密钥分配与密钥管理

1 单钥加密体制的密钥分配

密钥分配方法

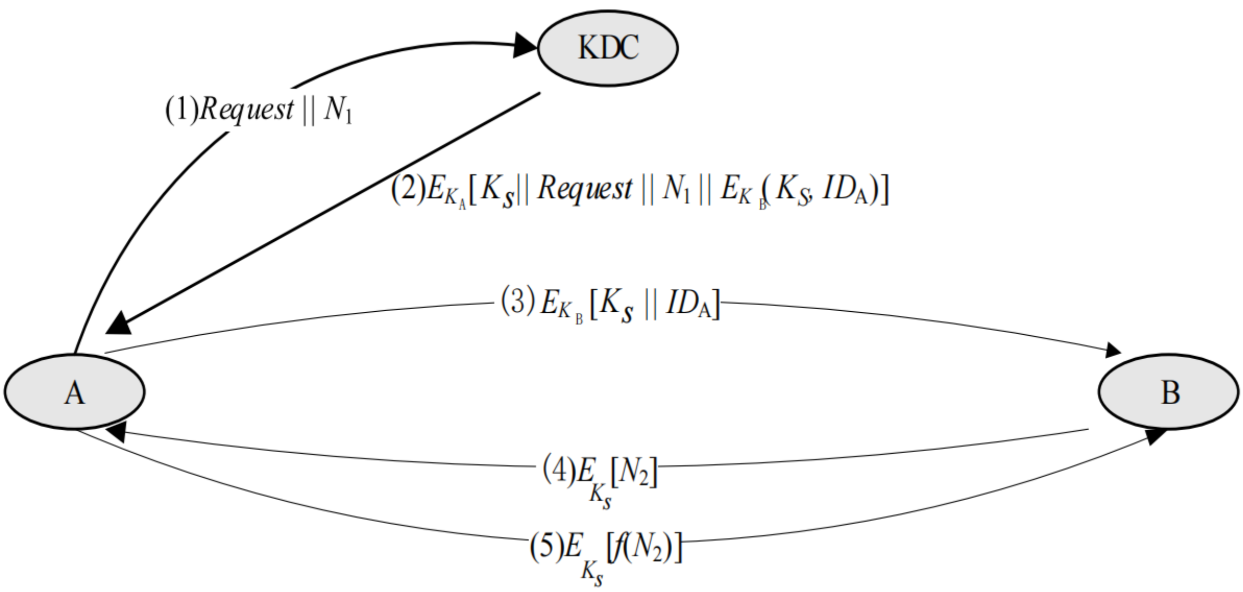
1. A选取物理手段发送给B
2. 第三方选取，物理手段发送给AB
3. AB事先有一密钥，选取新密钥后用已有密钥加密，发送给另一方
4. **AB与第三方C分别有一保密信道，则C为AB选取密钥后，分别在两个保密信道上发送给AB。**

其中，第4种方法常用，以下介绍第4种方法。

密钥分配中心
第三方——密钥分配中心KDC(Key Distribution Center)
主密钥（密钥加密密钥）——每一用户与密钥分配中心的共享密钥
会话密钥（加密密钥）——通过主密钥分配给一对用户的密钥，用于这一对用户之间的保密通信

