**信息安全**

1. 古典密码学

密码需求：保密性、完整性、可用性（安全需求、安全服务）

羊皮传书（transposition）、藏头诗【线代称“隐写术”，包含冗余信息，不符合对称秘钥密码模型】、Caesar Cipher（substitution）

Terminologies:

**对称秘钥密码模型**（Symmetric Cipher Model）五要素：

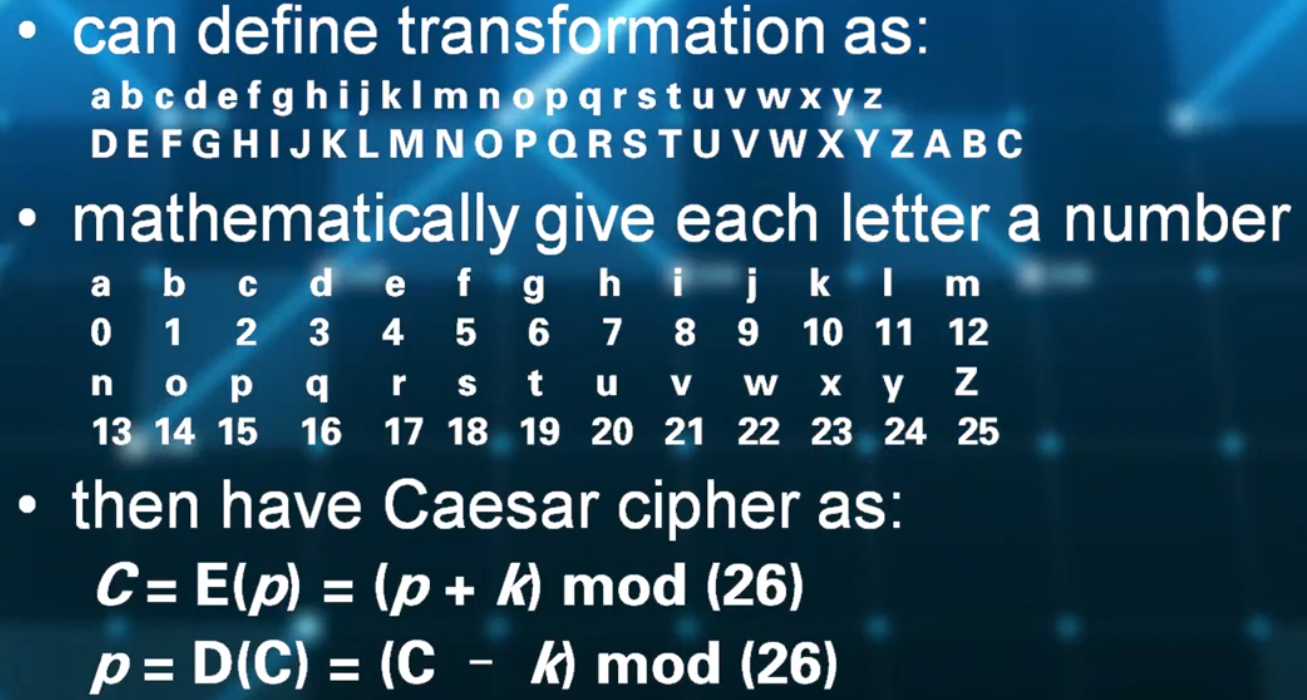
plaintext – the original message

ciphertext – the coded message

key – info used in cipher known only to sender/receiver

encipher/encrypt – converting plaintext to ciphertext

decipher/decrypt – recovering plaintext from ciphertext



1. 密码学的三个基础假设

要求：秘钥要在通讯开始前带外传递；明文需要保密，秘钥需要保密，秘文需要公开【密码要完全寓于秘钥，并不等于算法一定要公开。民用和商用加密算法通常公开，军用通常不公开】；易用性

