第二章 密码学基础
第二节 密码学基本概念

主讲人：李建华 张全海
网络空间安全技术研究院

2024 年 11 月

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

密码体制基本概念

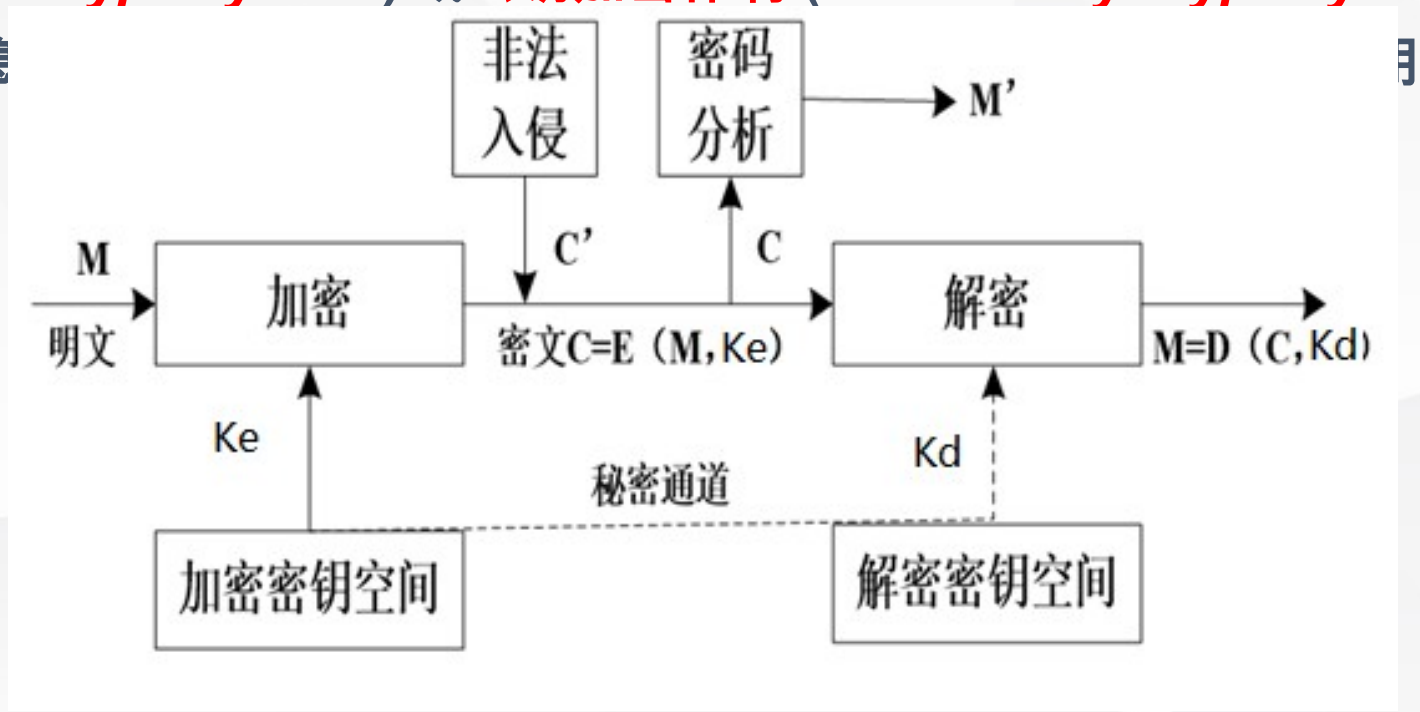
- **保密学（密码学 Cryptology）：** 是研究信息系统安全保密（秘密通信和破译密码的方法）的一门科学．
- **密码编码学（Cryptography）：** 主要研究对信息进行编码，实现对信息的隐蔽．
- **密码分析学（Cryptanalytics）：** 主要研究加密消息的破译或消息的伪造，恢复被隐藏的信息的本来面目，即分析破译密码．
- **密码系统：** 包含明文字母空间、密文字母空间、密钥空间和算法，两个基本单元是算法和密钥。
- **密码体制：** 一对用于数据加密和解密的数据变换。

密码体制基本概念

- **明文**：需要秘密传送的可以读得懂的消息。**明文消息空间 M** ：可能的明文字母串集合。
- **密文**：明文经过密码变换后的不可读消息。**密文消息空间 C** ： 可能的密文字母串集合。
- **加密**：由明文到密文的数学变换。
- **解密**：从密文恢复出明文的数学变换。
- **加密算法**：对明文进行加密时采用的一组规则。
- **解密算法**：对密文进行解密时采用的一组规则。
- **密钥**：加密和解密时使用的一组秘密信息。**加密密钥空间 K** ： 可能的加密密钥集合；**解密密钥空间 K'** ： 可能的解密密钥集合
- 加密算法 E ： M X K → C ；解密算法 D ： C X K' → M

密码体制基本概念

- 若 $k_e = k_d$ ，则加密算法称为**单钥加密体制**（ *One-key Cryptosystem* ）（**对称加密体制**（ *Symmetric Cryptosystem* ）或**秘密密钥加密体制**（ *Scret-key Cryptosystem*）、传统密钥密码体制；
- 若 $k_e \neq k_d$ ，则加密算法称为**双钥加密体制** (*Two-key Cryptosystem* ）（非对称加密体制 (*Asymmetric Cryptosystem*) 或**公钥加密体制**（ *Public -key Cryptosystem* ）（特点：实现多个用户加密的消息，只有一个用户可以解读 -- **数字签名**；**密钥管理**）。



密码体制基本概念

- 对称加密算法采用了对称密码编码技术，它的特点是文件加密和解密使用相同的密钥或或相近，由其中一个很容易得出另一个，即加密密钥也可以用作解密密钥，这种方法在密码学中叫做对称加密算法，对称加密算法使用起来简单快捷，密钥较短，且破译困难。如： DES 、 IDEA 、 TDEA （即 3DES ）、 AES
  - 在对称密钥密码算法中，加密和解密双方使用的是相同的密钥，所以，在**双方进行保密通信之前必须持有相同的密钥**。若有 N 个人要相互进行保密通信，网络中就会有（ N-1) 个密钥，这为**密钥的管理和更新都带来了极大地不便**，这是对称算法的一大缺点。
- 非对称加密算法需要两个密钥：**公开密钥（ publickey ）和私有密钥（ privatekey ）**。公开密钥与私有密钥是一对，如果用**公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密**。
  - 加密算法可以把**加密密钥和算法公开**，所以任何人都可用之来加密要传送的明文信息。但只有拥有解密密钥的人才能将传送过来的已经加了密的消息解密，还原原信息。

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

密码分析与密码安全性

- 密钥分析的实质就是在攻击者不知道密钥的情 况下，对所截获的密文或明 - 密文对采用各种不 同的密码分析方法试图恢复出明文或密钥。密 码分析在外交、军事、公安、商业等方面都具 有重要作用，也是研究历史、考古、古语言学 和古乐理论的重要手段之一。
  - 密码设计和密码分析是共生的、又是互逆的，两者密切相关，但追求的目标相反；
  - 密码设计是利用数学来构造密码；密码分析除了依靠数学、工程背景、语言学等知识外，还要靠经验、统计、测试、眼力、直觉判断能力等，有时还靠点运气。
  - 密码分析过程通常包括分析（统计截获报文材料）、假设、推断和证实等步骤。

- 密码的安全性
  - 无条件安全（ Unconditionally secure ）：无论破译者有多少密文，他也无法解出对应的明文，即使他解出了，他也无法验证结果的正确性；具有无限计算资源（诸如时间、空间、资金和设备等）的密码分析者也无法破译某个密码系统
  - 计算上安全（ Computationally secure ）：理论上可破译，即只要给攻击者足够的时间和存储资源， 都是可以破译的，但是实际运用时
    - ✓ 破译的代价超出信息本身的价值
    - ✓ 破译的时间超出了信息的有用寿命

密码分析

- 假设破译者是**在已知密码体制**的前提下来破译加密者使用的密钥。最常见的破解类型如下：
  - **唯密文攻击**：破译者具有密文串 y 和算法，试图获得明文及密钥；
    - 只知道密码体制及算法与一些密文
    - 最常见的一种密码分析类型，也是难度最大的一种分析方法
  - **已知明文攻击**：破译者具有明文串 x 和相应的密文串 y 和加密算法，推算出明文及密钥；
    - 知道一些明文 / 密文对、相当数量的密文，
    - 利用已知的明文密文对进行攻击，如一些固定的关键字，固定的格式及约定的文字
  - **选择明文攻击**：破译者具备选择明文串 x 并获得相应的密文串 y ，推算出密钥和算法；
    - 能够选择明文并得到相应的密文（如通过欺骗的方式获得）
    - 常用于破译采用公开密钥密码系统加密的信息内容
  - **选择密文攻击**：破译者具备选择密文串 y 并获得相应的明文 x ，试图获得明文及密钥；
    - 知道密码体制
    - 能够选择密文并得到对应的明文
    - 基于公开密钥密码系统的数字签名易受此类型攻击
  - **＊选择文本攻击**：破译者具有密文串 y 、加密算法，选择的明文及相应的密文，选择的密文及相应的明文

