2017 级《信息安全综合课程实践》题目及要求

要求：

1、纸质版的报告按照课程设计的要求完成；

2、电子版材料包括：a)报告，b)程序源码，c)可执行文件或工程，d)程序的说明文档。

3、材料提交的最后期限为生产实习的最后一天。

题目 1：

秘密共享是指将一个含有秘密的数据D（例如，密码系统中的密钥、保险柜的号两组合等）分成n块$D_1,\cdots,D_n$，并满足下面的要求；

（1）知道任意k个或更多的D_j，就能够有效地计算出D；

（2）知道任意$k-1$个或更少的D_j，由于信息不够，不可能有效地计算出D。

Shamir称这种方法为(k,n)门限方案，并基于拉格朗日插值多项式提出了一种具体实现方案。其构造过程为：

在二维平面上给出k个点$(x_1,y_1),\cdots,(x_k,y_k)$,其中$x_i$各不相同，则有一个且仅有一个$k-1$次多项式$q(x)$满足：

$$q(x_i)=y_i, 1\leqslant i\leqslant k$$

不失一般性，可以假定数据D是一个数，为了把D分成小块D_j，选取一个随机的$k-1$次多项式：

$$q(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}$$

其中$a_0=D$，并计算出：

$$D_1=q(1),\cdots,D_n=q(n)$$

给定上述D_j值中的任意k个，可以通过插值法求出$q(x)$的系数，因此可以计算出$D=q(0)$。相反，如果仅仅知道这些D_j值中的$k-1$个，则由于信息不够而无法确定$q(x)$，所以不能求出D值。

当给定k个小块$D_{j_1},D_{j_2},\cdots,D_{j_k}$时，可以根据拉格朗日多项式，重新构造

$q(x)$：

$$q\left(x\right)=\sum_{i=1}^{k}D_{j_i}\prod_{\substack{s=1\\ s\neq i}}^{k}\frac{x-x_{j_s}}{x_{j_i}-x_{j_s}}\bmod p$$

因为进行的是模 p 下的运算，所以上式中的除法，是通过求出模 p 的逆之后再进行乘法运算实现的。

由于 $q(x)$ 中的系数 $a_1,\cdots,a_{k-1}$ 是从 $\left[0,p-1\right]$ 中的整数的均匀分布中随机地选取的。在密码分析员得到 $k-1$ 块 $D_{j_1},\cdots,D_{j_{k-1}}$ 的情形下，任何 $\left[0,p-1\right]$ 中的整数 D' 都有可能成为真正的 D 的候选值。对每一个 D'，密码分析员能构造且仅能构造一个 $k-1$ 次多项式 $q'\left(x\right)$，满足：

$$q'\left(0\right)=D'$$

及

$$q'\left(j_1\right)=D_{j_1},\cdots,q'\left(j_{k-1}\right)=D_{j_{k-1}}$$

由构造的方法可知，这 p 个可能的多项式作为 $q(x)$ 概率都是相等的，因此密码分析员得不到能够帮助他推导出 $q(x)$ 的任何信息。

需要注意的是，这里进行的是模数运算，而不是实数运算。因为插值定理在任何多项式环 $F\left[x\right]$ 中（其中多项式系数的集合F是一个域）都成立，且当 p 是素数时，$\mathbb{Z}_p$ 是一个域。所以给定整数 D 后，选取一个大于 D 和 n 的素数 p，此后所进行的计算，都是模 p 下的运算。