现代密码：DES算法、RSA算法

密码学分类：密码编码学cryptography、密码分析学cryptanalysis、密码学cryptology

按明文变成密文的方法：替代substitution、置换transposition、乘积Product（很多轮的置换和替代）

按照秘钥：

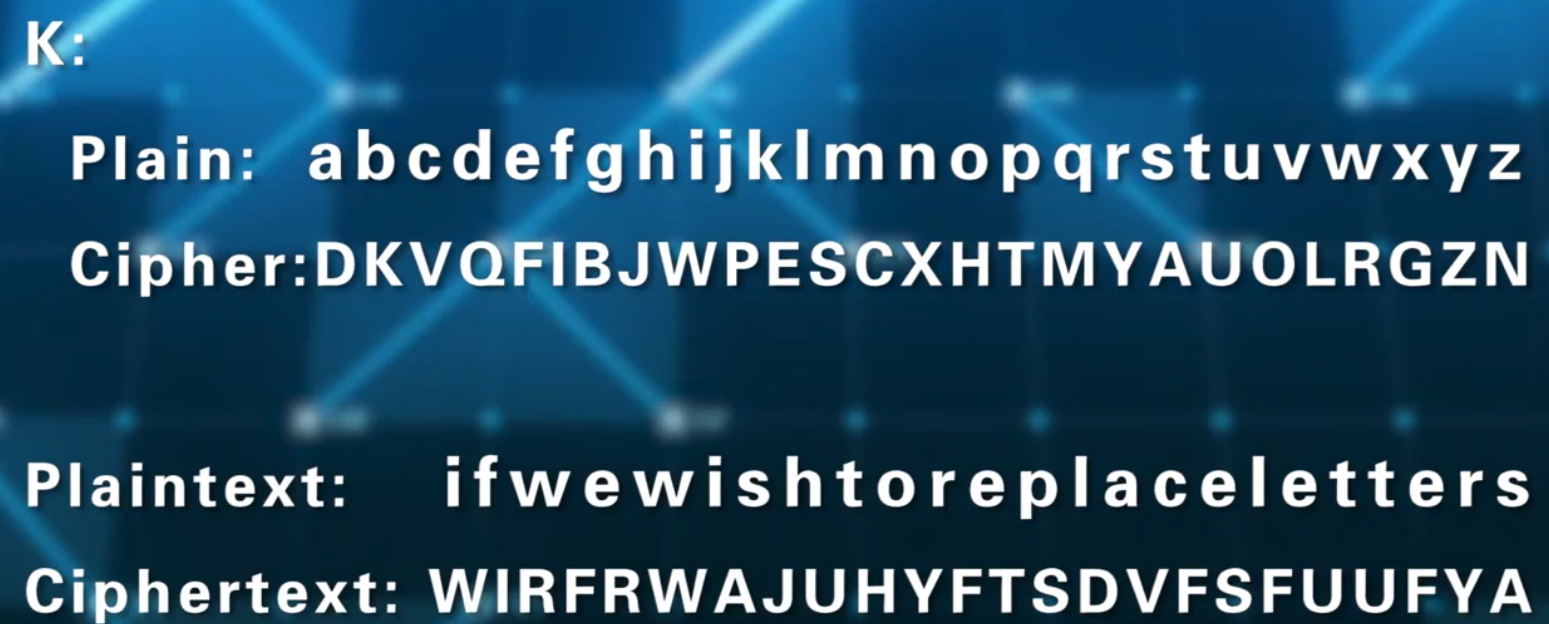
对称秘钥密码系统（Symmetric, single-key, secret-key, conventional encryption）：Both sender and receiver use the same key

公开秘钥密码系统（Asymmetric, two-key, public-key encryption）：the sender and receiver each uses a different key

按照明文被处理的方式：分组密码Block cipher：明文在处理前先对明文进行分组，然后以组为单位进行替换和置换【主要用于民用和商用密码系统，速度稍微慢一点】、流密码Stream cipher

1. Caesar Cipher和单字母表密码

* Caesar Cipher秘钥个数一共25个，所以可以穷举攻击【原因是秘钥数量少，明文是有冗余信息的，如果明文是随机数，则无法解密】
* **Monoalphabetic Cipher**：增加凯撒密码秘钥数量（26!）