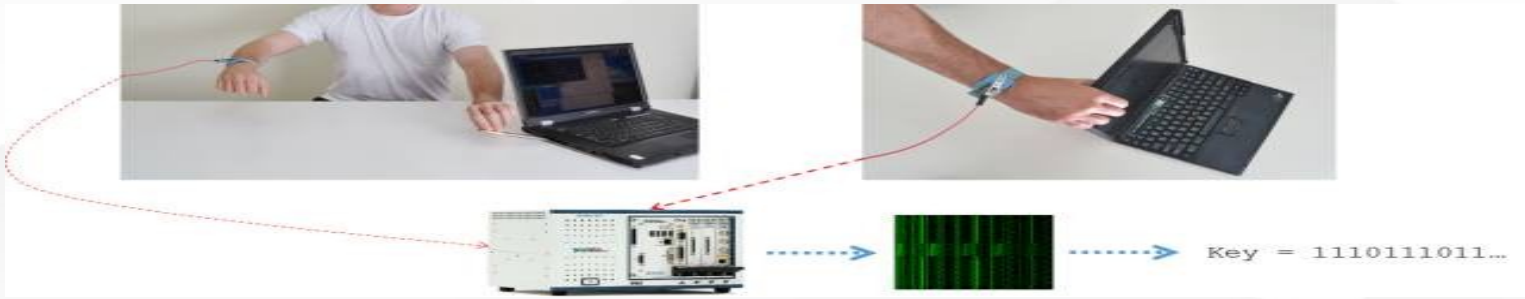
这一切的目的在于破译出密钥或密文

密码分析方法

- 密码分析方法：穷举攻击法、数学攻击法、物理攻击法
  - 原则上，只要攻击者有足够多的计算时间和存储容量，穷举法总是可以成功的。
  - 对于基于数学难题的密码系统，数学分析法是一种重要的破解手段。
  - 攻击者利用密码系统或密码芯片的物理特性，通过对系统或芯片运行过程中所产生的一些物理量进行物理和数学分析。
- 穷举攻击法（强力攻击法）
  - 穷尽密钥搜索攻击（完全试凑法）；
- 数学攻击方法
  - 差分密码分析：通过分析明文对的差值对密文对的差值的影响来恢复某些密钥比特．（针对分组密码）
  - 确定性分析法 -- 线性密码分析：本质上是一种已知明文攻击方法，通过寻找一个给定密码算法的有效的线性近似表达式来破译密码系统
  - 确定性分析法 -- 插值攻击方法：使用一个代数函数来代表一个 S-Box ，此函数可以用已知明文攻击法取得样本点，再用拉格朗日插值法产生。这个代数函数可能是在有限体上的二次函数、多项式函数或有理函数。
  - 统计分析法：利用明文的已知统计规律进行破译的方法。
- 物理攻击方法
  - 侧信道攻击（能够直接获取密码算法运算过程中的中间值信息；能够分段恢复较长的密钥）

侧信道攻击

- 通常，密码算法（或密码方案）在实际应用中都会实现在具体的硬件平台上，形成密码模块、密码芯片、密码系统等，从而完成所需的密码功能，用于满足特定的信息安全需求。如果我们能够有效检测和测量这种“时间”和“能量”的变化，就能够推断出所执行的操作（或数据），即推断出密码实现运行过程中的操作（或数据），从而能够进行密码破解。
- 密码系统的安全性不仅取决于密码算法本身的数学安全性，更严重依赖于密码实现的物理安全性。
- 侧信道攻击（ Side Channel Attack ）又称侧信道密码分析，由美国密码学家 P.C. Kocher 于上世纪九十年代末期提出，是一种针对密码实现（包括密码芯片、密码模块、密码系统等）的物理攻击方法。这种攻击方法的本质上是利用密码实现在执行密码相关操作的过程中产生的侧信息来恢复出密码实现中所使用的密钥。其中，这里的侧信息（ Side Channel Information ）指除了攻击者通过除主通信信道以外的途径获取到的关于密码实现运行状态相关的信息，典型的侧信息包括密码实现运行过程中的能量消耗、电磁辐射、运行时间等信息。
  - 侧信道攻击主要面向密码实现的物理安全性，采用能量分析攻击、电磁分析攻击、计时攻击、缓存攻击、故障攻击等一系列方法对其实现安全性进行分析
  - 2014 年 8 月，以色列特拉维夫大学的计算机安全专家 Eran Tromer 等公布了一种通过用手触碰笔记本电脑的外壳就能得到这台计算机上存储数据的安全密钥的方法，该团队测试了广泛使用的高安全标准的解密算法，并成功恢复了 4096 位 RSA 密钥和 3072 位 ElGamal 密钥



上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

密码学基本数学知识

- 整数分解
- 模运算
- 有限域
- 欧几里得算法
- 中国剩余定理
- 椭圆曲线

整数分解

- 整数分解又称为**素因数分解**，即任意一个大于 1 的自然数都 可以写成**素数乘积**的形式。
- $N = P_1^{a1} P_2^{a2} P_3^{a3} \cdots P_n^{an}$，其中 $P_1 < P_2 < P_3 \cdots < P_n$

模运算

- 模运算即求余运算。
  - 给定一个正整数n，任意一个整数a，一定存在等式：$a = qn + r$，$0 \le r < n, q = [a/n]$
- 模运算类型
  - **取模运算：** $a \bmod n$
  - **模 n 加法：** $(a + b) \bmod n$
  - **模 n 减法：** $(a - b) \bmod n$
  - **模 n 乘法：** $(a \times b) \bmod n$
  - **求逆运算：若存在$ab = 1 \bmod n$，则 a 、 b 互为逆元**
- 模运算的基本运算
  - **若$a \bmod n = b \bmod n$，则a和b模n同余，记作$a \equiv b \bmod n$**
  - $(a + b) \bmod n = (a \bmod n + b \bmod n) \bmod n$
  - $(a - b) \bmod n = (a \bmod n - b \bmod n) \bmod n$
  - $(a \times b) \bmod n = (a \bmod n \times b \bmod n) \bmod n$
  - **模指数运算：$a^m \bmod n$**

模运算举例

- 设$Z_6=\{0,1,2,3,4,5\}$，计算Z_6上的模乘运算

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

有限域

设G是一个集合，$*$是G上的运算，$\langle G,* \rangle$是一个代数结构，如果$*$满足下述条件，则称$\langle G,* \rangle$为群：

封闭性：若$\forall a,b \in G$，有$a*b \in G$；

结合律：若$\forall a,b,c \in G$，有$(ab)c = a(bc)$；

单位元：若$\exists e \in G$，使得$\forall a \in G$有$ea = ae = a$；

逆　元：若$\forall a \in G$，存在元素a^{-1}使得$a*a^{-1} = a^{-1}*a = e$。

若群G上的运算还满足交换律，即$\forall a,b \in G$，有$ab = ba$，则称群G为交换群或Abel群。

$G = \langle a \rangle = \{a^0 = e, a, a^2, \cdots\}$称为由$a$生成的循环群，a称为生成元。

整数集 Z 对加法运算构成交换群，对乘法运算不构成群。

有限域

- 有限域是指元素个数有限的域，又被称为 Galois 域；
  - 定义了加法和乘法
  - 集合内的元素经过加法和乘法计算，结果仍然在集合内
  - 计算符合交换率、结合率、分配率
  - 加法和乘法有单位元素（所有的集合内的值都有对应的负数，所有集合内非零值都有倒数）
- 有限域的元素个数一定是某个素数的幂，GF（p^n）。

域的定义

设$\langle F,+,=\rangle$是一个代数结构，+和=满足下述条件，
则称$\langle F,+,=\rangle$为域：
$\langle F,+\rangle$ 是交换群；
$\langle F\backslash\{0\},=\rangle$ 是交换群；
分配律：$\forall a,b,c\in F$，有 $a(b+c)=ab+ac,\ (b+c)a=ba+ca$。

欧几里得算法

- **欧几里得算法是一种求两个整数最大公因子的快速算法；**
- **设是 a 和 b 两个任意正整数， $\gcd(a, b)$ 为它们的最大公因子；**
- **$\gcd(a, b) = \gcd(b, a \bmod b)$**

- 设a，b 是两个任意正整数，则$s_n a + t_n b = \gcd(a, b)$，其中$s_j$，$t_j$ $(0 \le j \le n)$ 定义为，其中q_j是不完全商。

$$\begin{cases} s_0 = 1, s_1 = 0, s_j = s_{j-2} - q_{j-1} s_{j-1} \\ t_0 = 0, t_1 = 1, t_j = t_{j-2} - q_{j-1} t_{j-1} \end{cases}$$
$$j = 2, 3, \cdots, n$$

- 若a和b互素，则有$s_n a + t_n b = \gcd(a, b) = 1$ ， t_n为b的乘法逆元
- *(77,33)=(33,77mod 33)=(33,11)=(11,0)=11; (124,48)=(48,124 mod 48)=(48,28)=(28,48 mod 28)=(28,20)=(20,28 mod 20)=(20,8)....=(4,0)=4*

中国剩余定理

假设 $m_1, m_2, \cdots, m_k$ 是两两互素的正整数，$M = \prod_{i=1}^{k} m_i$

则一次同余方程组
$$\begin{cases} x \equiv a_1 (mod\ m_1) \\ x \equiv a_2 (mod\ m_2) \\ \vdots \\ x \equiv a_k (mod\ m_k) \end{cases}$$

对模M有唯一解：

$$x \equiv \left(\frac{M}{m_1} e_1 a_1 + \frac{M}{m_2} e_2 a_2 + \cdots + \frac{M}{m_K} e_K a_K \right) (mod\ M)$$

其中 e_i 满足 $\frac{M}{m_i} e_i \equiv 1 (mod\ m_i)\ (i = 1, 2, \cdots, k)$

- 孙子定理是中国古代求解一次同余式组（见同余）的方法。是数论中一个重要定理。又称中国剩余定理。一元线性同余方程组问题最早可见于中国南北朝时期（公元 5 世纪）的数学著作《孙子算经》卷下第二十六题，叫做“物不知数”问题，原文如下：
- 有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何？即，一个整数除以三余二，除以五余三，除以七余二，求这个整数。《孙子算经》中首次提到了同余方程组问题，以及以上具体问题的解法。

