要求生成一个三百位的大数k当作秘密，若门限参数为(n,t)表示分成n份，只有大于等于t个人到场时才能解除秘密。

生成一组数d_i，$i\in[0,n]$，且$d_i<d_j$恒成立对于所有的$i<j$。即数列d严格单调递减。

我们有秘密k要小于任意t个数列d中项的乘积，要大于任意$t-1$个数列d中项的乘积，这样才保证大于t个人的时候能够解秘密而小于t的时候解不出来。

重点就是生成这个数列d。

为了简化问题，可以考虑一个$relaxed\ model$，使得$k^{\frac{1}{2}}>d_5>d_4>d_3>d_2>d_1>k^{\frac{1}{3}}$，则必定有$d_1d_2d_3>k,\ d_4d_5<k$

思路：创建一个有七个元素的数组，设为$d[0]\to d[6]$，令$d[0]=k^{\frac{1}{3}}$，令$d[6]=k^{\frac{1}{2}}$，用$rand(a,b)$来表示生成$[a,b)$之间的随机数。

伪代码：

```
for i = 1 to 5:
    d[i] = NULL;
end for;

for i = 1 to 5
    while (elements of d excluding d[0],d[],NULL are NOT coprime)
        d[i] = random(d[i-1], k^(1/2))
    end while;
end for
```