可以通过词频分析（从高到低猜测），攻击者不需要进行穷举。

* 提高单字母表密码的安全性

**多对一**：先对明文进行分组，一次加密一组明文。

如：**Playfair密码**，5\*5的矩阵，先选一个英文单词作为秘钥，一行写五个，然后将剩余的字母按顺序写下，规定i/j不做区分。明文两个字母一组，两个字母相同或者最后一组不够则进行padding填充。【可以通过构建26\*26的词频分析表做攻击。】

**一对多**：明文一个字母在密文有个字母进行替代。

如：**维吉尼亚密码**，多字母表密码，26个Caesar密码表。【攻击者如果发现了秘钥的长度就可以按照单字母表的方式进行攻击，秘钥长度可以通过找相同的字符串去试】

**autokey cipher**：先由一个初始秘钥加密刚开始的明文，然后将密文发送给接收方，接收方解密得到初始明文，发送方通过初始明文作为秘钥来加密后面的明文。【秘钥文本和明文字母频率上的统计规律是一致的，具有相关性。比如字母e加密e的概率高于其他情况】（按照该算法好的秘钥应该和明文一样长，同时秘钥和明文没有统计上的联系）

**vernam密码**：理论的标杆，用物理界随机的秘钥加密明文。

* unconditional security无条件安全：no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext（实际不存在，理论思想）

computational security计算式安全：有限时间有限资源的情况下不能被解密，攻击者成本远大于密码使用的成本。

1. 对称式秘钥密码的理论标杆

One-Time Pad：一次一密，**秘钥和明文一样长，且秘钥真正随机**，该密码无条件安全。但是需要通信双方能够事先共享一个纯粹的秘钥序列，实用性较差。香农于1949年证明了该加密算法的无条件安全性。

抑或运算的性质：

1. 简单置换密码

**Rail Fence密码**（羊皮传书本质上就是一种Rail Fence密码）、**行置换密码**：都有深度的说法，不够的进行padding

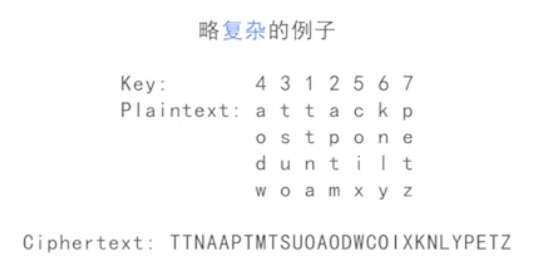


Figure 1行置换密码

乘积密码Product Cipher：多次替代、多次置换。通向现代密码技术的基本道路。

1. 转子机Rotor Machines

转子机是一种多轮替代的乘积密码，古典密码的高峰。3轮转子字母表有

比如：Enigma-Rotors

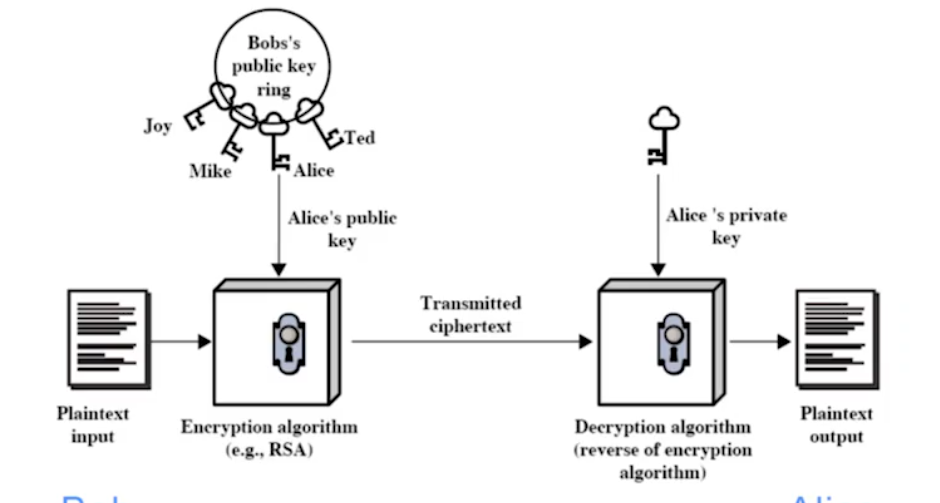
1. 古典隐写术：藏头诗、隐形墨水。特点：大量冗余信息隐藏了相对较少的信息量。现代信息隐藏技术有伪装式保密通信【图片像素点的最低位隐藏信息，相比加密更加隐蔽，但是需要更大的空间浪费】、数字水印【一种基本的数字版权标记手段】。
2. 公开秘钥密码（Public Key Cryptography）
3. 对称秘钥密码的秘钥交换问题：通信开始前需要实现秘钥的共享