- 宋朝数学家秦九韶于 1247 年《数书九章》卷一、二《大衍类》对“物不知数”问题做出了完整系统的解答。明朝数学家程大位将解法编成易于上口的《孙子歌诀》：三人同行七十稀，五树梅花廿一支，七子团圆正半月，除百零五使得知
- 这个歌诀给出了模数为 3 、 5 、 7 时候的同余方程的秦九韶解法。意思是：将除以 3 得到的余数乘以 70 ，将除以 5 得到的余数乘以 21 ，将除以 7 得到的余数乘以 15 ，全部加起来后除以 105 （或者 105 的倍数），得到的余数就是答案。比如说在以上的物不知数问题里面，按歌诀求出的结果就是 23 。

实数域上椭圆曲线

- 实数域上的椭圆曲线可以定义为满足方程： $y^2=x^3+ax+b$ 的所有点 (x, y) 的集合

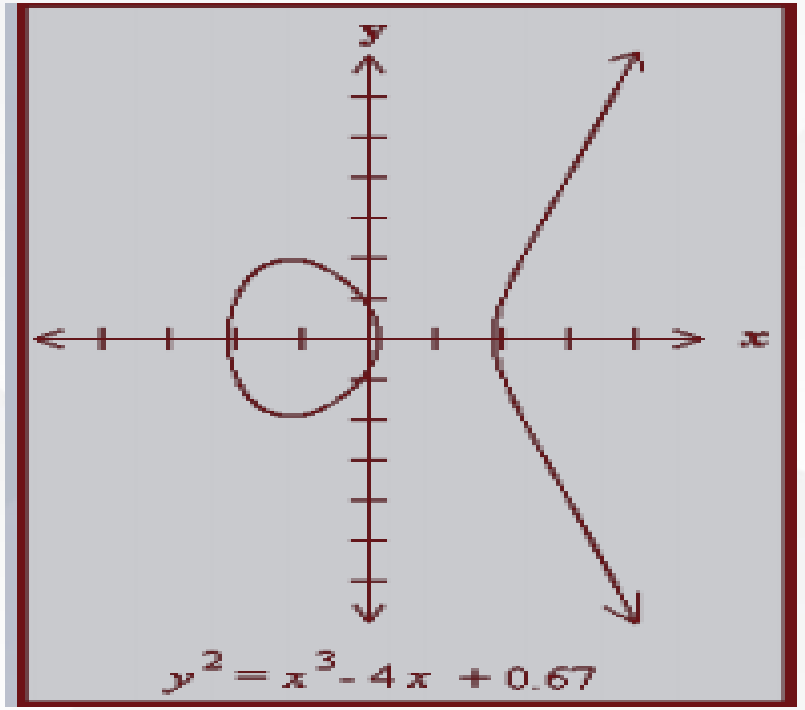
  注意：椭圆曲线并不是椭圆，只因为该方程与计算椭圆周长的方程相似

  $$y^2+axy+by=x^3+cx^2+dx+e$$

- 可以证明：如果 x3+ax+b 没有重复因子，或者满足 4a3 + 27b2≠0 ，那么椭圆曲线上的点集 E(a, b) 可构成一个 Abel 群

- 椭圆曲线群包括所有曲线上的点以及一个特殊的点 ，我们称其为无限远点 O

（群定义：若在集合上定义的加法运算是封闭的 ，且满足交换律和结合律，我们就称这个集合为群）



实数域上椭圆曲线

- 有限域 G F(p) 上的椭圆曲线 $y^2=x^3+ax+b$ ，其点集 (x, y) 构成有限域上的 Abel 群，记为 $E_p(a, b)$ 。条件为：
- $4a^3 + 27b^2 \neq 0 \bmod p$
- 设 $P=(x_1, y_1)$, $Q=(x_2, y_2)$, $P+Q=(x_3, y_3)$

当 $P \neq Q$ 时：

$$\lambda = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) mod\ p$$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod p$$

$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod p$$

当 $P = Q$ 时：

$$\lambda = \left(\frac{3{x_1}^2 + a}{2y_1}\right) \bmod p$$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod p$$

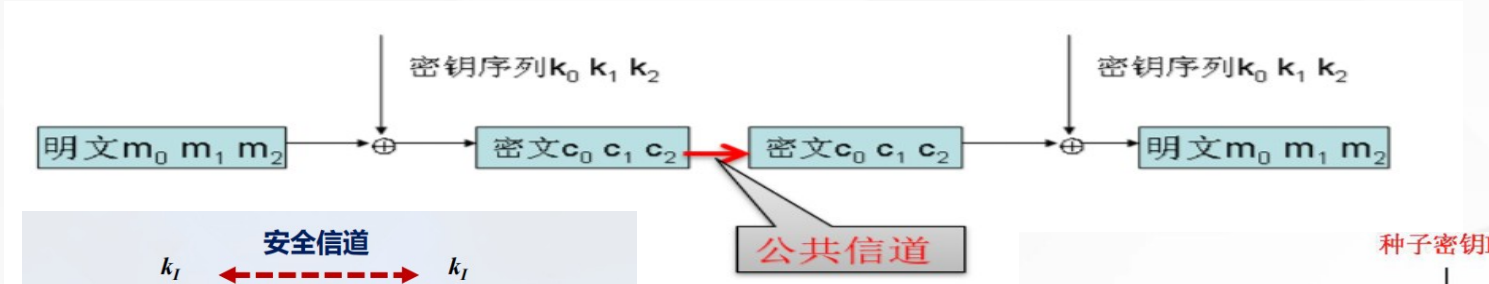
$$y_3 = (\lambda(x_1 - x_3) - y_1) \bmod p$$

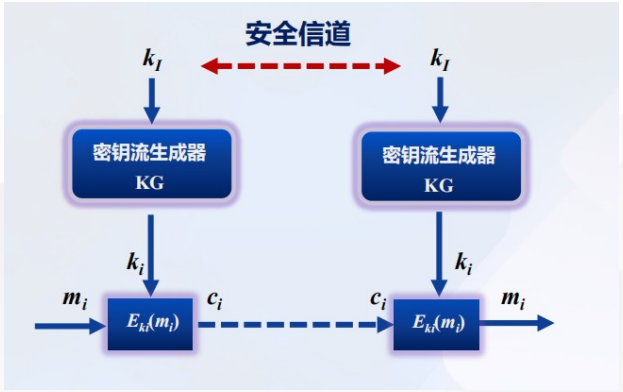
上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

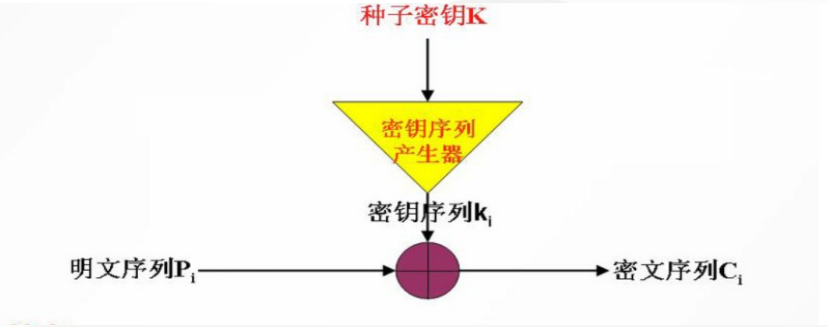
目 录

序列密码原理

- 序列密码也成为流密码
- 明文 $m=m_1,m_2,.....m_l$ 将明文字母替换成其他的字母、数字和符号，伪随机序列 $k=k_1,k_2,.....k_l$, 密文 $c_i= E_{k_i}(m_i)$， 解密过程与加密过程相同且互逆，序列密码的安全性完全依赖于伪随机数的强度
- 数学表达：由种子密钥通过密钥流发生器得到的密钥流为： $K=k_1k_2.....k_n$, 则加密变换为：$C=c_1c_2.....c_n$ ，其中 $c_i=m_i \oplus k_i$ ，$(i=1,2,.....,n)$, 其中 m,k,c 是 0 ， 1 序列，⊕表示模 2 加法（异或）。





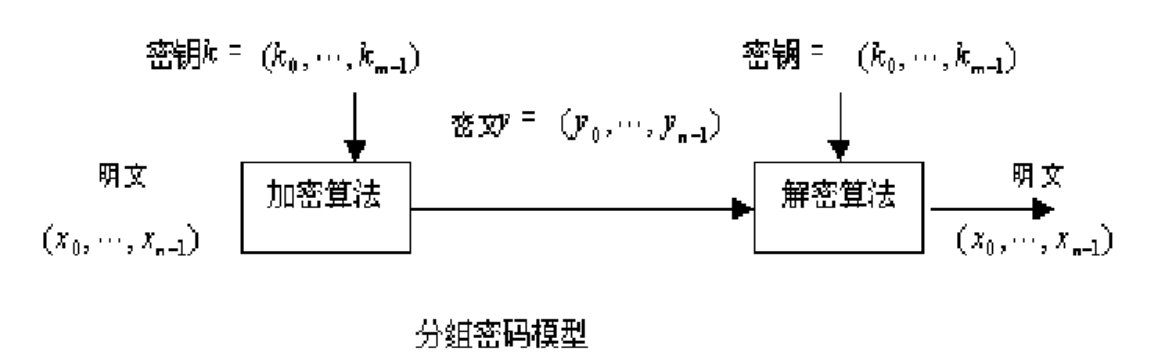


流密码

- 流密码（ Stream Cipher ）也称为序列密码，它是对称密码算法的一种。
  - 特点：流密码具有**实现简单、便于硬件实施、加解密处理速度快、没有或只有有限的错误传播**等特点，因此在实际应用中，特别是**专用或机密机构中**保持着优势，典型的应用领域包括**无线通信、外交通信**。 流密码强度依赖于密钥流产生器所生成**序列的随机性和不可预测性**。
  - 1949 年 Shannon 证明了**只有一次一密的密码体制是绝对安全的**，流密码方案的发展是模仿一次一密系统的尝试。如果**流密码所使用的是真正随机方式的、与消息流长度相同的密钥流，则此时的流密码就是一次一密的密码体制**。
  - 若能以**一种方式产生一随机序列（密钥流）**，这一序列由密钥所确定，则利用这样的序列就可以进行加密，即将密钥、明文表示成连续的符号或二进制，对应地进行加密，加解密时一次处理明文中的一个或几个比特。
  - 但实用中的流密码大多采用**有限存储单元和确定性算法**，可用有限状态自动机 (Finite State Automation) 来描述。 因此，**由有限状态机产生的序列是伪随机序列**。
- **典型算法： RC4**（在 SSL/TLS 、 IEEE 802.11 WEP 协议，以及 Microsoft Windows 、 Lotus Notes 、 Apple AOCE 、 Oracle Secure SQL 等系统中）

