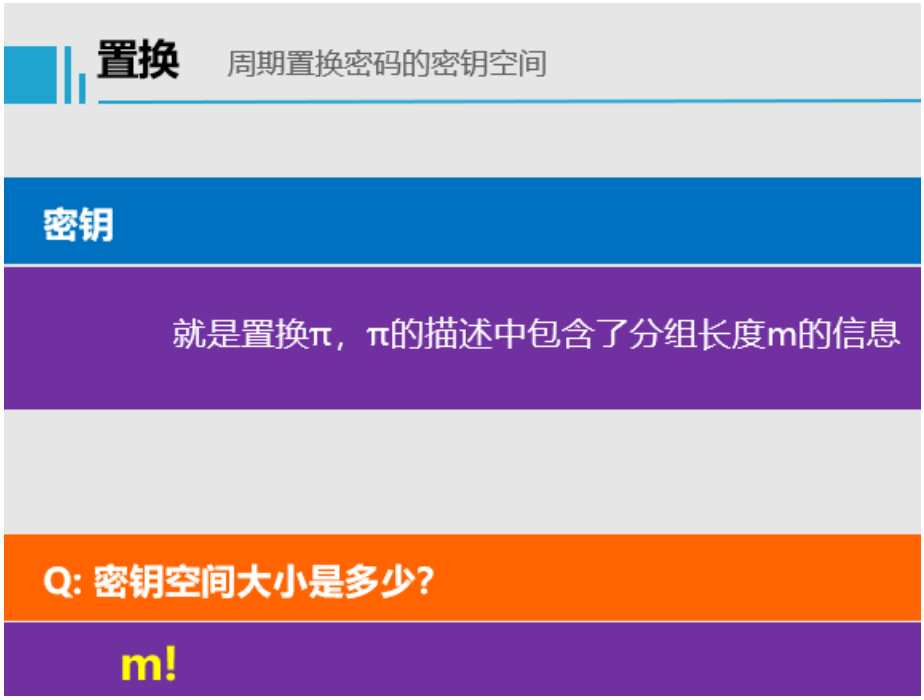
置换：
古典密码的一种最基本的处理技术
改变明文中各字符的相对位置，但明文字符本身的取值不变
典型代表：周期置换密码



单表代换密码：
代换：古典密码的另一种最基本的处理技术
改变明文中各字符的取值
但明文字符的出现位置不变

凯撒密码 明文字母代换为字母表中其后第 3 个字母

移位密码：
工作原理
- 加密 明文字母代换为字母表中其后第 k 个字母
- 解密 密文字母代换为字母表中其前第 k 个字母（与加密相反）
- 移位密码的密钥是 k
- 密钥有多少个？（26）
- **密钥空间很小** 穷举攻击可以在很短时间内破译

简单代换密码 :使用一张固定的代换表明文字母到密文字母的对应关系不一定像移位密码那样有规律

- 简单代换密码的 **密钥空间很大**

  26 个字母的不同排列形成不同的密钥，共有 $26!=4\times10^{26}$ 个

穷举攻击在计算上是不可行的，即使 1 微秒试一个密钥，遍历全部密钥需要 10^{13} 年!!!! 虽然密钥空间大但简单代换密码并不安全

频率分析：简单代换密码的终结者

维吉尼亚密码 多表代换密码的典型代表

密钥空间与密钥长度 m 有关

共有 26^m 个密钥，即使 m 很小，穷举攻击也不太现实

假设 m=5，密钥空间超过 1.1×10^7 ，已超出手工计算进行穷举攻击的能力范围。

但这并不表示维吉尼亚密码无法用手工破译

维吉尼亚密码的分析

- 在维吉尼亚密码的分析中，要先确定密钥长度，再确定具体密钥
- 确定密钥长度的常用方法有两种：

Kasiski 测试法

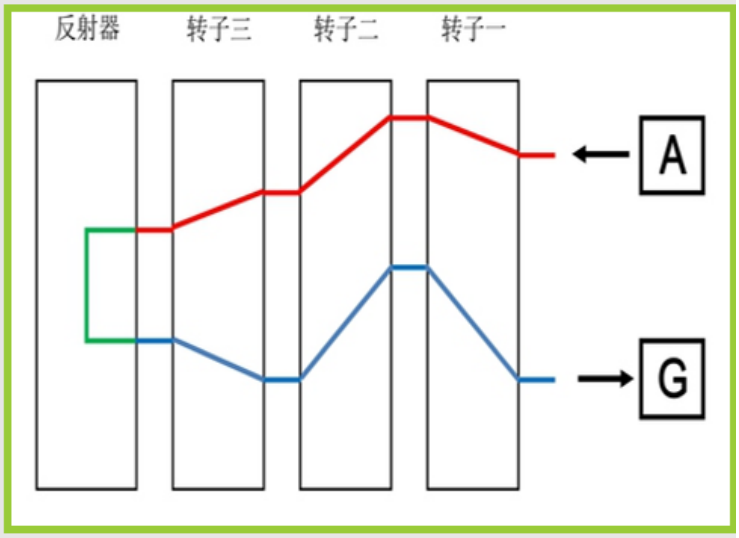
重合指数法

维吉尼亚密码的特点：

- 用给定的 m 个移位代换表周期性地对明文字母加密；
- **当两个相同的明文段间隔的字母数为 m 或 m 的整数倍时，将加密成相同的密文段；**
- 假设密文中出现两个相同的段落，对应的明文段不一定相同，但相同的可能性很大。

Enigma　Enigma的结构——反射器

- 反射器的作用
  - 加密与解密的过程完全相同
  - 明文字母与对应的密文字母不会相同



- 置换密码、单表代换密码、维吉尼亚密码等对已知明文攻击都是非常脆弱的。
- 即使用唯密文攻击，大多数古典密码体制都容易被攻破，因为**它们不能很好地隐藏明文消息的统计特征**。
- 虽然有些古典密码（如 Zodiac-340 密码）至今未被破译，但这并不表示古典密码的设计理念就是科学的。事实上，古典密码时期的设计者们，往往凭借经验和直觉设计密码，这显然是不靠谱的。
- **只有采用科学的理念，才能设计出安全的密码体制**。

练习题

1. 恺撒密码属于(　B　)

A.置换密码　B.移位密码　C.转轮机密码　D.以上都不对

2. 维吉尼亚密码属于(　D　)

A.置换密码　B.移位密码　C.转轮机密码　D.多表代换密码

3. 周期置换密码中，明文分组长度是m，密钥空间大小为(　A　)

A. m!　　B. 2^m　　C. m　　D. m^2

4. 多表代换密码中，采用字母为密钥，且密钥长度是m，密钥空间大小为（ B ）

A. $(26^m)!$　　B. 26^m　　C. m!　　D. m^{26}