对称的、单秘钥的、秘密秘钥的、传统密码技术

使用扩散、扰乱、替代、置换、乘积等设计加密算法

1. 公钥密码模型的提出（**非对称密码模型**）

每个人需要有两个秘钥：Public Key公钥公开，Private Key私钥保密



攻击者得到Alice的公钥，密文，加密算法依旧得不到明文。

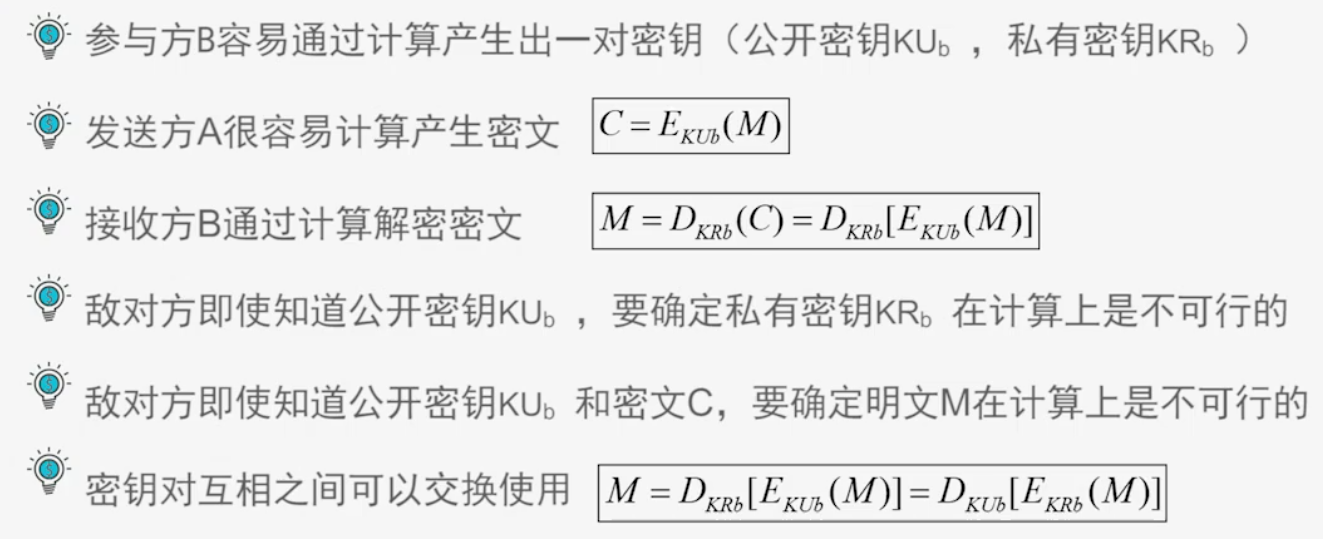
通过数论函数精心构造。

公开秘钥密码的主要缺点是加密和解密速度相对较慢。可以通过公开秘钥密码模型实现秘钥交换，然后通过对称秘钥密码模型实现通信。

1. 设计秘钥密码要求

明文、公开秘钥PU/KU、私有秘钥KR/PR、加密算法、密文、解密算法

理论基础：基于计算复杂性。让加密和解密者的加密和解密是多项式时间复杂度的，让敌方求解目前仍未找到多项式时间算法的NP完全问题。



**秘钥互相之间可以交换使用**，用公钥加密的可以用私钥解密，用私钥加密的可以用公钥解密。

1. 数字签名