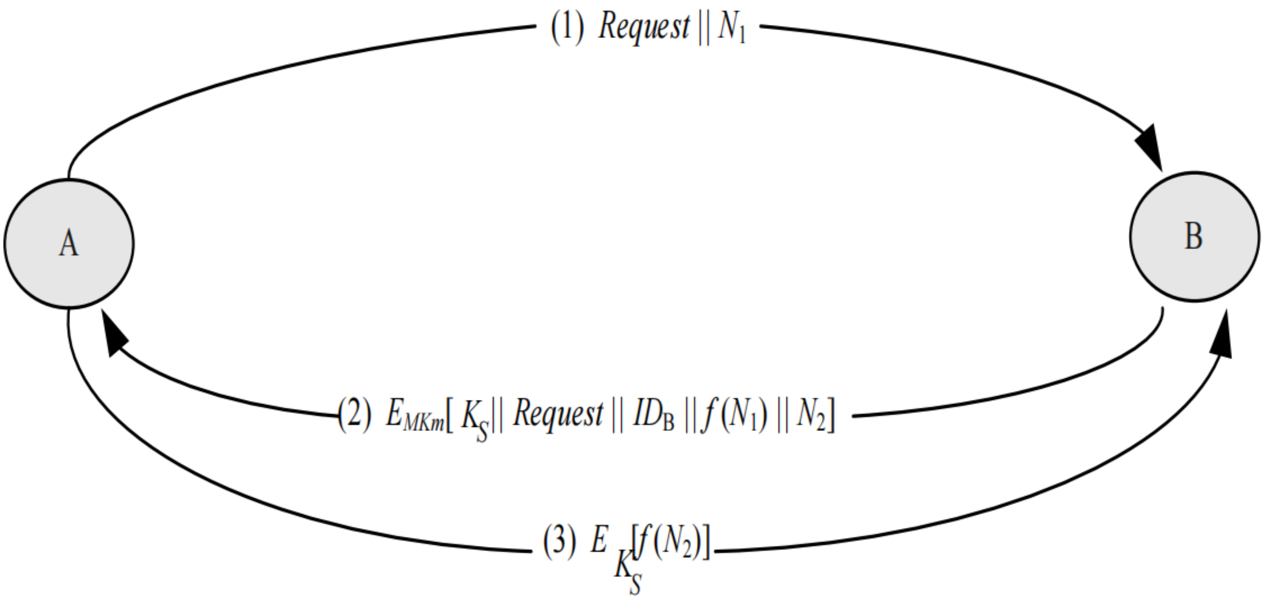
密钥分配过程

1. A向KDC发出请求，请求消息包括：
    - A与B的身份$Request$
    - 本次业务的唯一识别符N_1（通常为随机数）
2. KDC对A的请求发出应答，由K_A加密，消息包括：
    - 一次性会话密钥K_S
    - $Request$（防止请求在KDC收到前被篡改）
    - N_1（防止应答是过去的回放）
    - 用K_B加密的内容$E_{K_B}(K_S,ID_A)$：（向B证明A的身份）
        - 一次性会话密钥
        - A的身份ID_A
3. A将$E_{K_B}(K_S,ID_A)$发送给B
    B收到后可以确定是KDC发来的，得到会话密钥，同时得知另一方是A
    至此，会话密钥已成功分配给AB。
4. B用会话密钥加密另一个一次性随机数N_2，将结果发给A
5. A以$f(N_2)$作为对B的应答，用会话密钥加密后发给B
    4，5步骤使B相信第3步收到的消息不是重放，属于认证过程。



