§4.4 相关补充

一、多密钥的公钥密码体制

它是RSA的一种推广。令n=pq，p和q为两个大素数，选择t个密钥k_1，k_2，…，k_t，使$k_1 \times k_2 \times \ldots \times k_t \equiv 1 \bmod \phi(n)$

令M是明文消息，

$$M^{k1 \times k2 \times \ldots \times kt} \equiv M \bmod n$$

因此可以由k_1，k_2，…，k_t组成多种加解密组合。

如，若t=5，则以k_3和k_5加密的消息M，可以用k_1、k_2和k_4进行解密：

$$C = M^{k3 \times k5} \bmod n$$

$$M = C^{k1 \times k2 \times k4} \bmod n$$

§4.4 相关补充

在多重签名中的应用。设想A和B都必须签署一个文件才能使之生效，可以使用三个密钥：k_1，k_2和k_3，k_1为A的私钥，k_2为B的私钥，k_3为公开密钥。

(1) A签署M，并发送给B：$S' = M^{k1} \bmod n$

(2) B证实文件内容：$M = S'^{k2 \times k3} \bmod n$

(3) B添加自己的签名：$S = S'^{k2} \bmod n$，

S即A和B共同对文件M的签名

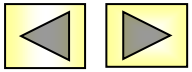
(4) 任何人都可以验证S的合法性：$M = S^{k3} \bmod n$

§4.4 相关补充

二、秘密共享密码体制

秘密共享系统是将秘密S在一组参与者集P中进行分配，使P中的合格子集能恢复秘密S，其余不合格子集都不能恢复S。

Shamir和Blakley最早提出秘密共享概念，并给出了(t,n)门限秘密共享体制。秘密共享体制使秘密被多个人掌管提供了可能。例如导弹控制发射、打开银行金库、遗嘱的生效等都必须由两人或多人共同参与。



§4.4 相关补充

Shamir提出利用有限域GF(p)上的t－1次多项式

$$h(x)=a_{t-1}x^{t-1}+\ldots+a_1x+a_0 \bmod p$$

构造秘密共享的(t，n)门限体制。

其中随机素数p大于最大可能的秘密S和参与者总数n，并且公开； $S=h(0)=a_0$，而a_{t-1}，…，a_1为选用的随机系数，需要保密，在生成n个秘密份额后即可销毁。通过计算多项式h(x)对n个不同x_i的取值就给出了每个人的秘密份额

$$S_i=h(x_i) \bmod p \qquad i=1,2,\ldots,n$$

(S_i，x_i)为用户的标识。

任意t个用户出示其份额可重构秘密S。

§4.4 相关补充

由LaGrange内插法

$$h(x)=\sum_{r=1}^{t} S_r \prod_{j\neq r,\, j=1}^{t} \frac{x-x_{i_j}}{x_{i_r}-x_{i_j}} \mod p$$

例如：(3, 5)门限体制。选S=13, p=17, $h(x)=2x^2+10x+13$

选x=1,2,3,4,5，5个秘密份额

$S_1=h(1)=(2+10+13) \bmod 17=8$

$S_2=h(2)=(8+20+13) \bmod 17=7$

$S_3=h(3)=(18+30+13) \bmod 17=10$

$S_4=h(4)=(32+40+13) \bmod 17=0$

$S_5=h(5)=(50+50+13) \bmod 17=11$

§4.4 相关补充

从任意三个秘密份额可重构多项式h(x)。

如给定S_1，S_3，S_5，则有

$$h(x)=8\frac{(x-3)(x-5)}{(1-3)(1-5)}+10\frac{(x-1)(x-5)}{(3-1)(3-5)}+11\frac{(x-1)(x-3)}{(5-1)(5-3)} \bmod 17$$

$$=x^2-8x+15-\frac{5}{2}(x^2-6x+5)+\frac{11}{8}(x^2-4x+3) \bmod 17$$

$$=-\frac{1}{8}x^2+\frac{3}{2}x+\frac{53}{8} \bmod 17$$

$$=2x^2+10x+13 \bmod 17$$

§4.4 相关补充

(t，n)门限体制的特点：

（1）在参与者集P中成员总数不超过p的前提下，可以增加新成员，即计算新的秘密份额不会改变已有的秘密份额。

（2）通过选用常数项不变的另一个t-1次多项式，可将某个成员的秘密份额作废。

（3）可以根据成员重要性不同分给不等个数的秘密份额，实现分级方案。