用公开秘钥加密，私有秘钥解密可以实现保密通信；用私有秘钥加密，用公开秘钥解密可以实现数字签名。

签名：可认证、抗抵赖。

【用公开秘钥能提供的服务：保密通信，秘钥交换，数字签名。但并不是所有公开秘钥算法都能实现以上三个安全服务。】



1. 公开秘钥算法基本要求

加密与解密由不同的秘钥完成；

知道加密算法，从加密秘钥得到解密秘钥在计算上是不可行的；

两个秘钥中任何一个都可以作为加密而另一个作为解密。

1. 公开密钥密码算法基础

**单向函数**：对于一个函数，如果对于其定义域上的任意，都容易计算，同时，对于其值域中几乎所有的取值，计算其逆函数都是不可行的，则函数被称为单向函数。

**可以提供单向函数的三个数学难题**：

大整数分解问题（IFP）

离散对数问题（DLP）

椭圆曲线离散对数问题（ECDLP）

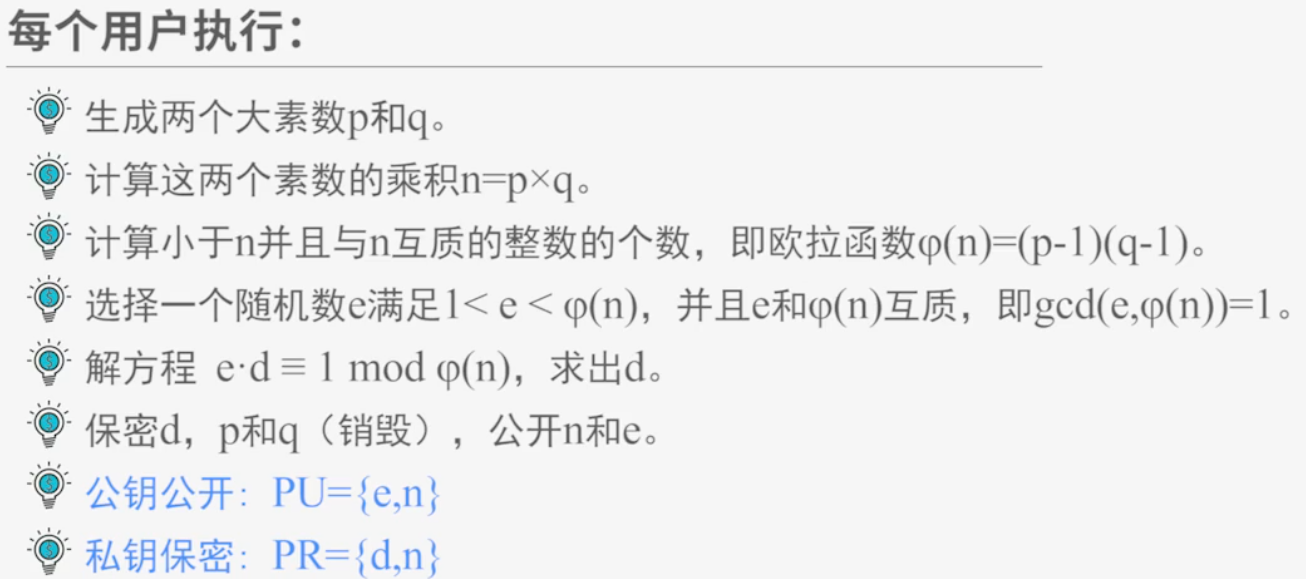
**单向陷门函数**：对于一个单向函数，如果其逆函数在已知某些辅助信息的情况下容易求解得出，则称该单向函数为单向陷门函数。

