基于中国剩余定理的秘密共享方案

课程名称：信息安全基础综合实验

单　　位：西安电子科技大学

网络与信息安全学院

秘密共享是将秘密以适当的方式拆分，拆分后的每一个子秘密由不同的参与者管理，单个参与者无法恢复秘密信息，只有若干个参与者一同协作才能恢复秘密消息。并且，当其中某些参与者出问题时，秘密仍可以恢复。

(t,n)门限秘密共享方案

将秘密 k 分成 n 个子秘密 $k_1, k_2, \cdots, k_n$，满足下面两个条件：

（1） 如果已知任意 t 个k_i值，易于恢复出 k ；

（2） 如果已知任意 $t-1$ 个或更少个k_i值，不能恢复出 k。

将一个密钥分成n份，那么n个人中至少t人在场才能获得密钥。

1983年，Asmuth和Bloom提出基于中国剩余定理的(t,n)门限秘密共享方案

基于中国剩余定理的(t, n)门限秘密共享方案

秘密分割

一个秘密k，被分割成n个子秘密(d_i, k_i)

秘密恢复

n个子秘密(d_i, k_i)中任意选择t个，恢复出秘密k

(t,n)门限，一个秘密k，被分割成n个子秘密(d_i,k_i)

对于某个秘密 k，计算
$$\begin{cases} k_1 \equiv k(mod\ d_1) \\ k_2 \equiv k(mod\ d_2) \\ \vdots \\ k_n \equiv k(mod\ d_n) \end{cases}$$
则子秘密为(d_i,k_i)。

要求一： 选择n个整数$d_1,d_2,\cdots,d_n$，满足

（1）$d_1 < d_2 < \cdots < d_n$； d_i严格递增

（2）$(d_i,d_j) = 1,\ \ i \neq j$； d_i两两互素

（3）$N = d_1 \times d_2 \times \cdots \times d_t \quad M = d_{n-t+2} \times d_{n-t+3} \times \cdots \times d_n$，有$N > M$

t个最小的d_i的乘积严格大于$t-1$个最大的d_i的乘积

要求二： $N > k > M$

基于中国剩余定理的(t, n)门限秘密共享方案

秘密分割

一个秘密k，被分割成n个子秘密(d_i, k_i)

秘密恢复

n个子秘密(d_i, k_i)中任意选择t个，恢复出秘密k

n 个子秘密中任意选择 t 个，$(k_{i_1}, d_{i_1}), (k_{i_2}, d_{i_2}), \cdots, (k_{i_t}, d_{i_t})$，恢复出秘密 k

计算 $\begin{cases} x \equiv k_{i_1} (mod\ d_{i_1}) \\ x \equiv k_{i_2} (mod\ d_{i_2}) \\ \vdots \\ x \equiv k_{i_t} (mod\ d_{i_t}) \end{cases}$ 恢复出秘密 $x \equiv k (mod\ N_1)$，$N_1 = d_{i_1} d_{i_2} \cdots d_{i_t}$ 。

t 个子秘密能恢复出秘密

$t-1$个子秘密不能

没有足够的信息去确定k

任意选择 $t-1$ 个子秘密：

$(k_{j_1}, d_{j_1}), (k_{j_2}, d_{j_2}), \cdots, (k_{j_{t-1}}, d_{j_{t-1}})$

$x \equiv k (mod\ M_1)$，$M_1 = d_{j_1} d_{j_2} \cdots d_{j_{t-1}}$

$N_1 > N > k > M > M_1$

例题　基于中国剩余定理的(t,n)门限秘密共享方案

(t,n)门限，选择n个整数$d_1, d_2, \cdots, d_n$，满足

（1）$d_1 < d_2 < \cdots < d_n$；　　d_i严格递增

（2）$(d_i, d_j) = 1,\ \ i \neq j$；　　d_i两两互素

（3）$N = d_1 \times d_2 \times \cdots \times d_t$

$M = d_{n-t+2} \times d_{n-t+3} \times \cdots \times d_n$，有

$N > M$

t个最小的d_i的乘积严格大于$t-1$个最大的d_i的乘积

对于某个秘密k，要求$N > k > M$，计算

$$\begin{cases} k_1 \equiv k (mod\ d_1) \\ k_2 \equiv k (mod\ d_2) \\ \vdots \\ k_n \equiv k (mod\ d_n) \end{cases}$$

则子秘密为(d_i, k_i)。

一个秘密k，被分成n个子秘密(d_i, k_i)

秘密分割

$(2,3)$门限，选择3个整数$d_1 = 9, d_2 = 11, d_3 = 13$

$N = 99$，$M = 13$，有$N > M$

对于秘密$k = 74$，要求$99 > 74 > 13$，计算

$$\begin{cases} k_1 \equiv 74 \equiv 2 (mod\ 9) \\ k_2 \equiv 74 \equiv 8 (mod\ 11) \\ k_n \equiv 74 \equiv 9 (mod\ 13) \end{cases}$$

子密钥为$\{(9,2), (11,8), (13,9)\}$。

例题 于中国剩余定理的(t,n)门限秘密共享方案

3个子密钥$\{(9,2),(11,8),(13,9)\}$中任意选择2个：

$$(9,2),(11,8)$$

建立下列方程组

$$\begin{cases} x \equiv 2 \pmod 9 \\ x \equiv 8 \pmod{11} \end{cases}$$

基于中国剩余定理，解之得$x \equiv 74 \pmod{99}$。

恢复出秘密$k = 74$

秘密恢复

n个子秘密(d_i, k_i)中任意选择t个：

$$(k_{i_1}, d_{i_1}), (k_{i_2}, d_{i_2}), \cdots, (k_{i_t}, d_{i_t})$$

基于中国剩余定理计算下列一次同余方程组

$$\begin{cases} x \equiv k_{i_1} \pmod{d_{i_1}} \\ x \equiv k_{i_2} \pmod{d_{i_2}} \\ \quad\vdots \\ x \equiv k_{i_t} \pmod{d_{i_t}} \end{cases}$$

恢复出秘密$x \equiv k \pmod{N_1}$，$N_1 = d_{i_1} d_{i_2} \cdots d_{i_t}$。

The End