**Fortuna伪随机数发生器设计文档**

1. 环境说明：

运行环境：Win10, Java 8（JDK 1.8）

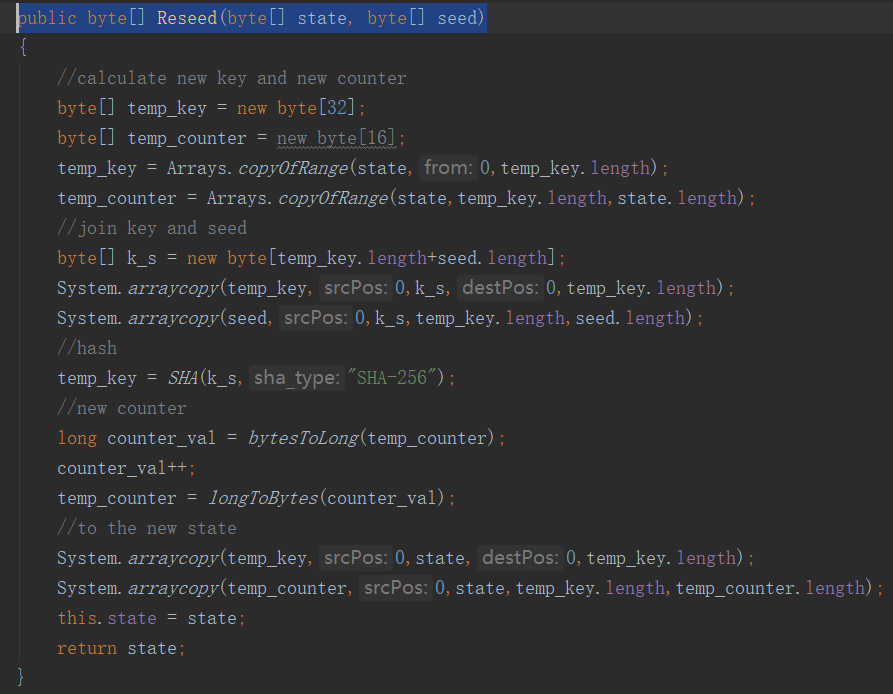
IDE：Intellij Idea 2017

测试环境：Win10

1. 代码说明：
2. 生成器
3. Reseed：

功能：改变随机数发生器状态，重新生成种子

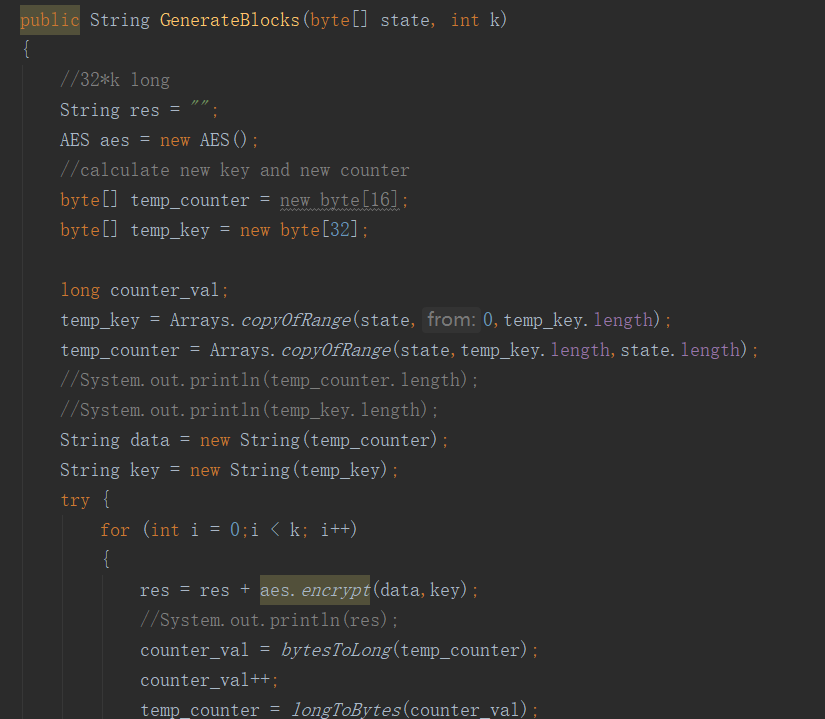
思路：使用字节串存储明文和密钥，对密钥进行哈希，更新密钥的同时更新状态



1. GenerateBlocks

功能：产生k个分组的伪随机数