密钥分层控制
多个KDC分层
优点：减少主密钥分布；将虚假KDC的危害限制到一个局部区域

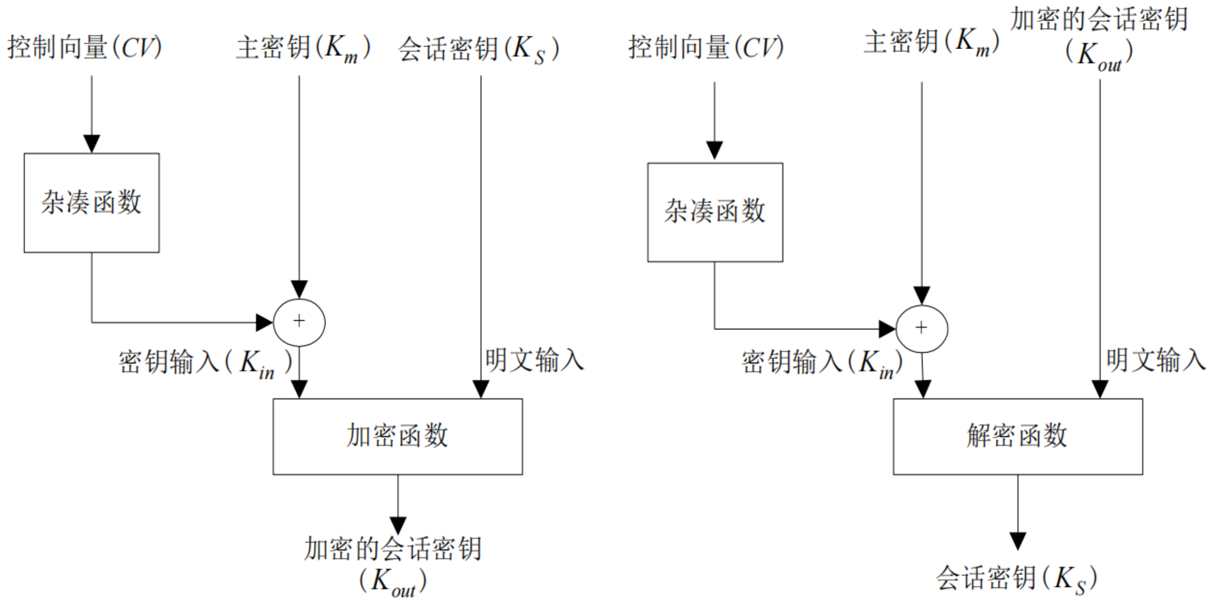
无中心的密钥分配
用户数量小时使用：



密钥控制技术

- **密钥标签**
  用于DES的密钥控制
  定长：8个校验位，其中1比特表示会话密钥/主密钥；1比特表示能否用于加密；1比特表示能否用于解密。
  密文形式传送

- **控制矢量**
  变长：由杂凑函数将其压缩到与加密密钥等长，然后与主密钥异或后作为加密会话密钥的密钥 $$H=h(CV)$$ $$K_{in}=K_m\oplus H$$ $$K_{out}=E_{K_m \oplus H}[K_S]$$ **明文形式传送**