分组密码

- 分组密码是将明文消息编码表示后的数字（简称明文数字）序列，划分成**长度为 n** 的组（可看成长度为 n 的矢量）$x = (x_0, x_1, \ldots, x_{n-1})$，分别在密钥 $k = (k_0, k_1, \ldots, k_{t-1})$ 的控制下变换成**等长的输出数字序列** $y = (y_0, y_1, \ldots, y_{n-1})$，（长为 n 的矢量）

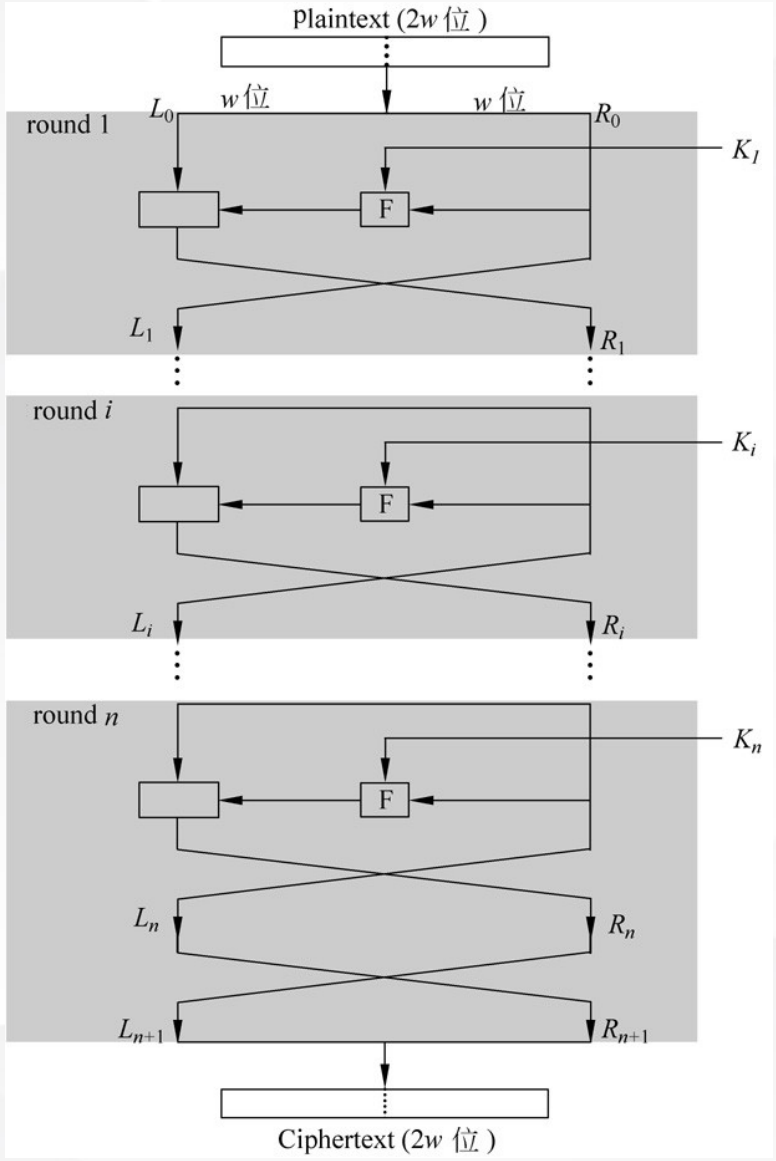


分组密码模型

- 典型的分组密码：**DES（三重 DES）、IDEA、RC5、RC6、CAST-128 等**

- 设计要求
  - 分组长度足够大（≥ 128~256 比特）
  - 密钥量要足够大（≥ 128~192~256 比特）
  - 算法足够复杂（包括子密钥产生算法）
  - 加密、解密算法简单，易软、硬件实现
  - 数据无扩展（只在引入同态置换和随机化加密时有扩展）
  - 差错传播尽可能得小

Feistel 密码结构



- IBM 公司的 Horst Feistel 结构的本质就是**单个循环不能提供足够的安全性，而多个循环提供的安全性高**，典型的循环次数是 16 次循环；
- **分组大小**：明文消息编码表示后的数字（简称明文数字）序列，划分成**长度为 n 的组**，每组分别在密钥的控制下变换成**等长的输出数字序列**
- **密钥大小**：密钥有不同的产生算法，密钥的长度影响密文的安全性
- **迭代轮数**：多轮重复循环处理
- **子密钥产生算法**：用于产生加密过程中的密钥
- **轮函数**：函数越复杂，安全性越好，更能抵抗密码分析，逻辑函数包括加法、减法和异或，固定循环 / 移位等

DES 具体算法过程（ 1 ）

- DES 是一种分组密码，假设明文 *m* 是有 0 和 1 组成的**长度为 64 比特的符号串**，密钥 *k* 也是 64 比特的 0,1 符号串，设：

$$m = m_1 m_2 \cdots m_{64}$$

$$k = k_1 k_2 \cdots k_{64}$$

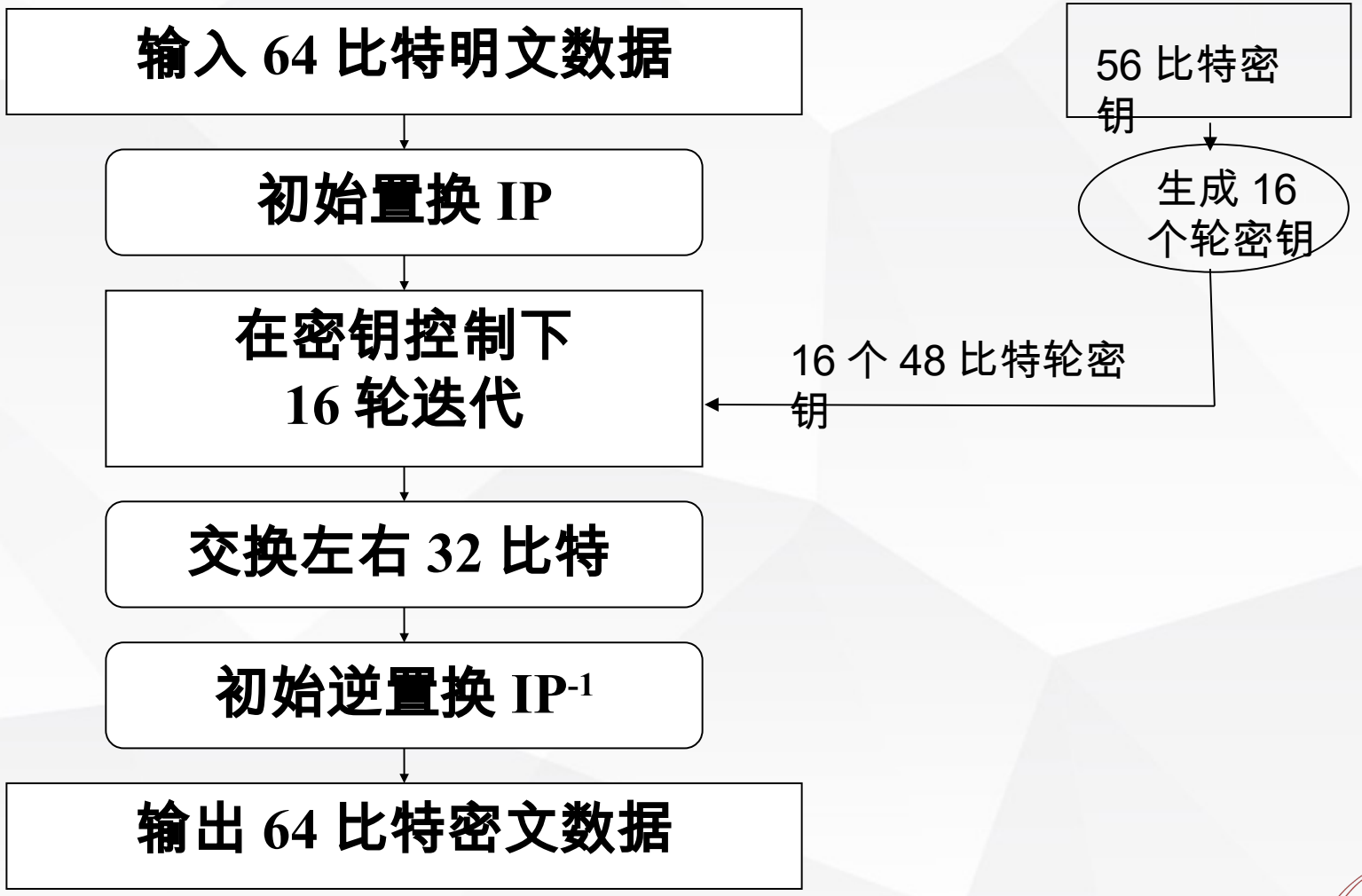
$$m_i, k_i = 0 \text{ 或 } 1, \quad i = 1, 2, \cdots, 64$$