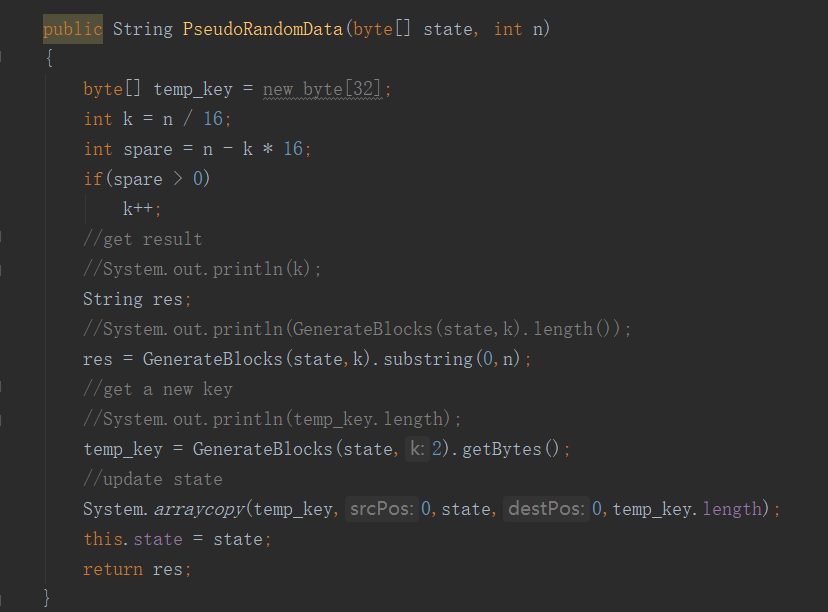
思路：每组为16字节，使用AES循环产生随机数并连接在字符串上



1. PesudoRandomData

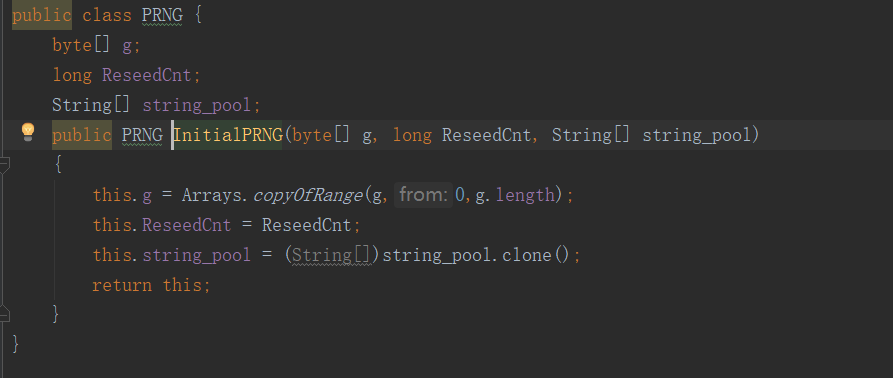
功能：产生n个随机数

思路：计算m个随机数，从m中取n个，并且计算新密钥更新发生器状态



1. PRNG

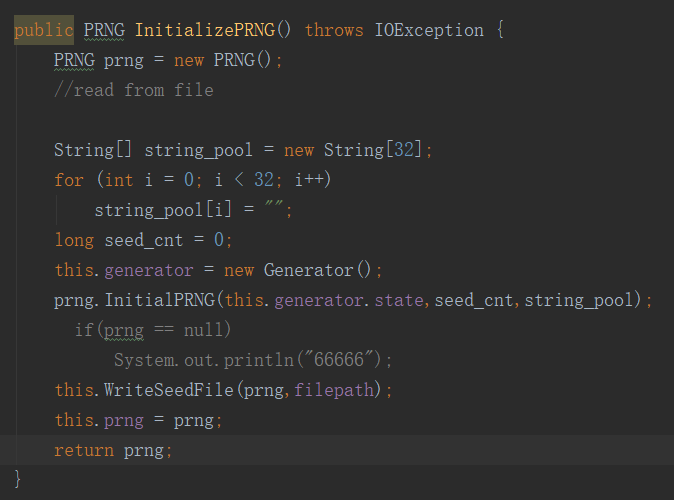
说明：PRNG包含随机数发生器的状态g，重新生成种子的次数Cnt，以及熵源池string\_pool