构造公钥密码系统的关键是如何在求解某个单向函数的逆函数的NP完全问题中设置合理的“陷门”。



1. RSA算法
2. 秘钥生成

是一个分组加密方法。数论理论：求得两个大素数的乘积是容易的，但要分解一个合数为两个大素数的乘积，在计算上几乎是不可行的。



p、q至少是100位以上10进制素数。

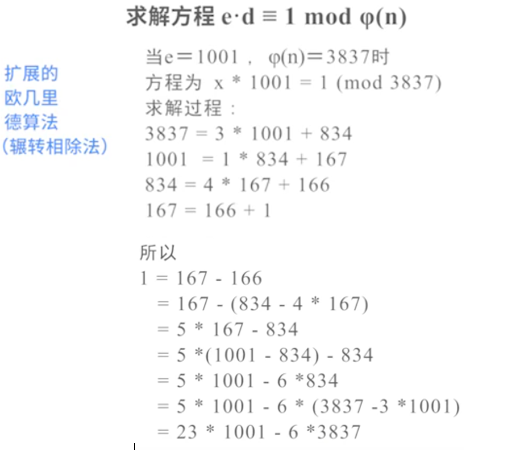
如何得到足够大的随机素数：

实际应用中采用的方法是，先产生一个足够的奇数随机数，然后通过采用一个概率多项式时间算法来检测随机数是否为素数（即是否具有素性）。

常用的两个素性测试算法：Solovay-Strassen素性测试、Miller-Rabin素性测试（通常采用该方法，经过30次迭代，该数不是素数的可能性已经很小）。