- **64 比特密钥 *k* 只有 56 比特**有效 $k_8, k_{16}, k_{24}, k_{32}, k_{40}, k_{48}, k_{56}, k_{64}$ 这 8 位是奇偶校验位，在算法中不起作用，加密过程可表示为：

$$DES(m) = IP^{-1} \circ T_{16} \circ T_{15} \circ \cdots \circ T_2 \circ T_1 \circ IP(m)$$

DES 具体算法过程（ 2 ）

- DES 利用 56 比特串长度的密钥 K 来加密长度为 64 位的明文，得到长度为 64 位的密文



DES 具体算法过程（ 3 ）

初始置换 IP 和初始逆置换 IP^{-1}

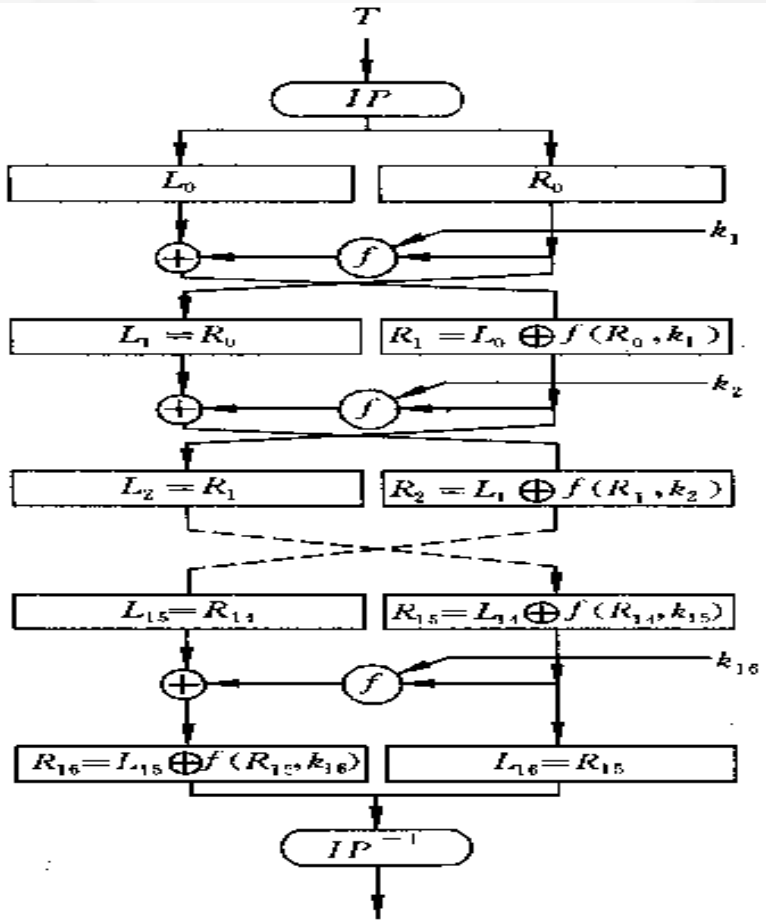
初始置换 IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

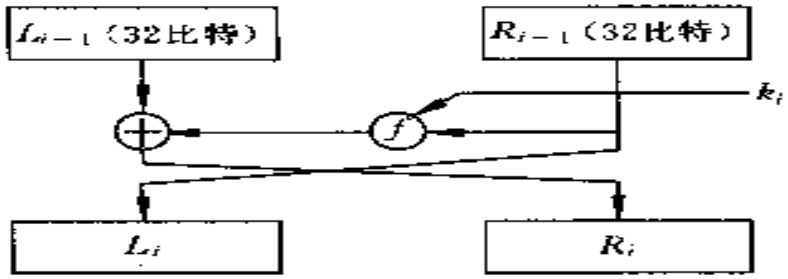
初始逆置换 IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