1. 累加器
2. InitializePRNG

功能：初始化PRNG，清空熵源池，重新产生种子的计数器清零并且初始化发生器

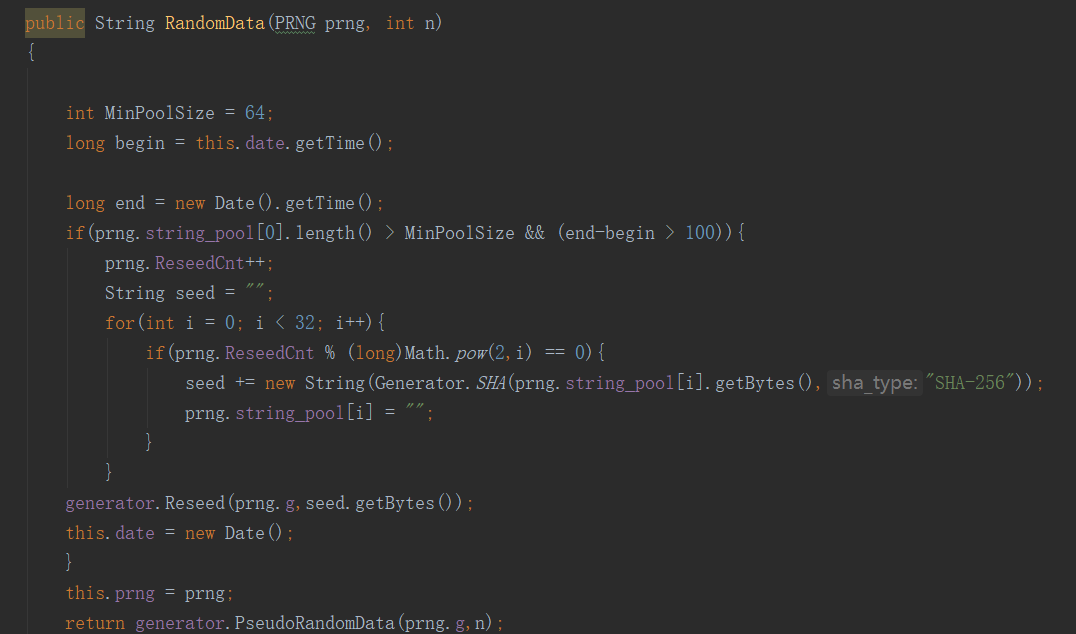
思路：初始化之后将状态保存在种子文件中



1. RandomData

功能：重新产生种子，并产生n长度的伪随机数

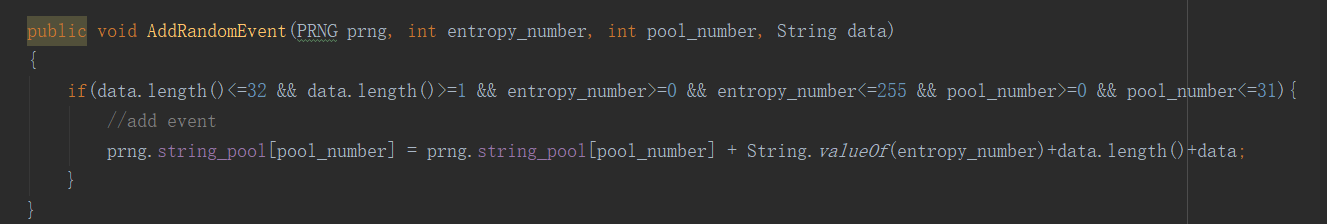
思路：使用全局的Date类记录时间变化，超过100ms并且第一个熵源池大于64字节后取数据重新产生种子