下面举一个具体的例子来说明该过程。

令 $k=3,n=5,p=19,D=11$。在 [0,18] 中随机地选取 $q(x)$ 的系数 $a_1=2,a_2=7$，因此：

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

分别计算出：

$$D_1=q\left(1\right)=\left(7+2+11\right)\bmod 19=20\bmod 19=1$$

$$D_2=q\left(2\right)=\left(28+4+11\right)\bmod 19=43\bmod 19=5$$

$$D_3 = q(3) = (63 + 6 + 11) \bmod 19 = 80 \bmod 19 = 4$$

$$D_4 = q(4) = (112 + 8 + 11) \bmod 19 = 131 \bmod 19 = 17$$

$$D_5 = q(5) = (175 + 10 + 11) \bmod 19 = 196 \bmod 19 = 6$$

假定知道其中三个小块$D_2 = 5$，$D_3 = 4$和$D_5 = 6$，就可以通过拉格朗日插值多项式求出$q(x)$。从而有：

$$5\frac{(x-3)(x-5)}{(2-3)(2-5)} = 5\frac{(x-3)(x-5)}{(-1)(-3)}$$

$$= 5\frac{(x-3)(x-5)}{3}$$

$$= 5 \cdot \mathrm{inv}(3,19) \cdot (x-3)(x-5)$$

$$= 5 \cdot 13 \cdot (x-3)(x-5)$$

$$= 65\ (x-3)(x-5)$$

其中inv(3,19)=13表示$3 \cdot 13 \equiv 1 (\bmod 19)$。此外还有：

$$4\frac{(x-2)(x-5)}{(3-2)(3-5)} = 4\frac{(x-2)(x-5)}{(1)(-2)}$$

$$= 4\frac{(x-2)(x-5)}{-2}$$

$$=4 \cdot \mathrm{inv}(-2,19) \cdot (x-2)(x-5)$$

$$= 4 \cdot \mathrm{inv}(17,19) \cdot (x-2)(x-5)$$

$$= 4 \cdot 9 \cdot (x-2)(x-5)$$

$$= 36\ (x-2)(x-5)$$

$$6\frac{(x-2)(x-5)}{(5-2)(5-3)} = 6\frac{(x-2)(x-3)}{(3)(2)}$$

$$= 6\frac{(x-2)(x-3)}{6}$$

$$= 6 \cdot \mathrm{inv}(6,19) \cdot (x-2)(x-3)$$

$$= 6 \cdot 16 \cdot (x-2)(x-3)$$

$$=96\left(x-2\right)\left(x-3\right)$$

所以：

$$q(x)=\left[65\left(x-3\right)\left(x-5\right)+36\left(x-2\right)\left(x-5\right)+96\left(x-2\right)\left(x-3\right)\right]\bmod 19$$

$$=\left[8\left(x-3\right)\left(x-5\right)+17\left(x-2\right)\left(x-5\right)+\left(x-2\right)\left(x-3\right)\right]\bmod 19$$

$$=\left(26x^2-188x+296\right)\bmod 19$$

$$=7x^2+2x+11$$

因此，只要知道$D_2=5$，$D_3=4$和$D_5=6$，就可以求出：

$$D=q\left(0\right)=11$$

如果尝试任意其他3个D_j值，也可以得到同样的结果。

请编写程序实现Shamir$\left(k,n\right)$ 门限方案，其中k和n是任意满足$k\le n$的正整数。

题目2：

1980年，Asmuth和Bloom提出了一种基于中国剩余定理的$\left(k,n\right)$门限方案。这里，各小块D_i与一个和D相关的数D'同余。在他们的方案中，令$\left\{p,d_1,d_2,\cdots,d_n\right\}$为一组满足下述条件的整数：

(1) $p>D$;

(2) $d_1<d_2<\cdots<d_n$;

(3) $\gcd(p,d_i)=1,1\leqslant i\leqslant n$;

(4) $\gcd(d_i,d_j)=1,i\neq j,1\leqslant i,j\leqslant n$;

(5) $d_1d_2\cdots d_k>pd_{n-k+2}d_{n-k+3}\cdots d_n$。

条件(3)和(4)说明，这组整数$\left\{p,d_1,\cdots,d_n\right\}$是两两互素的。条件(5)说明，$k$个最小的$d_i$的乘积大于$p$和$k-1$个最大的$d_i$的乘积。令$m=d_1d_2\cdots d_k$是$k$个最小的

di的乘积，则m/p大于任何$k-1$个di的乘积。在$[0,(m/p)-1]$的范围内随机地选取一个r，计算出$D'=D+rp$。由r的选取方法和条件(1)可知，D'一定在$[0,m-1]$的范围之内。最后，如下计算出n个D_i块：