DES 具体算法过程（ 4 ）



DES 迭代示意图



DES 第 i 次迭代示意图

L_{i-1}和 R_{i-1}分别是第 $i-1$ 次迭代结果的左右两部分，各 32 比特。则

$$L_i = R_{i-1},\ R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

$m_0 = IP(m) = L_0R_0$, L_0 是 m_0 的前 32 比特，R_0 是 m_0 的后 32 比特

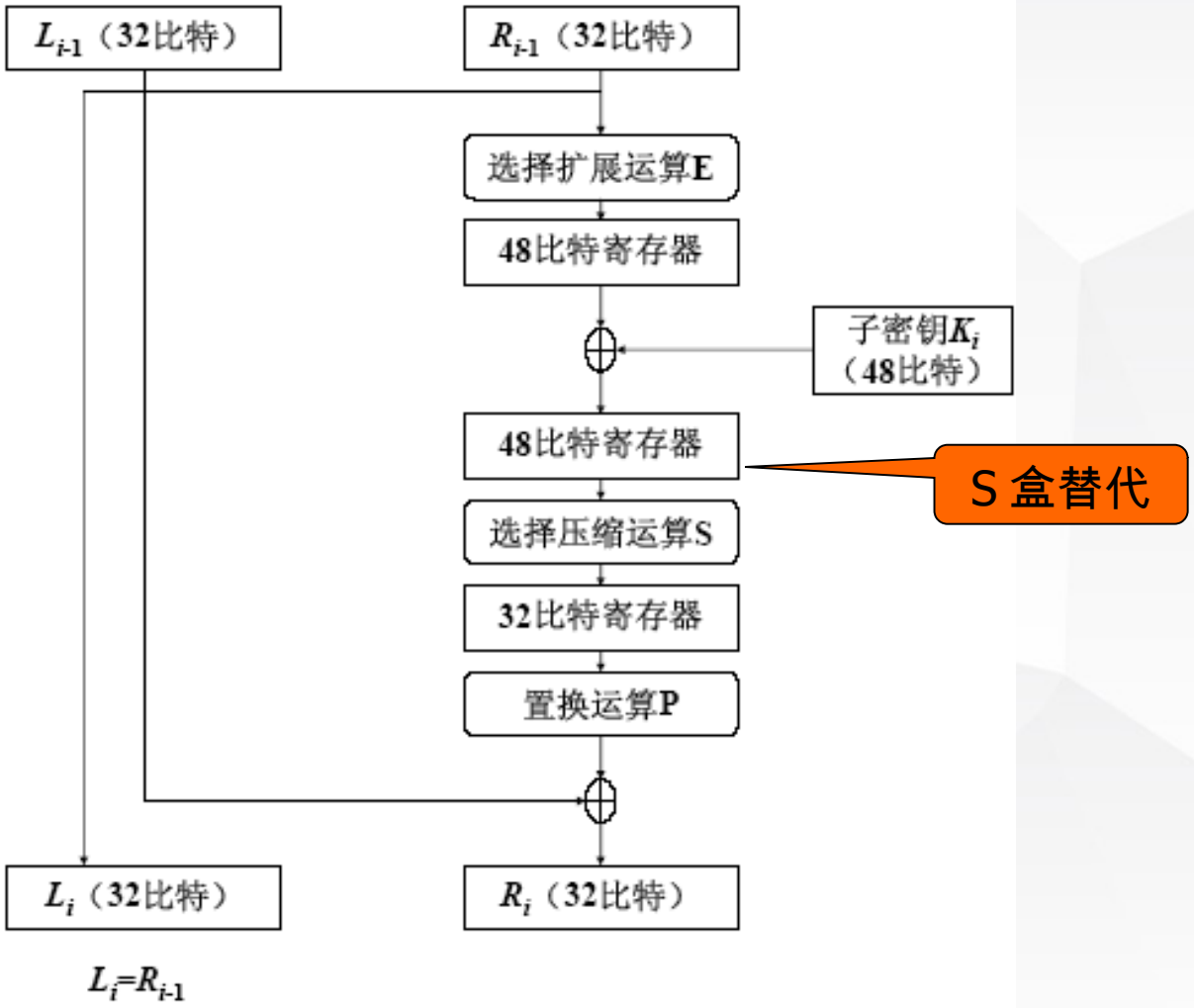
L_0, R_0 是初始输入经 IP 置换的结果。

⊕是按位作不进位加法运算，即

$$1 \oplus 0 = 0 \oplus 1 = 1,\ 0 \oplus 0 = 1 \oplus 1 = 0$$

k_i 是由 64 比特的密钥产生的子密钥，k_i 是 48 比特，

DES 的一轮迭代



DES的一轮迭代

三重 DES 算法 TDEA

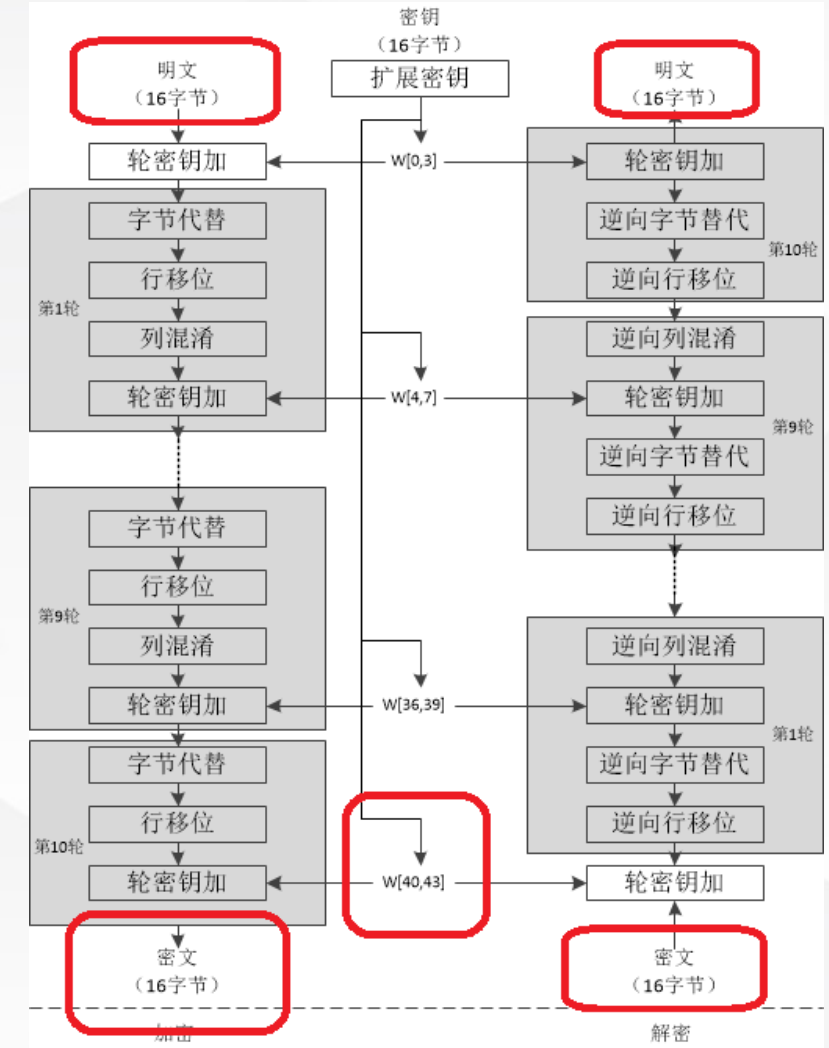
- 使用 3 倍 DES 密钥长度的密钥，执行 3 次 DES 算法
- 密钥长度是 112 位（两个不同的密钥）或 168 位（三个不同的密钥），对抗穷举攻击的能力得到极大加强
- 四种模式，包括：
  - DES-EEE3 模式，使用三个不同的密钥（ k1, k2, k3 ），进行三次加密
  - DES-EDE3 模式，使用三个不同的密钥（ k1, k2, k3 ），采用加密 - 解密 - 加密模式
  - DES-EEE2 模式，使用两个不同的密钥（ k1= k3, k2 ），进行三次加密。
  - DES-EDE2 模式，使用两个不同的密钥（ k1= k3, k2 ），采用加密 - 解密 - 加密模式。

高级加密标准 AES

- 1997 年 4 月 15 日，（美国）国家标准技术研究所（ NIST ）发起征集高级加密标准 AES 的活动，1999 年 3 月 22 日第二次 AES 会议上确定了 5 个候选算法：(Rivest Cipher)RC6 ， Rijndael ， SERPENT ， Twofish 和 MARS 。目的旨在代替 DES 算法。
- RC 系列被选为 21 世纪加密标准算法，由 RSA 公司的首席科学家 Ron Rivest 于 1994 年设计。 RC5-32/12/5, RC5-32/12/6,RC-32/12/7 已分别在 1997 年被破译，RC6 是 RC5 的进一步改进。
- 2000 年 10 月 2 日， NIST 宣布了获胜者— Rijndael 算法（分组 128/196/256 比特，密钥长度 128/192/256 比特），2001 年 11 月出版了最终标准 FIPS PUB197 ，作为下一代对称密码算法的标准，不具有 Feistel 结构，速度快、对内存要求小，操作简单，以针对差分分析和线性分析，算法的抗攻击能力强。

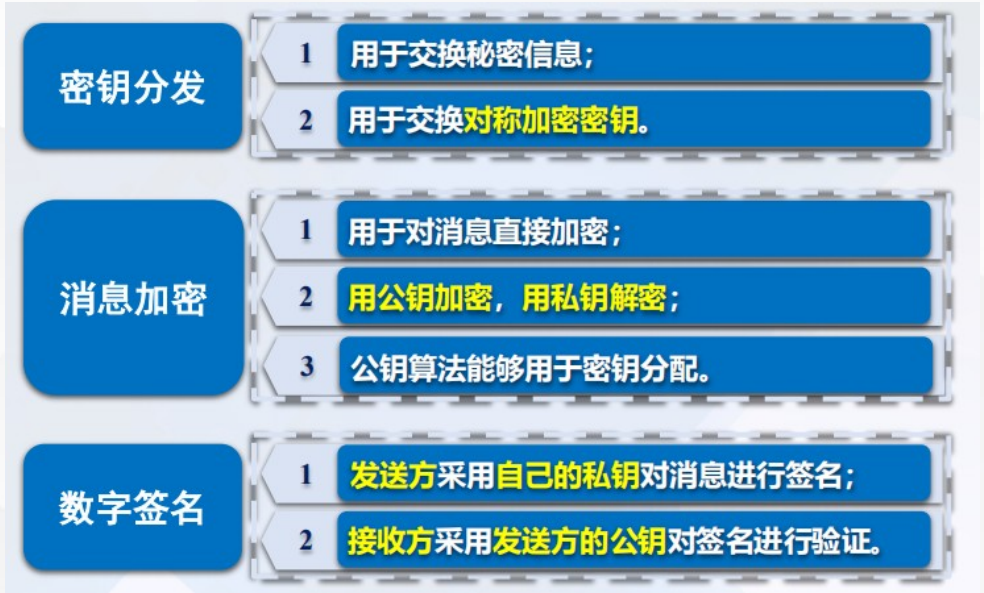
AES 算法举例

- 分组 16 字节 128 位
- 子秘钥 44 个，每个 32 位，每轮使用 4 个字， 128 位
- 每轮进行“字节替换”、“行移位”、“列混淆”、“轮密钥加”
- 10 轮迭代，但是非 **Feistel 结构**
- **每一步都简单可逆 A⊕B⊕B = A**



公钥加密体制

- 公钥技术是加密史上第一个真正有革命意义的进步，改变了密钥分发的方式，具备 密钥的分配和管理、数字签名和身份认证、数据加解密功能
  - 私钥为密码拥有者保管，不涉及分发问题，公钥采取公开渠道分发而不影响安全性，大大提高密钥分发的方便性，解决了对称密码体制中的密钥管理、分发和数字签名难题
- 公钥加密算法是基于数学函数而不是对“位”的形式的简单操作（如替换和置换、逻辑加、乘和异或），更为重要的是，加/解密钥是非对称的：公钥密码体制使用两个不同的密钥，在机密性、密钥分配及认证领域中，具有深远的影响。
- 目前，通常要求足够大的密钥长度（>1024 bits），密钥太长会导致加密速度缓慢，因此公钥算法常用于密钥传递，而一般 不用于实时的数据加密

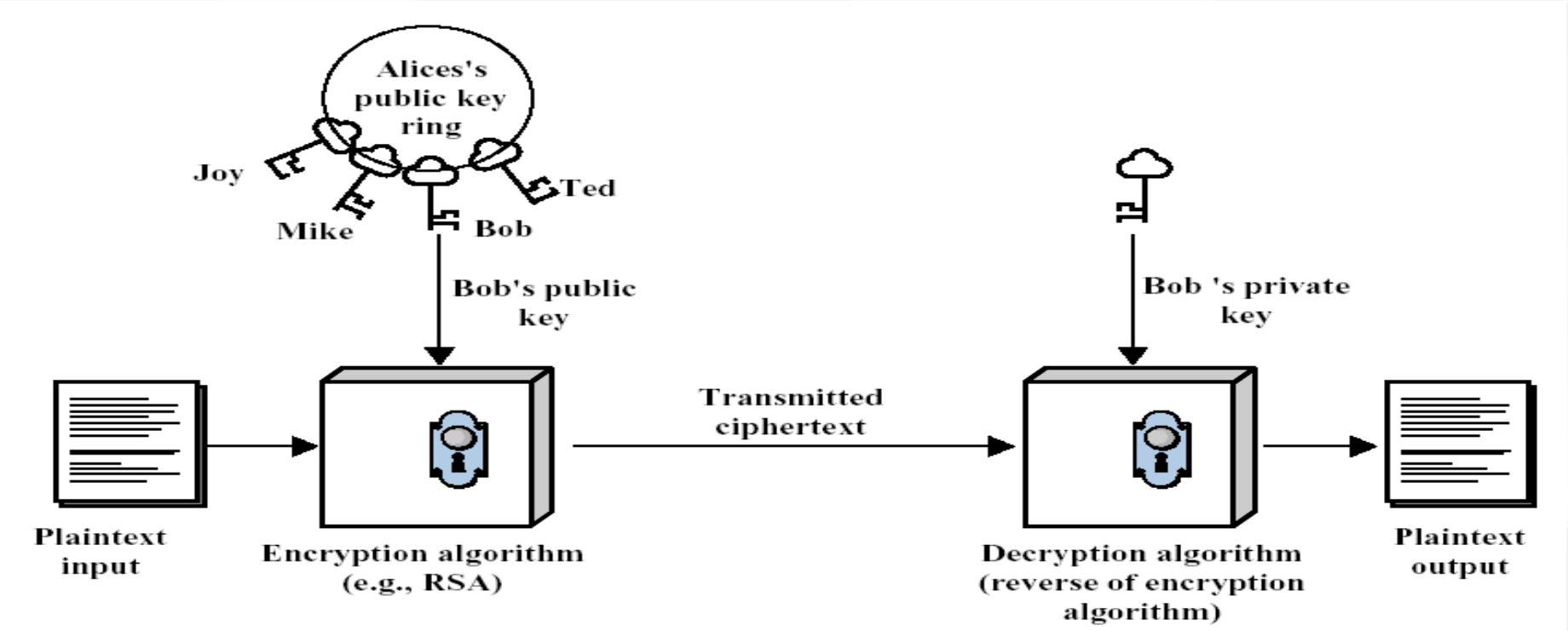


公钥加密体制

- 由公钥及算法描述，计算私钥是难的（an NP-time problem）（NP 问题，非确定性多项式时间可解的判定问题），相对应：由私钥及其他密码信息容易计算出公开密钥（a polynomial time (P-time) problem)
- 公钥密码体制是基于单向陷门函数的概念。单向函数是一些易于计算但难于求逆的函数，而单向陷门函数就是在已知一些额外信息的情况下易于求逆的单向函数，这些额外信息就是所谓的陷门。
- 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”。
- 典型公钥算法：RSA 算法三种方式都适合，Diffe-Hellman 算法只适合于密钥交换，DSS（数字签名标准）适合于数字签名，ElGamal 适合于前两种，椭圆曲线算法（ECC）三种都适合。