1. AddRandomEvent

功能：添加随机事件

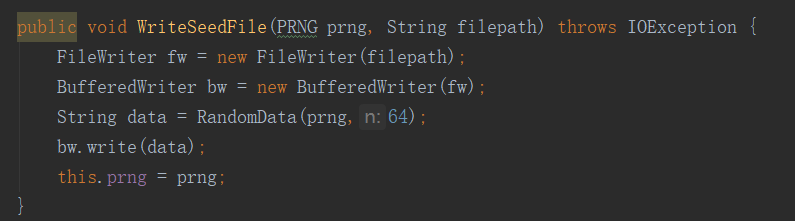
思路：略



1. WriteSeedFile

功能：将PRNG状态写入种子文件

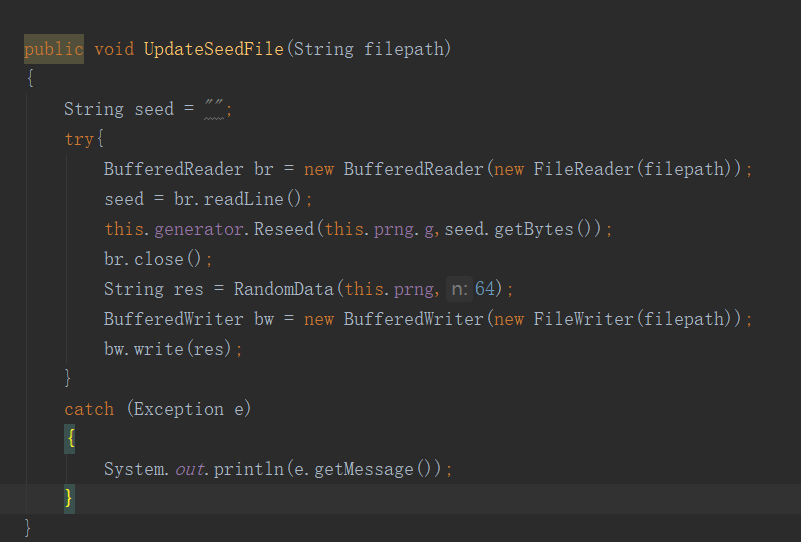
思路：简单文件操作



1. UpdateSeedFile

功能：更新种子文件

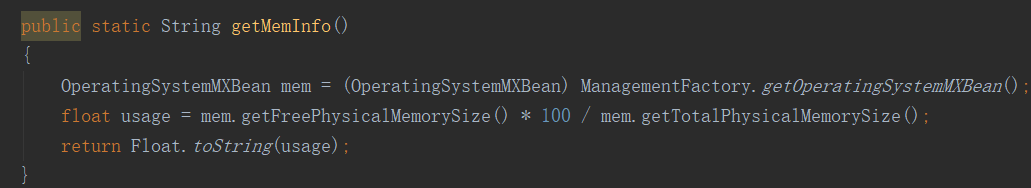
