> 教材第三章。可汗学院公开课「古典密码学」

对称密码模型

五个基本成分：明文、加密算法、密钥、密文、解密算法。

密码编码学（Cryptography）

密码编码学系统具有以下三个独立的特征：

（1）**转换明文为密文的运算类型** 所有的加密算法都基于两个原理：代替和置换，代替是将明文中的每个元素（如位、字母、位组或字母组等）映射成另一个元素；置换是将明文中的元素重新排列。上述运算的基本要求是不允许有信息丢失（即所有的运算是可逆的）。大多数密码体制，也称为乘积密码系统，都使用了多层代替和置换。

（2）**所用的密钥数** 如果发送方和接收方使用相同的密钥，这种密码就称为对称密码、单密钥密码、秘密钥密码或传统密码。如果发收双方使用不同的密钥，这种密码就称为非对称密码、双钥或公钥密码。

（3）**处理明文的方法** 分组密码每次处理输入的一组元素，相应地输出一组元素。流密码则是连续地处理输入元素，每次输出一个元素。

密码分析学（Cryptanalysis）和穷举攻击

攻击传统的密码体制有两种通用的方法：

- 密码分析学
- 穷举攻击

代替技术

单表代替加密

代表技术：凯撒密码（移位也属于单表代替）。

> 单表代替密码较容易被攻破，因为它带有原始字母使用频率的一些**统计学特征**。一种对策是对每个字母提供多种代替，称为同音词（就像一个读音可以代表多个单词的同音词一样），一个明文单元也可以变换成不同的密文单元。比如字母 e 可以替换成 16，74，35 和 21

多表代替加密

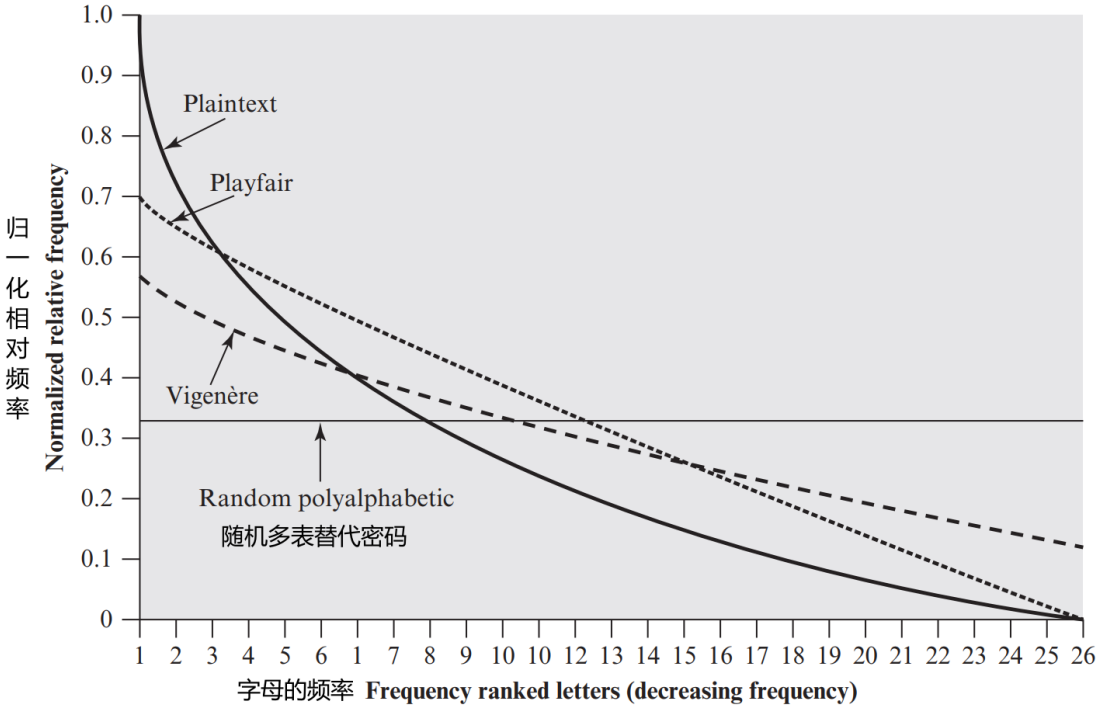
代表技术：

- PlayFair：双字母音节作为一个单元，具体加密方式在教材 P56
- Hill 密码：涉及矩阵变换，将 m 个连续的明文字母（字母可被指定为一个数值，如 $a=0$，$b=1$ ...）替换成 m 个密文字母，$m=3$ 时可描述为：

$$(c_1 c_2 c_3) = (p_1 p_2 p_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

- Vigenère 密码：流密码（示例如下），可通过转化为多个单表替换进行攻击

```
明文：ATTACKATDAWN
密钥：LEMONLEMONLE
密文：LXFOPVEFRNHR
```



PlayFair 和 Vigenère 密码都保留了许多频率信息，而 Hill 密码完全隐藏了单字母频率特性。

一次一密

- 使用与消息一样长且无重复的随机密钥来加密消息，且密钥只对一个消息进行加解密，之后丢弃不用（多次使用同一个密钥存在风险，见实验一）
- 和 Vigenère 密码一样，也是通过异或操作进行加解密
- 由于密钥的产生、分配和保护问题存在困难，一次一密实际上很少使用

置换技术

相当于打乱明文顺序。

到目前为止我们所讨论的都是将明文字母代替为密文字母。与之极不相同的一种加密方法是对明文进行置换，这种密码称为置换密码。

最简单的例子是栅栏技术，按照对角线的顺序写出明文，而按行的顺序读出作为密文。例如，用深度为 2 的栅栏技术加密信息“meet me after the toga party”，可写为

```
m e m a t r h t g p r y
  e   t   e   f   e   t   e   o   a   a   t
```

加密后的信息是

```
MEMATRHTGPRYETEFETEOAAT
```

这种技巧对密码分析者来说实在微不足道。一个更复杂的方案是把消息一行一行地写成矩形块，然后按列读出，但是把列的次序打乱。列的次序就是算法的密钥。例如

```
密钥:    4   3   1   2   5   6   7
明文:    a   t   t   a   c   k   p
         o   s   t   p   o   n   e
         d   u   n   t   i   l   t
         w   o   a   m   x   y   z
密文:    TTNAAPTMTDUOADWCDIXKNLYPETZ
```

因此在本例中，密钥是 4312567。为了加密，从标号为 1 的那列开始，本例中为第 3 列。写下那列的所有字母，接着是标号为 2 的列，即第 4 列，接着第 2 列，第 1 列，第 5，6，7 列。

单纯的置换密码因为有着与原始明文相同的字母频率特征而易被识别。对于上述所示的列变换类型密码，密码分析很直观，可以从将密文排列成矩阵入手，再来处理列的位置。双字母音节和三字母音节频率表分析可以派上用场。

多次置换密码相对来讲要安全得多。这种复杂的置换是不容易重构的。前面那条消息用相同算法再加密一次

```
密钥:    4   3   1   2   5   6   7
明文:    t   t   n   a   a   p   t
         m   t   s   u   o   a   o
         d   w   c   o   i   x   k
         n   l   y   p   e   t   z
密文:    NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

转轮机

进行多次代替

隐写术