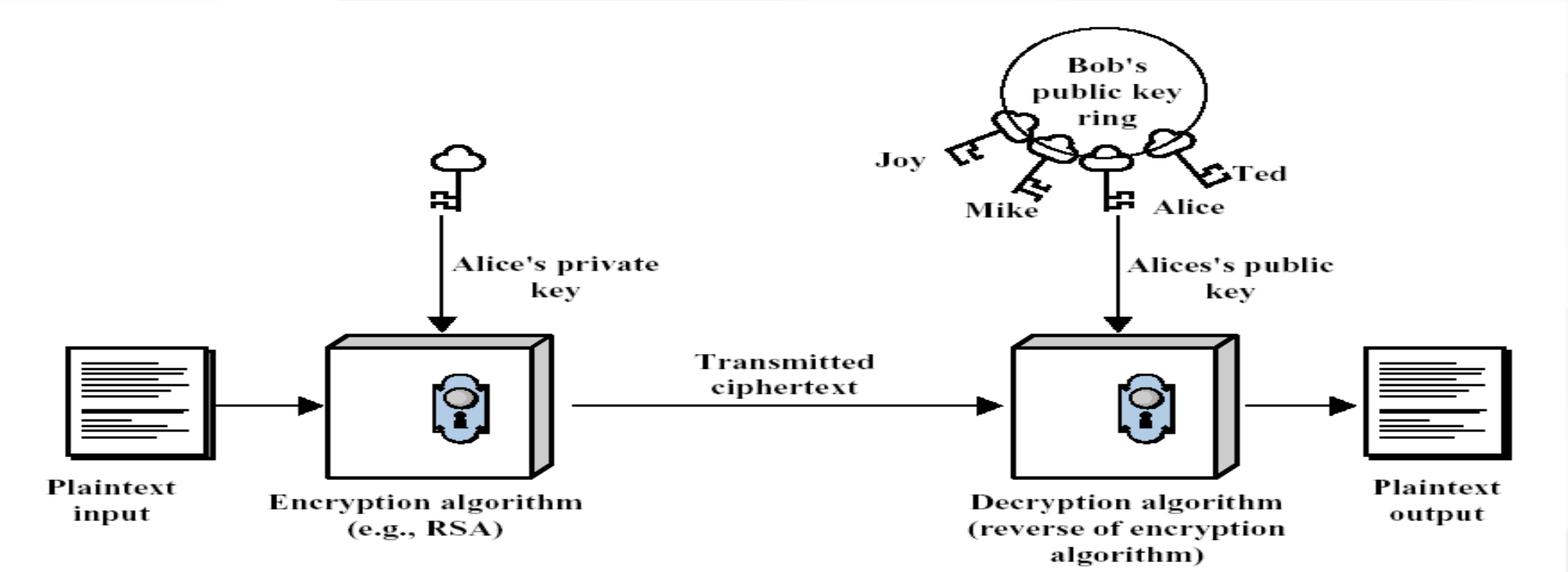
公钥加密方案

基于公开密钥的加密过程



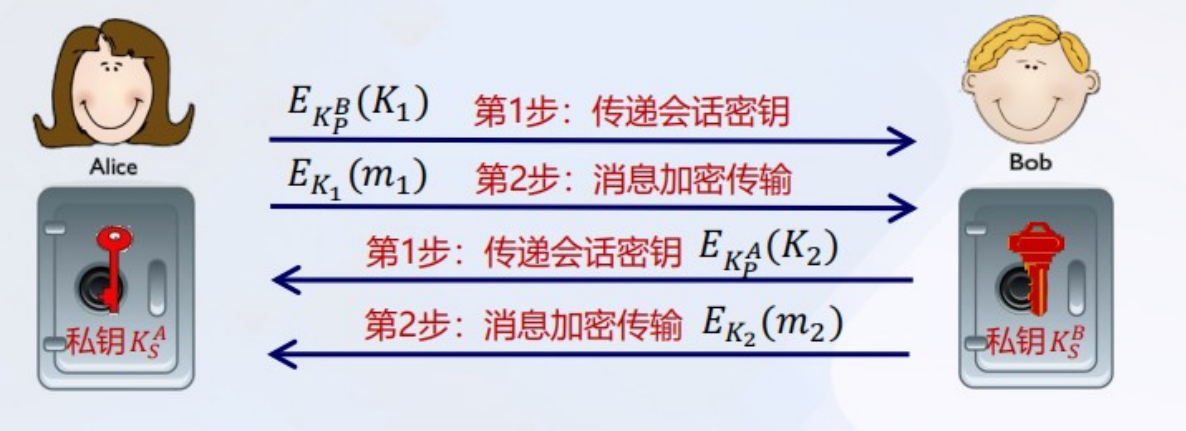
当 Alice 给 Bob 发信息时，她必须采用 Bob 的**公钥**K^B_P对消息加密，而不是采用 Alice 的公钥对消息加密。 Bob 采用自己的**私钥**K_S^B对密文解密。

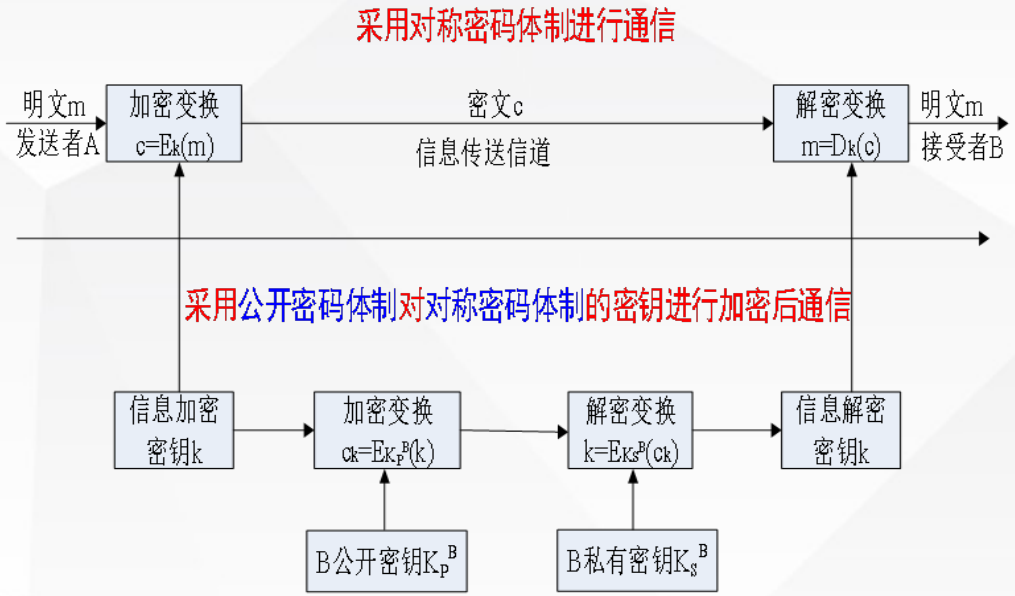
公钥算法应用：认证



当 Alice 给 Bob 发信息时，她必须采用自己的**私钥K_S^A**对消息加密（签名），而不是采用 Bob 的公钥对消息加密。 Bob 采用 Alice 的**公钥K_P^A**对密文解密，认证。

公钥+常规密钥结合的加密方案





原理：利用公开加密的方法来保护常规加密密钥的传送，保证常规加密密钥的安全性，然后用常规加密方法来保护传送的数据。这种方法利用了公开加密方法安全性的特点和常规加密方法速度快和适应性强的特点，同时避免了公开加密方法加/解密速度慢的缺点。

为了安全，再传递会话密钥前，还需要进行双方身份确认。

RSA 算法

- （1）取两个素数 p 和 q（保密）；
- （2）计算 $n=pq$（公开），$\varphi(n)=(p-1)(q-1)$（保密）；
- （3）随机选取整数 e，满足 $\gcd(e, \varphi(n))=1$（公开），即 gcd 最大公约数，e 与 $\varphi(n)$ 互素且小于 $\varphi(n)$；
- （4）计算 d，满足 $de \equiv 1 \pmod{\varphi(n)}$（保密）。
- 利用 RSA 加密第一步需将**明文数字化**，并取**长度小于 $\log_2 n$ 位**的数字作明文块。
- 加密算法：$c=E(m) \equiv m^e \pmod{n}$
- 解密算法：$D(c) \equiv c^d \pmod{n}$

RSA 算法举例（ 1 ）

- 假设 P=3 、 Q=11
- 计算 n=pq=33 ， $\varphi(n)=(p-1)(q-1)=20$
- 随机选择整数 e ，满足 $1<e<\varphi(n)=20$, gcd(e ， $\varphi(n)$)=gcd(e ， 20)=1, 这里选择 e=7
- 解方程 $de\equiv 1 \pmod{\varphi(n)}$ ， 即 $7d\equiv 1 \pmod{20}$ ，很容易得到 d=3
- 密钥对即为：（ 7 ， 3 ）
- 这里假设明文是： M=4
- 加密： $4^7=16384$ mod （ 33 ）=16 ，
- 解密： $16^3=4096$ mod （ 33 ）=4

RSA 算法举例（ 2 ）

1. 选素数 p=47 和 q = 71 ，得 n=3337，$\varphi(n)=46\times70 = 3220$ ；
2. 选择 e=79 ，求得私钥 $d=e^{-1} \equiv 1019 \pmod{3220}$ 。
3. 公开 n=3337 和 e=79.
4. 现要发送明文 688 ，计算：