思路：读取保存的种子文件，用以产生新的种子，之后再将新产生的随机数写入种子文件



d. 熵源类EntropySupply

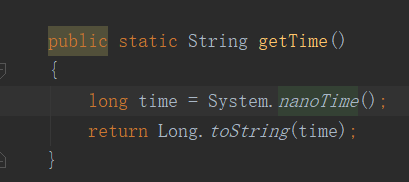
1.getMemInfo

功能：获取内存使用率



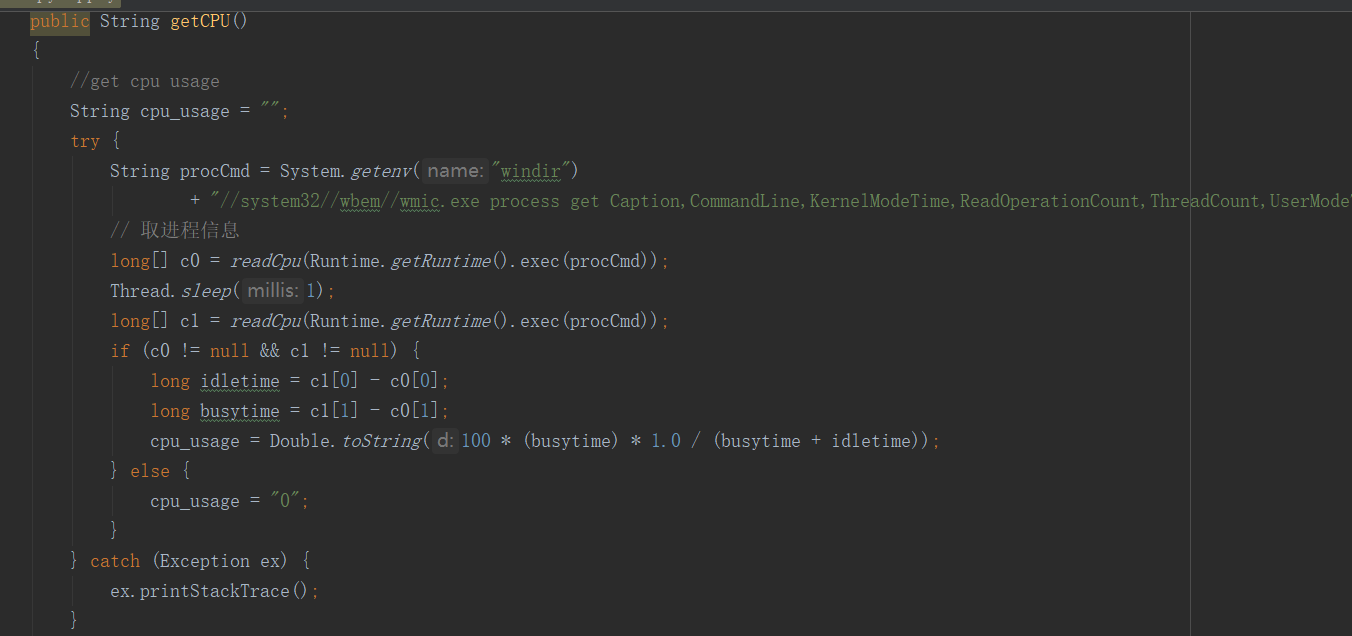
2. getTime

功能：获取时间



3. getCPU

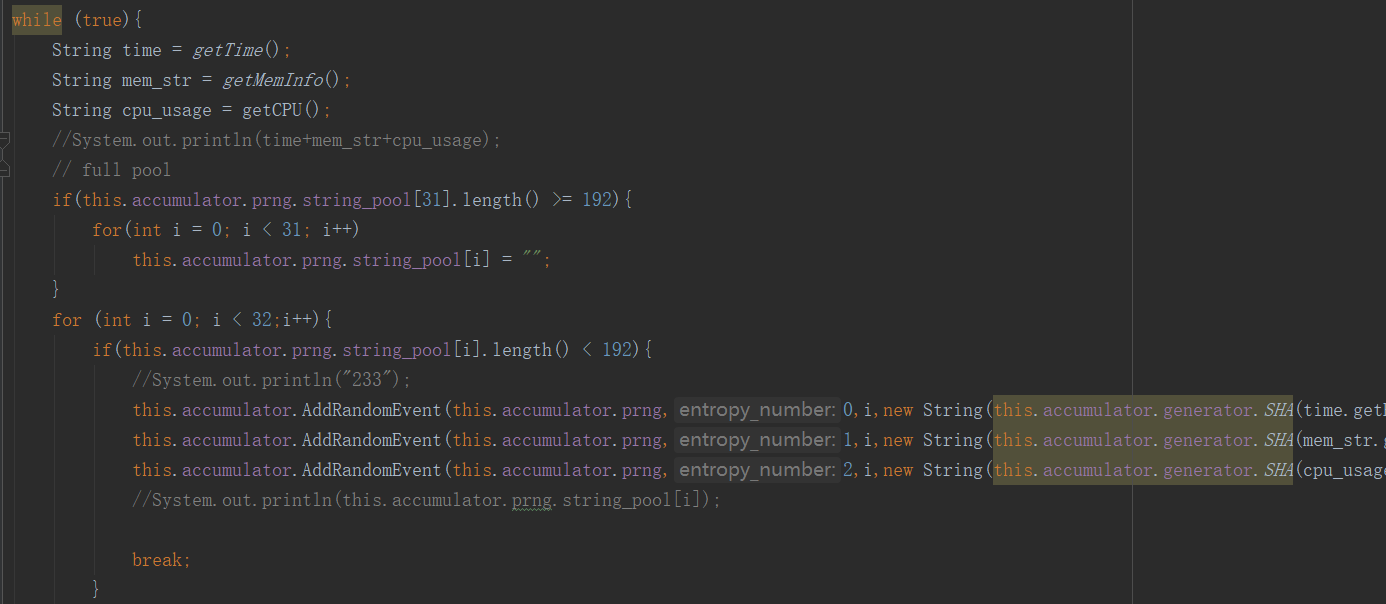