(a) 结合 (b) 去除

图5-3 控制矢量的使用方式

2 公钥加密体制的密钥分配

2.1 **公钥分配方法**

1. 公开发布
2. 公用目录表
3. 公钥管理机构

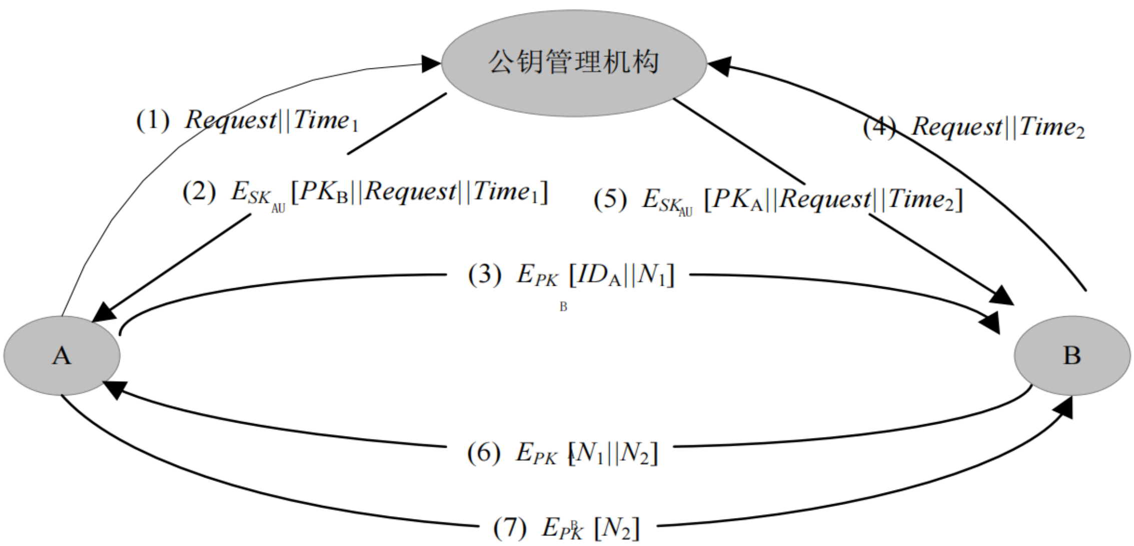
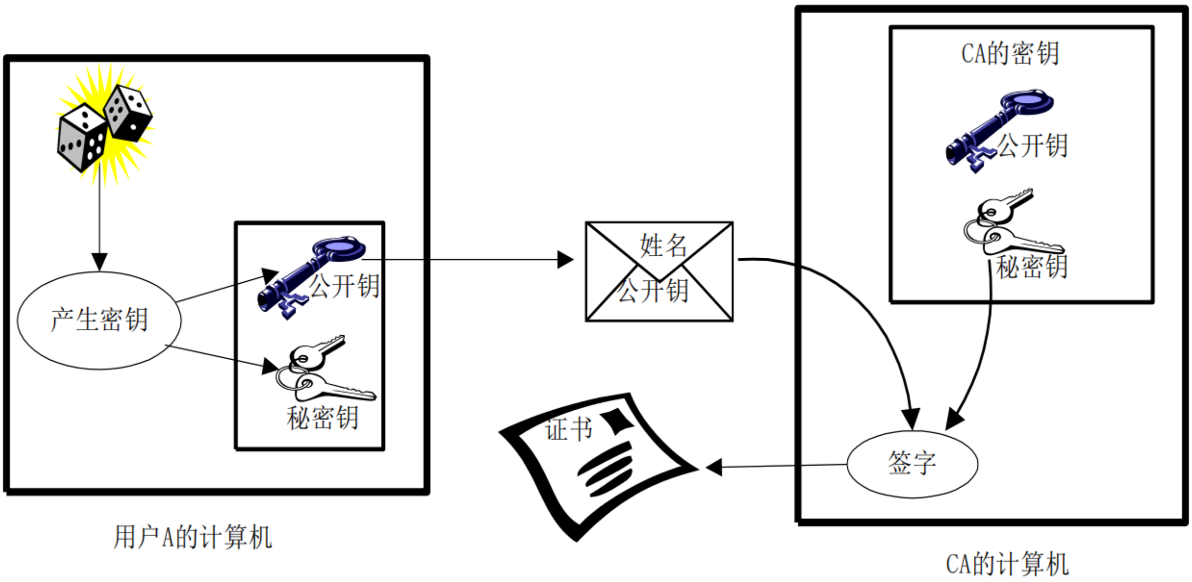


图5-4 公钥管理机构分配公钥

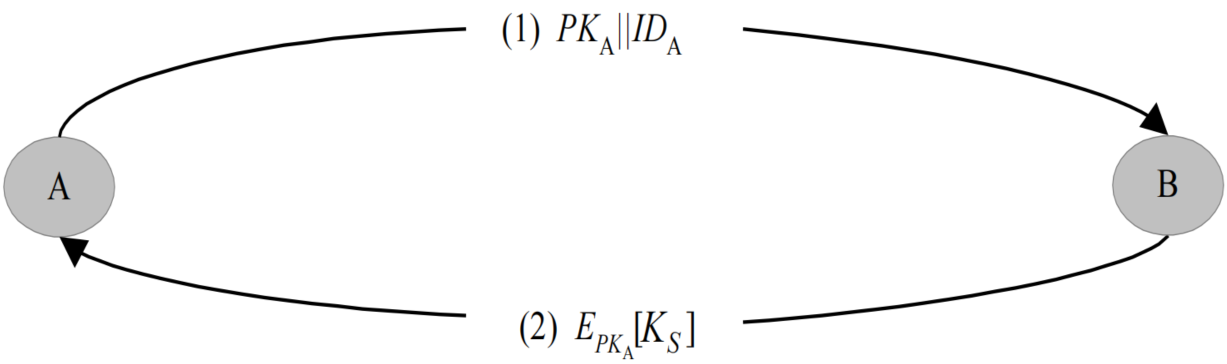
4. **公钥证书**
证书由**证书管理机构CA**(Certificate Authority)为用户建立
数据：用户私钥相匹配的公钥；用户身份；时戳
所有数据经CA用自己的密钥签字后，形成证书，**证书的形式**为$$C_A=E_{SK_{CA}}[T,ID_A,PK_A]$$ **证书产生过程**