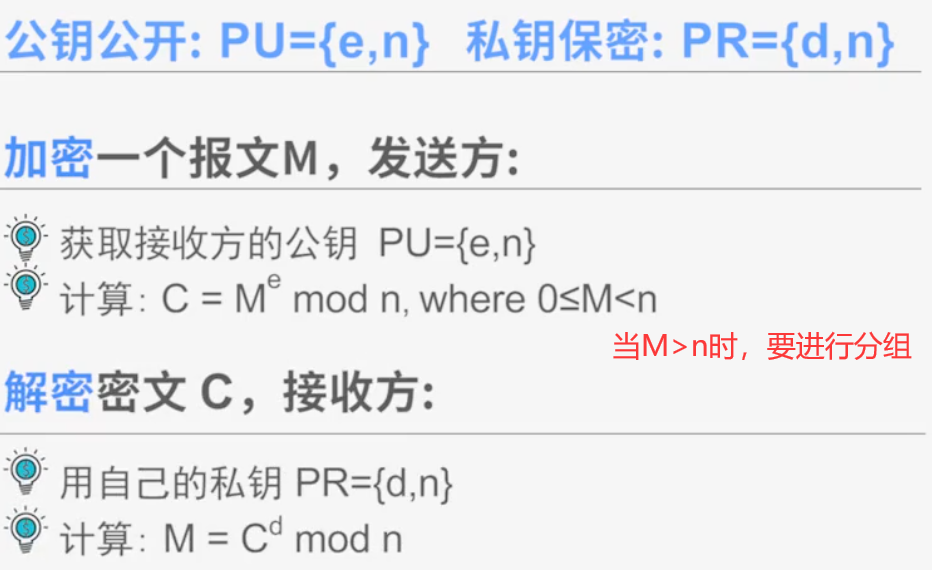
n又称为系统的模。

称为n的欧拉函数，数学意义是比n小和n互质的数的个数。显然是一个合数，是一个偶数。【通常e选取：是通过选择质数去除，如果有余数，则选取该e】

求d：【辗转相除法】 

1. 加解密算法

加解密算法一致，意味着硬件或软件设计一套就行。



证明：

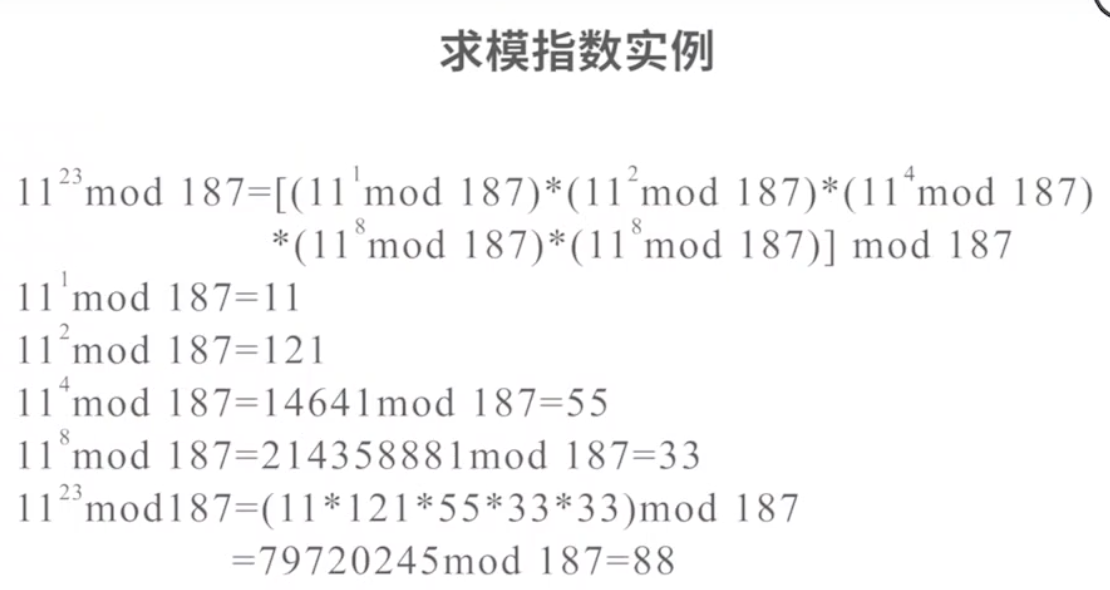
模指数运算简化：

在RSA密码体制中，加密解密运算都是模指数运算，计算量较大。

可以通过次模乘来实现计算，然而，如果e非常大，其效率还是很低。

可以使用**平方-乘算法**把计算所需的模次数降低。

模运算性质：

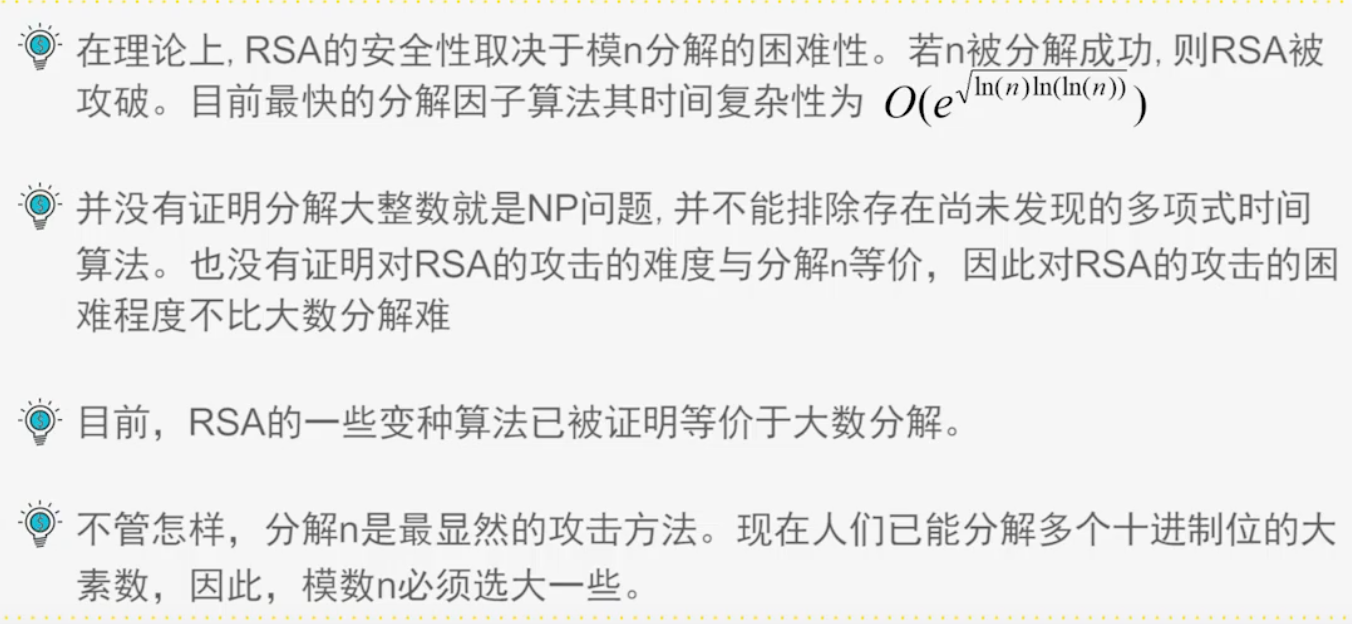


**注意：**

a. RSA加密时，明文以分组的方式加密：每一个分组的比特数应该小于比特，即M<n。

b. 选取的素数p和q要足够大，从而乘积n足够大，在事先不知道p和q的情况下分解n是计算上不可行的。

1. 安全性讨论



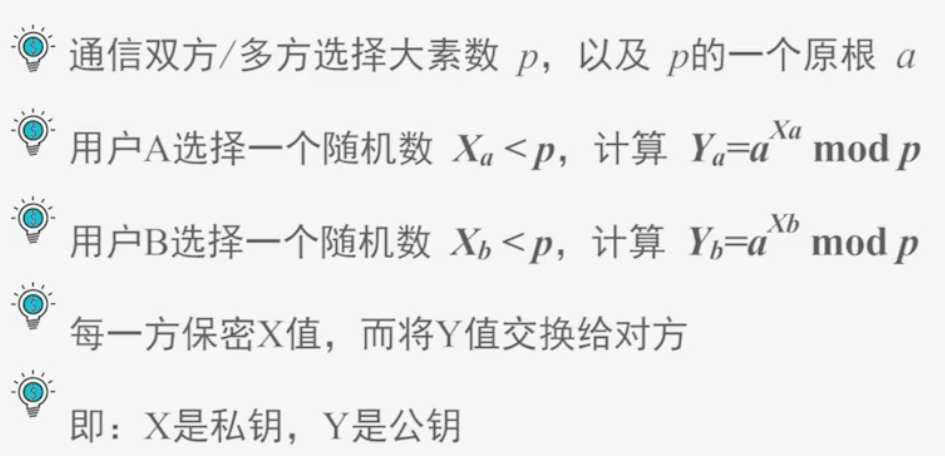
速度问题：由于都是大数计算，RSA最快的情况也比DES慢很多倍，无论是软件还是硬件实现，速度一直是RSA的缺陷，一般来说只用于少量数据加密。