功能：获取CPU使用率



4. run

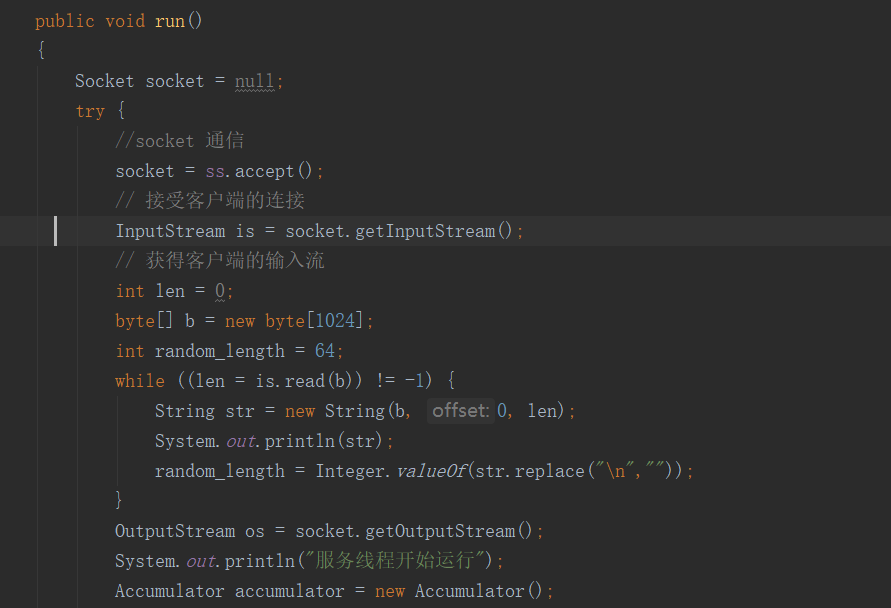
功能：线程类的核心代码，负责定时加入熵源池熵源，更新PRNG状态等

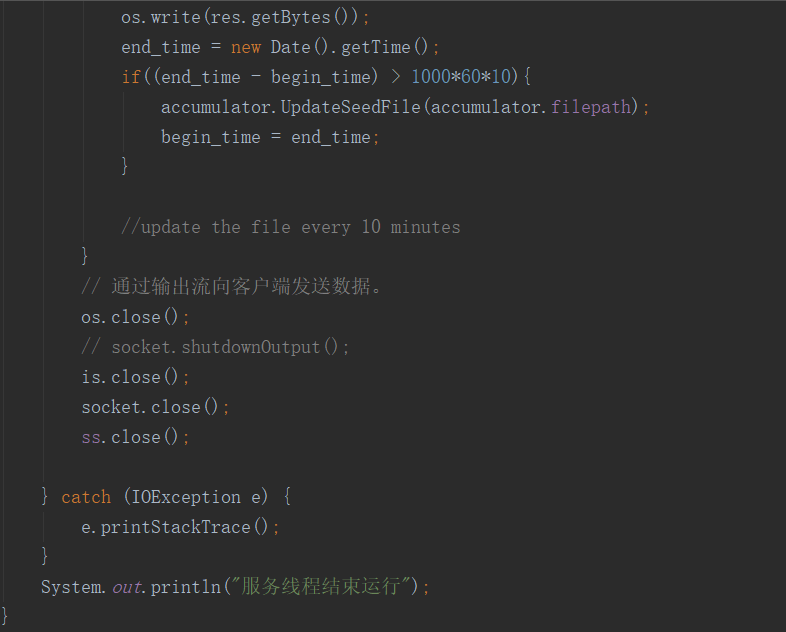
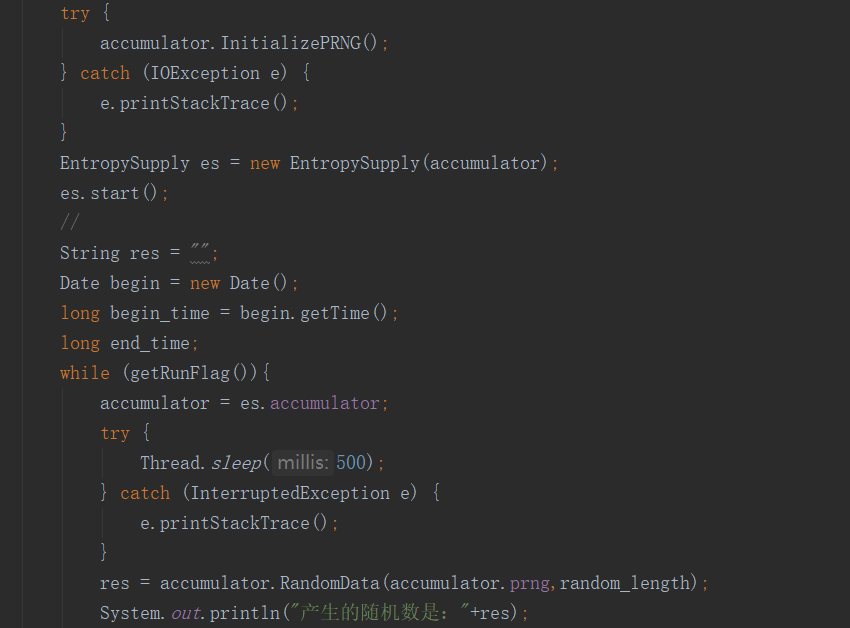
思路：调用AddRandomEvent，依次填充熵源的hash值，填满一个池子之后就会紧接着换下个池子，满之后清空