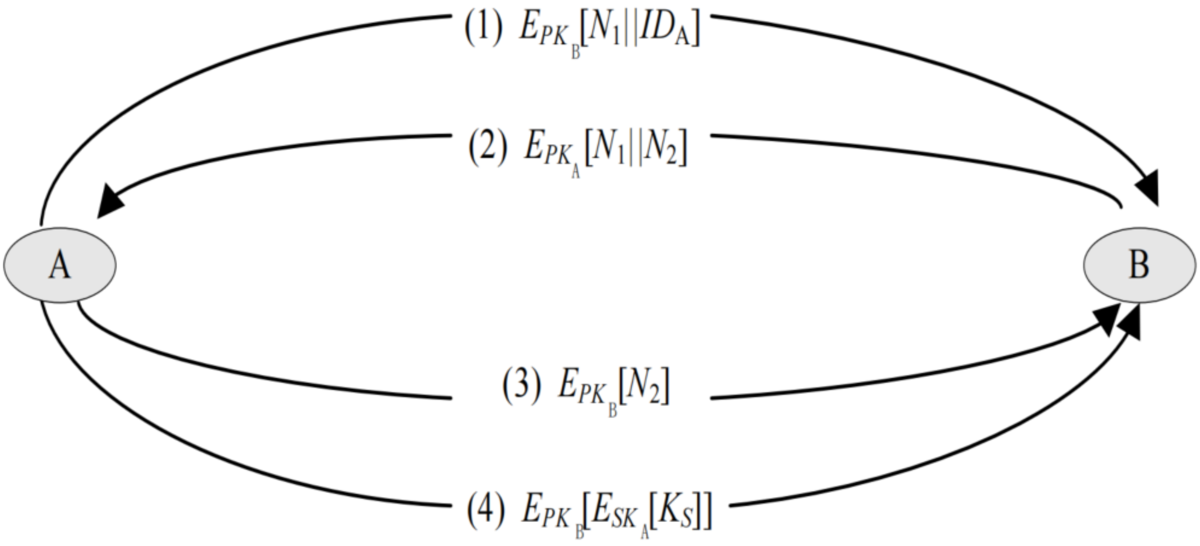
用户将自己的公钥证书发给另一用户，接收方使用CA的公钥对证书进行验证$$D_{PK_{CA}}[C_A]=D_{PK_{CA}}[E_{SK_{CA}}[T,ID_A,PK_A]]=(T,ID_A,PK_A)$$