$$D_i = D' \bmod d_i, 1 \leqslant i \leqslant n$$

只要知道上述D_i块中的任意k个，例如$D_{i_1},\cdots,D_{i_k}$，就可以应用中国剩余定理求出D'：

$$y \equiv D' \left(\bmod m_1 \right)$$

其中$m_1 = d_{i_1} d_{i_2} \cdots d_{i_k}$。因为$m_1 \geqslant m$，所以上述$D'$是唯一地确定的。

求出D'后，就不难算出：

$$D = D' - rp$$

相反，如果仅仅知道$k-1$块D_i，即知道$D_{i_1},\cdots,D_{i_{k-1}}$，则只能应用中国剩余定理求出满足下列同余式：

$$y \equiv D_{i_j} \left(\bmod d_{i_j} \right),\ 1 \leqslant j \leqslant k-1$$

的

$$y \equiv D'' \left(\bmod m_2 \right)$$

其中$m_2 = d_{i_1} \cdots d_{i_{k-1}}$。因为$m/m_2 > p$，且有$\gcd\left(m_2, p\right)=1$，所以在$[0,m]$中与$D''$模$m_2$同余的数在所有模$p$的同余类中均匀地分布，即没有足够的信息能够确定出$D'$。

下面用一个具体的例子说明上述同余类(k,n)门限方案。

令 $k=2, n=3, D=4, p=7, d_1=9, d_2=11, d_3=13$。因为，$m=d_1 d_2 = 9\cdot 11 = 99 > 91 = 7\cdot 13 = p\cdot d_3$，所以满足同余类方案的要求。可以在$[0,99/7-1]=[0,13]$中随机地选取一个$r=10$，因此：

$$D' = D + rp = 4 + 10\cdot 7 = 74$$

分别计算出：

$$D_1 = 74 \bmod 9 = 2$$
$$D_2 = 74 \bmod 11 = 8$$
$$D_3 = 74 \bmod 13 = 9$$

由上述计算可知：

$$y \equiv D' \left(\bmod 9 \cdot 11 \cdot 13\right)$$

是联立同余式：

$$\begin{cases} y \equiv 2\left(\bmod 9\right) \\ y \equiv 8\left(\bmod 11\right) \\ y \equiv 9\left(\bmod 13\right) \end{cases}$$

的解，其中 $D' = 74$ 。

如果知道上面的 D_j 中的任意两个，就可以计算出 D 。假如，已知 $D_1 = 2和D_2 = 8$，则有：

$$m_1 = d_1 d_2 = 9 \cdot 11 = 99$$

为了应用中国剩余定理，首先求出：

$$y_1 = \mathrm{inv}\left(m_1/d_1, d_1\right) = \mathrm{inv}\left(11, 9\right) = 5$$

$$y_2 = \mathrm{inv}\left(m_1/d_2, d_2\right) = \mathrm{inv}\left(9, 11\right) = 5$$

其中 $\mathrm{inv}\left(a, b\right) = c$ 表示 $a \cdot c \equiv 1\left(\bmod b\right)$。因此：

$$\begin{aligned} D' &= \left[\left(\frac{m_1}{d_1}\right) y_1 D_1 + \left(\frac{m_2}{d_2}\right) y_2 D_2\right] \bmod m_1 \\ &= \left[11 \cdot 5 \cdot 2 + 9 \cdot 5 \cdot 8\right] \bmod 99 \\ &= \left[110 + 360\right] \bmod 99 \\ &= 470 \bmod 99 \\ &= 74 \end{aligned}$$

最后，计算出：

$$D = D' - rp = 74 - 10 \cdot 7 = 4$$

请编写程序实现上述基于中国剩余定理的$\left(k, n\right)$门限方案，其中k和n是任意满足$k \leq n$的正整数。

题目3：

隐蔽性是木马等恶意软件的基本特性之一，是指木马必须有能力长期潜伏于目标机器中而不被发现，其采用的技术包括：

1）设置窗口不可见，即从任务栏中隐藏；

2）把木马程序注册为服务，即从进程列表中隐藏；

3）欺骗查看进程的函数，即从进程列表中隐藏；

4）替换系统驱动或系统DLL，一种真隐藏技术；

5）动态嵌入技术，一种真隐藏技术。

请编写程序模拟木马的自我隐藏功能，要求程序在运行过程中，从任务栏、任务管理器的进程列表中查看不到程序运行的痕迹。