1. Diffie-Hellman秘钥交换算法
2. 是第一个公钥方案。使用在一些常用的安全协议或产品（如SSH、IPSec）。

算法不能直接用于有大量数据传输的保密通信，只允许两个用户可以安全的建立一个共享的秘密信息，用于后续的通讯过程。该秘密信息仅为两个参与者知道。

算法的安全性依赖于**有限域上计算离散对数的问题**。

1. 算法



p、a为通信参与者都知道的秘密。

1. 秘钥交换

双方获得一个共享秘钥

对于用户A，可以通过计算

对于用户B，可以通过计算

对于攻击者要知道K，需要求解离散对数问题。（攻击者知道，需得出的解）

实际使用过程中，素数p以及p的原根a可由乙方选择后发给对方。

1. 报文鉴别与哈希函数
2. 安全需求/安全服务

保密性（Confidentiality）【可指数据保密和系统保密(访问控制)】、完整性（Integrity）【防止修改，如计算机病毒破坏了系统的完整性，因为他要通过篡改系统文件使自己在加载系统文件时得以被加载，可以通过报文鉴别密码和哈希函数实现保密】、可用性（Availability）【在任何用户访问请求总应该被允许，比如拒绝服务攻击（Dos、DDos）】、可认证（Authentication）、抗抵赖/抗否认（Non-repudiation）