2.2 用公钥加密分配单钥密码体制的密钥

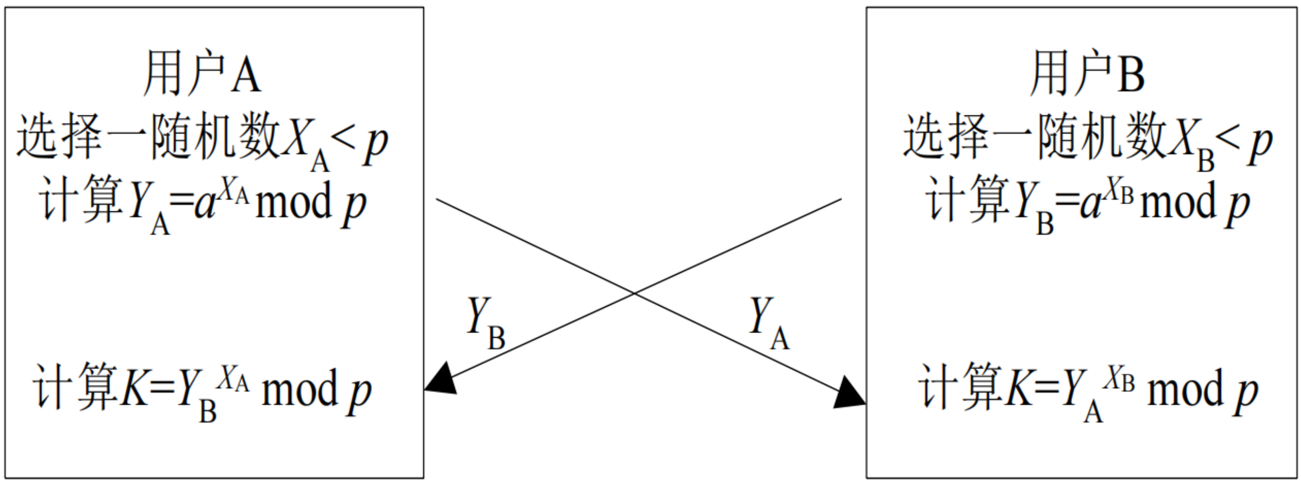
1. 简单分配



2. 具有保密性和认证性的密钥分配



2.3 Diffie-Hellman密钥交换



（见公钥密码部分）

3 随机数的产生

作用：一次性随机数防止重放攻击
nonce: number used for only once
随机数序列需要满足**随机性**和**不可预测性**

1. 随机性

- 均匀分布：每个数出现的频率相等
- 独立性：任意一数不能由其它数推出

2. 不可预测性

伪随机数产生器

1. **幂形式**
   迭代公式$$X_{n+1}=(X_n)^d\bmod m, n=1,2,3\dots$$ 其中，(d,m)为参数，X_0是种子
   根据参数的取法，幂形式分为以下两种：
   （1）RSA产生器
   m为大素数的乘积，d为RSA的密钥，满足$gcd(d,\phi (m))=1$
   （2）平方产生器
   $d=2, m=pq, p\equiv q\equiv3\bmod 4$ （类似Rabin密码体制的取法）
2. **离散指数形式**
   迭代公式$$X_{n+1}=g^{X_n}\bmod m, n=1,2,\dots$$ 其中，(g,m)为参数，X_0是种子

基于密码算法的随机数产生器

1. **循环加密**
2. **DES的输出反馈(OFB)模式**
3. **ANSI X9.17伪随机数产生器**

随机比特产生器

1. **BBS(Blum-Blum-Shub)产生器**
   选取 $p\equiv q\equiv3\bmod 4$，计算$ n=pq$
   随机数s，使 $gcd(s,n)=1$
   按以下算法产生比特序列${B_i}$: $$X_0=s^2\bmod n$$ $$for\quad i=1\quad to \quad \infty \quad do:$$ $$X_{i}=(X_{i-1})^2\bmod n$$ $$B_i=X_i\bmod 2$$ 即在每次循环中取X_i的最低位。
2. **Rabin产生器**
   迭代公式如下：$$X_i= \begin{cases} (X_{i-1})^2\bmod n\quad if(X_{i-1})^2 \bmod n < n/2\ n-(X_{i-1})^2\bmod n\quad if(X_{i-1})^2 \bmod n \geq n/2 \end{cases}$$ 取X_i最低位
3. **离散指数比特产生器**
   离散指数伪随机数产生器产生的随机数列的最高位

4 秘密分割

(k,n)-秘密分割门限方案
设秘密s被分成n个部分信息，每一部分信息称为一个子密钥或影子，由一个参与者持有，使得：

- 由k个或多于k个参与者所持有的部分信息可重构s
- 由少于k个参与者所持有的部分信息则无法重构 s

其中，k称为**门限值**

完善的(k,n)-秘密分割门限方案
在上述两条满足的基础上，满足：

- 由少于k个参与者所持有的部分信息得不到s任何信息

4.1 Shamir门限方案

基于多项式的**Lagrange插值公式**：

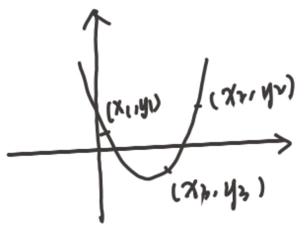
> Lagrange插值公式
> 已知$\phi(x)$在k个互不相同的点的函数值$\phi(x_i)(i=1,2,\dots,k)$，可构造$k-1$次插值多项式为

> $$f(x)=\sum^{k}_{j=1}\phi(x_j)\prod^{k}_{l=1 \& l\neq j}\frac{x-x_l}{x_j-x_l}$$

密钥s取为$f(0)$，n个子密钥取为$f(x_i)(i=1,\dots,k)$，则利用其中k个子密钥可重构s。
简要说明：

对Shamir门限方案的简单说明.

