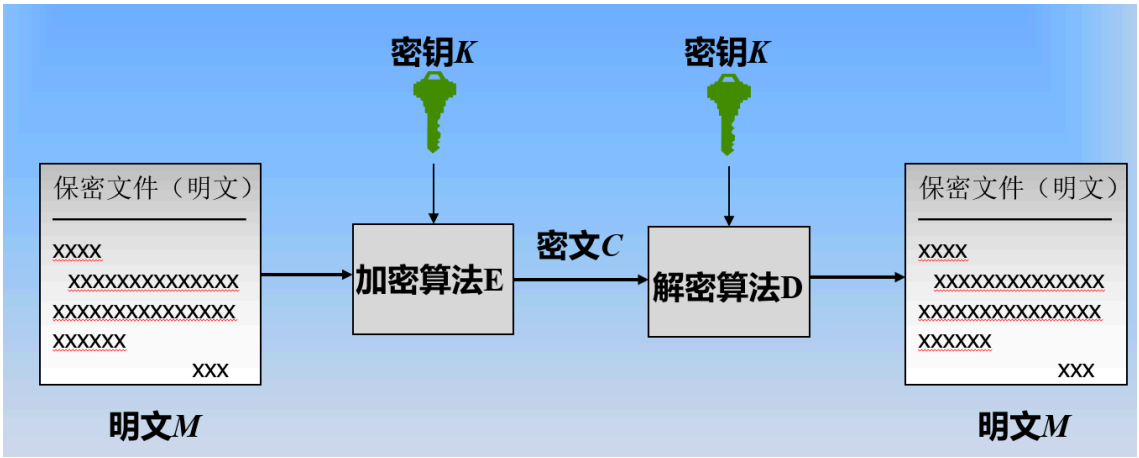
对称加密原理

对称加密模型

- 对称加密：发送方和接收方共享同一密钥
- 明文：原始消息
- 密文：编码后消息
- 密钥：发送方和接收方使用的秘密信息
- 加密器(加密算法)：将明文转换成密文的算法
- 解密器(解密算法)：将密文转换成明文的算法
- 模型



- 对称加密/解密算法可以表示为：

$$C = E(k, M)$$
$$M = D(K, C)$$

其中C是密文，M是明文，K是私钥，E是加密算法，D是解密算法。

- 对称密码的安全要求
  1. 两个安全使用要求：一个强安全的加密算法；只有发送方和接收方才知道私钥
  2. 加密算法是公开的
  3. 存在一个安全的通道去分发私钥

密码体制分类

- 按明文转换成密文的操作类型：
  - 替换密码：每一个元素（比特或字母）都映射到另外一个元素
  - 换位密码：所有元素都被重新再排列。
  - 乘积密码：包括了多级替换和换位组合
- 按使用的密钥数
  - 对称、单钥、秘密密钥或者传统加密：发送者和接收者都使用同一密钥。
  - 不对称、双钥或者公钥加密：发送者和接收者使用不同的密钥
- 按明文处理方式
  - 分组密码：一次处理一个输入元素分组，产生相应的一个输出分组。

- 流密码：运行过程中连续地处理输入元素，每次产生一个输出元素

密码分析

- 常见的攻击方法：
  1. 密码分析攻击：依靠加密算法的固有性质、明文的一些特征或者一些明密文对，推导分析出明文或使用的密钥。

     密码分析攻击有如下类型：

     - 唯密文攻击：加密算法；要解密的密文
     - 已知明文攻击：加密算法；要解密的密文；用密钥产生的一个或多个明文-密文对
     - 选择明文攻击：加密算法；要解密的密文；破译者选定明文消息，以及使用密钥产生的对应密文
     - 选择密文攻击：加密算法；要解密的密文；破译者选定密文，以及使用密钥产生的对应解密明文
     - 选择文本攻击：加密算法；要解密的密文；破译者选定明文消息，以及使用密钥产生的对应密文；破译者选定密文，以及使用密钥产生的对应解密明文
  2. 穷举搜索攻击：对特定的密文尝试所有可能的密钥，直到把密文转换为可读的有意义明文。

     简单尝试每一个密钥，攻击时间与密钥空间大小成正比，下面表格列出穷举搜索不同大小的密钥所花费时间。

密钥长度（比特）	密钥空间大小	以1秒加密10^9次的速率需要的时间	以1秒加密10^{13}次的速率需要的时间
32	$2^{32} = 4.3 \times 10^9$	2^{31} ns = 2.15 秒	215 μs
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} ns = 1.142 年	1.0 小时
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} ns = 5.4×10^{21}年	5.4×10^{17}年
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} ns = 5.9×10^{33}年	5.9×10^{29}年
26 字母(置换)	$26! = 4 \times 10^{26}$	2×10^{26} ns = 6.4×10^9年	6.4×10^5年

- 密码安全
  - 无条件安全：无论花多少时间，无论有多少已知信息，都不能唯一确定密文所对应的明文。一次一密可以保证无条件安全。
  - 计算安全：破译密文的代价超出被加密信息的价值；破译密文的时间超出信息的有效生命期。

古典密码

替换密码

将明文每一个元素（比特或字母）映射到另外一个元素

- 凯撒（Caesar）密码：最早的替换密码，26个小写英文字母按顺序与0-25数字相对应，对字母表中的每个字母用它之后的第三个字母进行替换。

  加密算法：$c = \mathbf{E}(3, m) = m+3 \pmod{26}, 0 \le m \le 25$

  解密算法：$m = \mathbf{D}(3, c) = c - 3 \pmod{26}, 0 \le c \le 25$

- 移位密码：对字母表中的每个字母用它之后的第k个字母进行替换。

  加密算法：$c = \mathbf{E}(k, m) = m+k \pmod{26}, 0 \le m \le 25$

  解密算法：$m = \mathbf{D}(k, c) = c - k \pmod{26}, 0 \le c \le 25$

维吉尼亚密码：属于多表替换方法，对第i个字母用它之后的第k_i个字母进行替换。假设给定d个字母序列的密钥$K=(k_1,k_2,\ldots,k_d)$，其对第$i+td$个字母（t为正整数）的加解密操作如下：

加密算法：$c_{i+td} = \mathbf{E}(K, m_{i+td}) = m_{i+td} + k_i \pmod{26}$

解密算法：$m_{i+td} = \mathbf{D}(K, c_{i+td}) = c_{i+td} - k_i \pmod{26}$

- 轮转机：现代密码出现之前，属于较为复杂的密码系统，是一个非常复杂多变的多表替换密码系统
- 3个圆筒的轮转机系统有$26^3=17576$个不同的替换字母表。

换位密码

- **栅栏密码：对角线顺序写入明文，行顺序读出作为密文，如：**

  明文： meet me at shenzhen university

  密文： m e m a s e z e u i e s t
  e t e t h n h n n v r i y

- **行变换密码：把消息一行一行写成矩形块，按列读出，但是把列次序打乱，列的次序就是密钥，如：**

  密钥： 8 4 3 1 2 5 6 7

  明文： m e e t m e a t
  s h e n z h e n
  u n i v e r s i

  密文： tnvmzeeeiehnehraestnimsu