   $688^{79} \pmod{3337}=1570$
5. 收到密文 1570 后，用私钥 d = 1019 进行解密：

   1570^{1019} （ $\pmod{3337}=688$

Rabin 公钥密码算法

其安全性依赖于模合数平方根困难问题

选择素数 p，q，满足 $p \equiv q \equiv 3 \bmod 4$

选择密钥：p，q

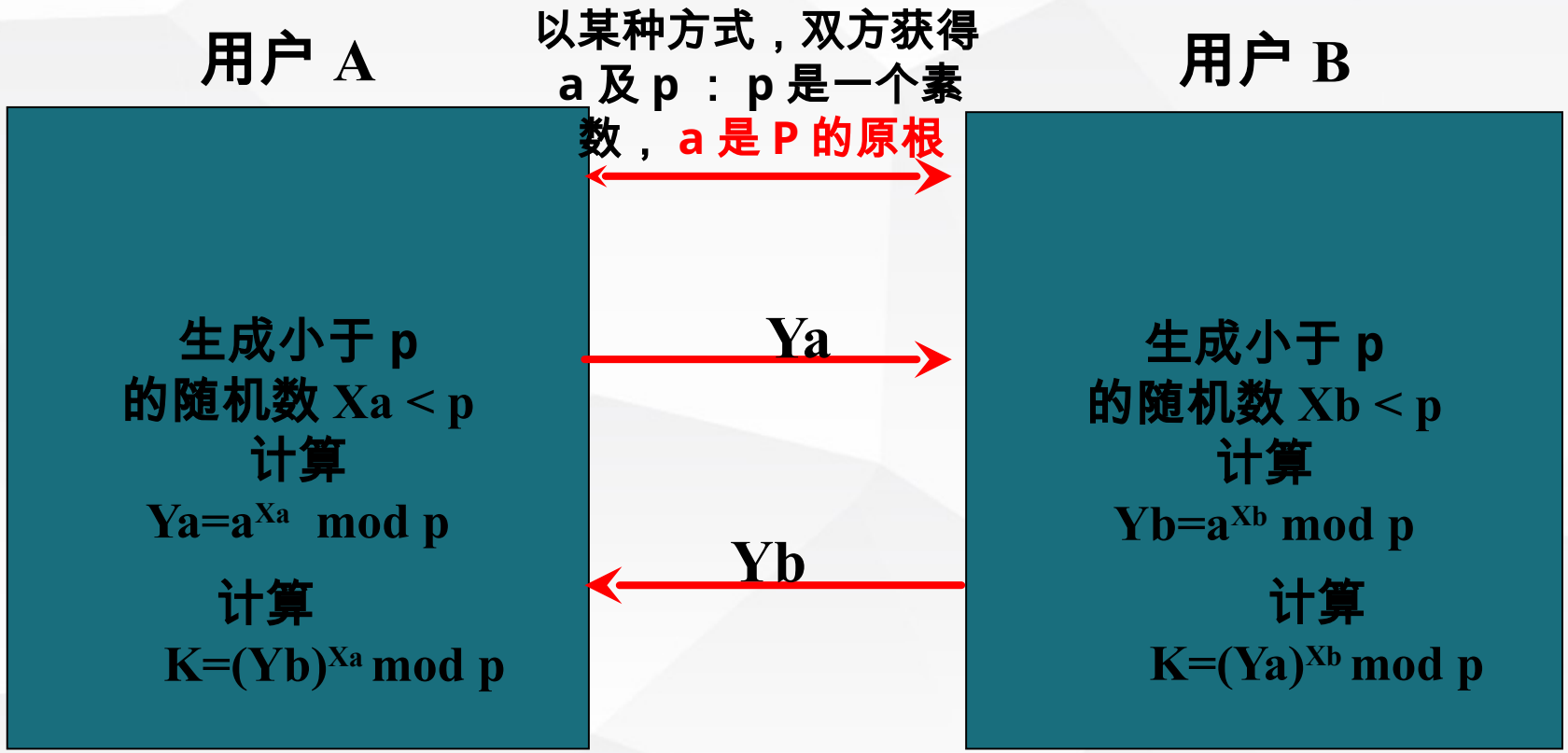
计算公钥：$n=pq$

加密：$C = M^2 \bmod n$

解密：$M = \pm C^{\frac{p+1}{4}} \bmod p$ 或者 $M = \pm C^{\frac{q+1}{4}} \bmod q$

Diffie-Hellman 算法 --- 密钥交换

- 允许两个用户可以安全地交换一个秘密信息，用于后续的通讯过程，大量的商用产品使用这种密钥交换技术；算法的安全性依赖于**计算离散对数的难度**。



Diffie-Hellman 算法

- 选取素数 p=97, 以及原根 a=5
- 用户 A 选取随机数 X_A=36 并计算公钥 $y_a=5^{36}=50 \bmod 97$
- 用户 B 选取随机数 X_B=58 并计算公钥 $y_b=5^{58}=44 \bmod 97$
- A 和 B 交换公钥（ 50 和 44 ）
- A 计算共享密钥 $K=44^{36}=75 \bmod 97$
- B 计算共享密钥 $K=50^{58}=75 \bmod 97$

ElGamal 公钥密码算法

- 1985 年 ElGamal 设计；
- ElGamal 公钥密码体制安全性是基于有限域上计算离散对数的困难性；
- 提出了加密模型和认证模型两种体制，加密模型没有被充分利用，而认证模型被广泛应用：如加 / 解密、密钥交换、数字签名等，形成美国数字签名标准 DSS 的基础
- 公钥算法加密解密速度慢

椭圆曲线公钥密码算法（ ECC)

- ECC 发展了 30 年，已经比较成熟， ECC 实际上是将原有的经典的加密算法通过某些运算移植到安全的椭圆曲线方程上，如 Diffie-Hellman 协议、 ElGamal 协议等。
- 椭圆曲线离散对数问题（ ECDLP ）是椭圆曲线密码学的基础
  - 给定一条椭圆曲线 E ，并在曲线上取一点 P ，并用 x_P 表示点 P 与自身相加 x 次，即 x_P=P+P+…… + P ，共有 x 个 P 相加。假设曲线 E 上有一点 Q ，使得 Q=x_P 成立，那么椭圆曲线离散对数问题就是给定点 P 和点 Q ，求解 x 的问题。
- RSA 的位长度一直在增加，加大了处理的负担， ECC 能够为相当小的代码提供近似相同的安全性，减少了处理开销：如 160 位 ECC 与 1024 位 RSA 有相同的安全强度。而 210 位 ECC 则与 2048 位 RSA 具有相同的安全强度
- 椭圆曲线密码体制的优点：安全性高，具有数学难题保证的安全性、密钥尺度小，参数选择较灵活、实现速度快，被广泛应用于商用密码领域。

单向散列算法

- 单向散列函数指的是根据输入消息（任何字节串，如文本字符串、 Word 文档、 JPG 文件等）输出固定长度数值的算法，输出数值也称为“散列值”或“消息摘要”，其长度取决于所采用的算法，通常在 128 ~ 256 位之间。单向散列函数旨在创建用于验证消息完整性的简短摘要，目的和好处是能使不同的消息生成不同的散列值。

由任意长的消息计算出一个固定长度数值的数学单向变换： m → H(m)

- 散列函数 h=H（ M ），其中， M 是发长的报文， h 是定长的散列值。设 x 、 x′ 是两个不同的消息，如果 H （ x ）=H （ x′ ），则称 x 和 x′ 是哈希函数 H 的一个（对）碰撞（ collision ）。
- 强加密单向散列函数是这样设计的：不可能通过计算找出两条散列值相同的消息。
- MD5 和 SHA-1 是两种强加密单向散列算法，其中 MD5 是 Ron Rivest （ RSA 算法的发明者之一）于 1992 年发明的，该算法生成 128 位的散列值；而 SHA-1 是由美国国家标准与技术研究院（ National Institute of Standards and Technology ， NIST ）于 1995 年发明的，它生成 160 位的散列值。
- 2002 年， NIST 发布了修改后的 SHA 版本 ,SHA-2 系列算法包括 SHA-224 、 SHA-256 、 SHA-384 和 SHA-512

国产密码

- 国密算法是国家商用密码管理办公室指定的一系列密码标准，又称**商用密码**。它能够实现加密、解密和认证等功能的技术，包括密码算法编程技术和密码算 法芯片、加密卡等的实现技术。
- 从根本上摆脱对国外密码技术和产品的过度依赖

国密算法

分组对称密码算法	SM1、SM4、SM7、祖冲之密码（ZUC）
非对称密码算法	SM2（椭圆曲线）、SM9（双线性对）
杂凑函数算法	SM3

国产密码

- SM1 、 SM4 算法与 AES 算法具有相同的密钥长度分组长度——128 位，因此在安全性上高于 112 位的 3DES 算法， SM1 主要用于有线网络，其加密强度与 AES 相当。该算法不公开，仅以 IP 核的形式存在于芯片中。调用该算法时，需要通过加密芯片的接口进行调用。
- SM4 是无线局域网标准的分组数据算法，是我国自主设计的分组对称密码算法，用于实现数据的加密 / 解密运算，以保证数据和信息的机密性。
- SM2 椭圆曲线公钥密码算法是我国自主设计的公钥密码算法，包括 SM2-1 椭圆曲线数字签名算法、 SM2-2 椭圆曲线密钥交换协议、 SM2-3 椭圆曲线公钥加密算法，分别用于实现数字签名密钥协商和数据加密等功能。
- SM3 密码摘要算法是中国国家密码管理局 2010 年公布的中国商用密码**杂凑算法标准**，适用于商用密码应用中的数字签名、验证数据认证码的生成与验证、随机数的生成，摘要长度 256 位。

上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

谢谢！

饮水思源 爱国荣校