考虑抛物线 $y=ax^2+bx+c$.



需已知3个点才可解出原方程. ⇒ 门限为3.

少于3个无法确定任何一个 ⇒ 完善的

每个点都是一个影子 通过解方程组可重构原密钥.

举例：

式(5.11)，所以已知$k-1$个子密钥得不到关于秘密s的任何信息，因此这个方案是完善

【例 5-4】 设$k=3,n=5,q=19,s=11$，随机选取$a_1=2,a_2=7$，得多项式为

$$f(x)=(7x^2+2x+11)\bmod 19$$

分别计算

$$f(1)=(7+2+11)\bmod 19=20 \bmod 19=1$$
$$f(2)=(28+4+11)\bmod 19=43 \bmod 19=5$$
$$f(3)=(63+6+11)\bmod 19=80 \bmod 19=4$$
$$f(4)=(112+8+11)\bmod 19=131 \bmod 19=17$$
$$f(5)=(175+10+11)\bmod 19=196 \bmod 19=6$$

得5个子密钥。

如果知道其中的3个子密钥$f(2)=5,f(3)=4,f(5)=6$，就可按以下方式重构$f(x)$：

$$\begin{aligned}5\frac{(x-3)(x-5)}{(2-3)(2-5)}&=5\frac{(x-3)(x-5)}{(-1)(-3)}=5\frac{(x-3)(x-5)}{3}\\&=5\cdot(3^{-1}\bmod 19)\cdot(x-3)(x-5)\\&=5\cdot 13\cdot(x-3)(x-5)=65(x-3)(x-5)\end{aligned}$$

$$\begin{aligned}4\frac{(x-2)(x-5)}{(3-2)(3-5)}&=4\frac{(x-2)(x-5)}{(1)(-2)}=4\frac{(x-2)(x-5)}{-2}\\&=4\cdot((-2)^{-1}\bmod 19)\cdot(x-2)(x-5)\\&=4\cdot 9\cdot(x-2)(x-5)=36(x-2)(x-5)\end{aligned}$$

$$\begin{aligned}6\frac{(x-2)(x-3)}{(5-2)(5-3)}&=6\frac{(x-2)(x-3)}{(3)(2)}=6\frac{(x-2)(x-3)}{6}\\&=6\cdot(6^{-1}\bmod 19)\cdot(x-2)(x-3)\\&=6\cdot 16\cdot(x-2)(x-3)=96(x-2)(x-3)\end{aligned}$$

所以

$$\begin{aligned}f(x)&=[65(x-3)(x-5)+36(x-2)(x-5)+96(x-2)(x-3)]\bmod 19\\&=[8(x-3)(x-5)+17(x-2)(x-5)+(x-2)(x-3)]\bmod 19\\&=(26x^2-188x+296)\bmod 19\\&=7x^2+2x+11\end{aligned}$$

从而得秘密为$s=11$。

4.2 基于中国剩余定理的门限方案

设$m_1,m_2,\dots,m_n$为n个大于1的整数，满足$$m_1\leq m_2\leq \dots\leq m_n$$ $$gcd{m_i,m_j}=1$$ $$m_1m_2\dotsm_k>m_nm_{n-1}\dots m_{n-k+2}$$ 秘密数据s满足$$m_1m_2\dotsm_k>s >m_nm_{n-1}\dots m_{n-k+2}$$ 计算$M=m_1m_2\dotsm_n, s_i=s\bmod m_i, (i=1,\dots,n)$
子密钥：(s_i,m_i,M)
计算方法：
对于k个参与者（记作$i_1,\dots,i_k$），每个人计算 $$\begin{cases} M_{i_j}=\frac{M}{m_{i_j}} \ N_{i_j}=M_{i_j}^{-1}\bmod m_{i_j} \ y_{i_j}=s_{i_j}M_{i_j}N_{i_j} \end{cases}$$ 结合起来，根据中国剩余定理可得方程组 $$\begin{cases} s\equiv s_{i_1} \bmod m_{i_1}\ \dots \ s\equiv s_{i_k} \bmod m_{i_k} \end{cases}$$ 的解

$$s=\sum^{k}{j=1}y{i_j}\bmod \prod^{k}{j=1}m{i_j}$$ 举例:

【例 5-5】 设 $k=3, n=5, m_1=97, m_2=98, m_3=99, m_4=101, m_5=103$，秘密数据 $s=671\ 875$，满足 $10\ 403=m_4m_5<s<m_1m_2m_3=941\ 094$。

计算 $M=m_1m_2m_3m_4m_5=9\ 790\ 200\ 882$，$s_i\equiv s(\bmod\ m_i)(i=1,\cdots,5)$ 得 $s_1=53$，$s_2=85, s_3=61, s_4=23, s_5=6$。5 个子密钥为(53,97,9 790 200 882)，(85,98,9 790 200 882)，(61,99,9 790 200 882)，(23,101,9 790 200 882)，(6,103,9 790 200 882)。

现在假定 i_1、i_2、i_3 联合起来计算 s，分别计算：

$$\begin{cases}M_1=\dfrac{M}{m_1}=100\ 929\ 906\\ N_1\equiv M_1^{-1}(\bmod\ m_1)\equiv 95\end{cases}\quad \begin{cases}M_2=\dfrac{M}{m_2}=99\ 900\ 009\\ N_2\equiv M_2^{-1}(\bmod\ m_2)\equiv 13\end{cases}\quad \begin{cases}M_3=\dfrac{M}{m_3}=98\ 890\ 918\\ N_3\equiv M_3^{-1}(\bmod\ m_1)\equiv 31\end{cases}$$

得到

$$\begin{aligned}s&\equiv s_1M_1N_1+s_2M_2N_2+s_3M_3N_3(\bmod\ m_1m_2m_3)\\&\equiv 53\cdot 100\ 929\ 906\cdot 95+85\cdot 99\ 900\ 009\cdot 13+\\&\quad 61\cdot 98\ 890\ 918\cdot 31(\bmod\ 97\cdot 98\cdot 99)\\&\equiv 805\ 574\ 312\ 593(\bmod\ 941\ 094)\\&\equiv 671\ 875\end{aligned}$$

假定 i_1、i_4、i_5 联合起来计算 s，分别计算：

$$\begin{cases}M_1=\dfrac{M}{m_1}=100\ 929\ 906\\ N_1\equiv M_1^{-1}(\bmod\ m_1)\equiv 95\end{cases}\quad \begin{cases}M_4=\dfrac{M}{m_4}=96\ 932\ 682\\ N_4\equiv M_4^{-1}(\bmod\ m_4)\equiv 61\end{cases}\quad \begin{cases}M_5=\dfrac{M}{m_5}=95\ 050\ 494\\ N_5\equiv M_5^{-1}(\bmod\ m_5)\equiv 100\end{cases}$$

得到

$$\begin{aligned}s&\equiv s_1M_1N_1+s_4M_4N_4+s_5M_5N_5(\bmod\ m_1m_4m_5)\\&\equiv 53\cdot 100\ 929\ 906\cdot 95+23\cdot 96\ 932\ 682\cdot 61+\\&\quad 6\cdot 95\ 050\ 494\cdot 100(\bmod\ 97\cdot 101\cdot 103)\\&\equiv 701\ 208\ 925\ 956(\bmod\ 1\ 009\ 091)\\&\equiv 671\ 875\end{aligned}$$

假定 i_1、i_4 联合起来计算 s，则

$$\begin{aligned}s&\equiv s_1M_1N_1+s_4M_4N_4(\bmod\ m_1m_4)\\&\equiv 53\cdot 100\ 929\ 906\cdot 95+23\cdot 96\ 932\ 682\cdot 61(\bmod\ 97\cdot 101)\\&\equiv 644\ 178\ 629\ 556(\bmod\ 9791)\\&\equiv 5679\end{aligned}$$

得到一个不正确的结果。