e. Service服务类

功能：建立TCP通信，绑定端口并监听客户端连接，之后根据客户端要求的长度生成随机数





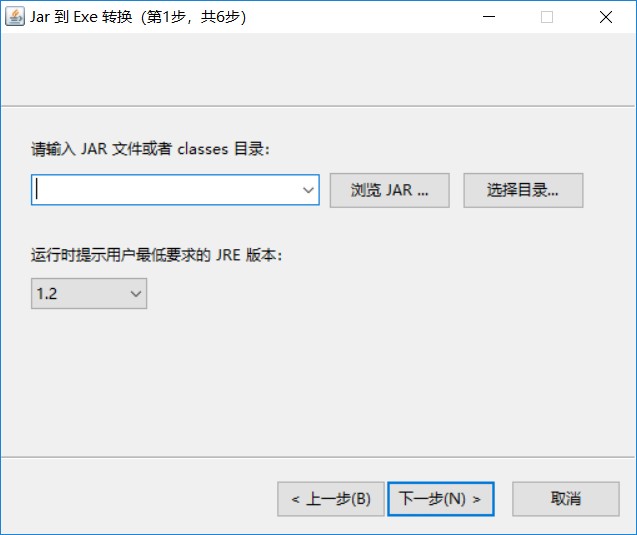
f. FortunaClient客户端

功能：与Fortuna服务建立连接获取数据



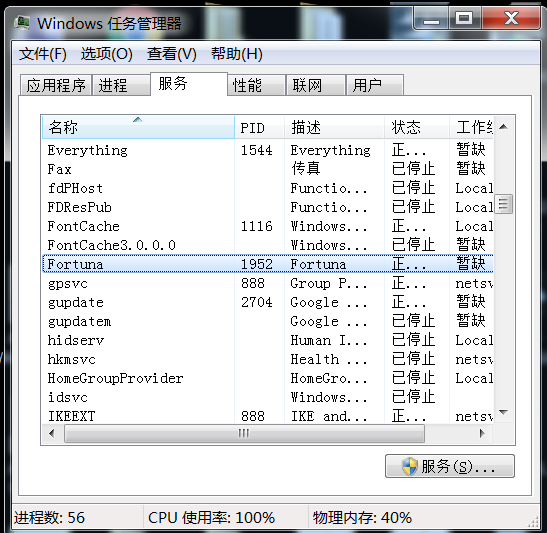
三、 测试说明

1. 将Fortuna和FortunaClient打包成jar包，之后使用工具将Fortuna.jar转换成服务型程序Fortuna.exe



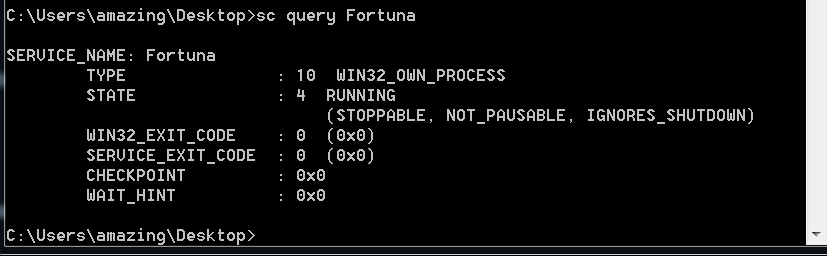
2. 在虚拟机中注册服务





3. 启动服务





4. 使用Client客户端测试

