§4.3 其他公钥密码体制

MH公钥背包密码：其背包系列$a_1,a_2,\ldots,a_n$是由超递增系列$b_1,b_2,\ldots,b_n$（$b_i > \sum_{j=1}^{i-1} b_j$）经过MH变换$a_k=wb_k$得到的。

虽然$a_1,a_2,\ldots a_n$不具有超递增性，但可经变换后成为超递增系列求解。若超递增背包问题确实有解，则容易用所谓的贪心算法求出其解。

例：超递增序列1，2，4，…，2^n，若背包方程

$$x_1+2x_2+4x_3+8x_4+16x_5+32x_6=47$$

则$x_6=1$，$x_5=0$，$x_4=1$，$x_3=1$，$x_2=1$，$x_1=1$

§4.3 其他公钥密码体制

MH公钥背包密码过程：

（1）密钥生成

用户构造长度为n的超递增背包分量$b_1, b_2, \ldots, b_n$，选择两个正整数M，W，其中$M \geq \sum_{i=1}^{n} b_i$，W<M且保证(W，M)=1。

则由$W\ W^{-1} = 1 \bmod M$，求出W^{-1}（$0 < W^{-1} < M$），

计算$a_i = Wb_i \bmod M$，$0 \leq i \leq n$

选择背包系统的公钥为$PK=(a_1, a_2, \ldots, a_n)$，

私钥为$SK=(b_1, b_2, \ldots, b_n, M, W^{-1})$

§4.3 其他公钥密码体制

（2）加密过程

用户A给用户B发送秘密消息时，使用B的公钥PK，对明文$m=(m_1, m_2, \ldots, m_n)$进行加密变换：

$$C = E_{PK}(m) = \sum_{i=1}^{n} m_i a_i$$

（3）解密过程

用户收到密文C后，使用自己的私钥SK，计算

$$C' = (W^{-1} \cdot C) \bmod M = (\sum_{i=1}^{n} W^{-1} m_i a_i \bmod M) \bmod M$$

$$= (\sum_{i=1}^{n} m_i b_i) \bmod M = \sum_{i=1}^{n} m_i b_i$$

§4.3 其他公钥密码体制

例：设超递增背包序列为{1, 2, 5, 9, 20, 41, 83, 164}，用MH背包算法进行加解密。

1）因为1+2+5+9+20+41+83+164=325，所以取M＝353，W＝233，用辗转相除法计算得W^{-1}＝50；

2）$a_1=W\cdot b_1(\text{mod } 353)=233*1(\text{mod } 353)= 233 (\text{mod } 353)$

$a_2=W\cdot b_2(\text{mod } 353)=233*2(\text{mod } 353)= 113 (\text{mod } 353)$

$a_3=W\cdot b_3(\text{mod } 353)=233*5(\text{mod } 353)= 106 (\text{mod } 353)$

$a_4=W\cdot b_4(\text{mod } 353)=233*9(\text{mod } 353)= 332 (\text{mod } 353)$

$a_5=W\cdot b_5(\text{mod } 353)=233*20(\text{mod } 353)= 71 (\text{mod } 353)$

$a_6=W\cdot b_6(\text{mod } 353)=233*41(\text{mod } 353)= 22 (\text{mod } 353)$

$a_7=W\cdot b_7(\text{mod } 353)=233*83(\text{mod } 353)= 277 (\text{mod } 353)$

$a_8=w\cdot b_8(\text{mod } 353)=233*164(\text{mod } 353)= 88 (\text{mod } 353)$

§4.3 其他公钥密码体制

3）得到背包序列{233, 113, 106, 332, 71, 22, 277, 88}，作为公钥公布，而{ 1, 2, 5, 9, 20, 41, 83, 164 }作为私钥保存；

4）假设要发送的明文是二进制信息：01011001

01011001对应的密文是$a_2+a_4+a_5+a_8$

$=113+332+71+88=604$

5）接收方收到密文后其解密过程为用50＊密文模353：

50＊604(mod 353)= 195(mod 353)=2+9 +20+164 (mod 353)

其对应的明文是01011001。

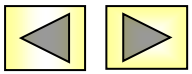
§4.3 其他公钥密码体制

二、ElGamal公钥密码体制

ElGamal算法在密码协议中有许多实际的应用，其安全性是基于求解离散对数问题的困难性。

ElGamal密码体制是1984年提出的一种双钥密码体制，既可以用于加密又可用于数字签名。

算法描述：设P至少是150位的十进制素数，p-1有大素因子。Z_p为有限域，若g为Z_p^*中的本原元，有$Z_p^* = <g>$。若取$y \in Z_p^* = Z_p \backslash \{0\}$，如何算得一个唯一的整数x（$0 \le x \le p-2$），满足$g^x = y \pmod p$，将x记为$x = \log_g y$ 。一般来说，求解x在计算上是难处理的。



§4.3 其他公钥密码体制

ElGamal公钥体制的描述：

设明文空间为P = Zp*，密文空间为C=Zp*×Zp*，定义密钥空间K={(p, g, x, y)|$y=g^x(\mathrm{mod}\ p)$}，公钥为：p, g ,y，私钥为：x

加密：Alice 取一个秘密随机数k∈Z_{p-1}，对明文M加密

$E(M, k)=(a, b)$

其中， $a=g^k(\mathrm{mod}\ p)$，$b=My^k(\mathrm{mod}\ p)$

解密：Bob计算

$D(a, b) = b(a^x)^{-1}(\mathrm{mod}\ p)$

注：1.容易验证$b(a^x)^{-1} = M(g^x)^k(g^{kx})^{-1} = M$

2.利用ElGamal加密算法可给出基于此的签名方案

§4.3 其他公钥密码体制

例：设p = 2579，如果选取g = 2，x = 765，则

1）$y = g^x \pmod p = 2^{765} \pmod{2579} = 949$ ；

2）设A要发送的消息m=1299,则A选择随机数k = 853并计算

$a = g^{853} \pmod{2579} = 435$；

及 $b = 1299 * 949^{853} \pmod{2579} = 2399$。

3）A发送密文c = (435, 2399)给B；

4）B收到后计算$m = 2399 * (435^{765})^{-1} \pmod{2579} = 1299$.

§4.3 其他公钥密码体制

三、椭圆曲线密码体制ECC

Elliptic Curve Cryptosystem

1985年，N. Koblitz和V. Miller分别独立提出了椭圆曲线密码体制(ECC)，其依据是定义在椭圆曲线点群上的离散对数问题的难解性。

椭圆曲线上的公钥密码体制的优点：速度快、安全性高、密钥短、灵活性好。

同等安全下的密钥长度：

RSA：512 1024 2048 21000

ECC：106 160 211 600