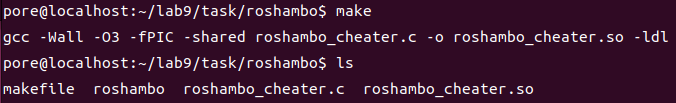
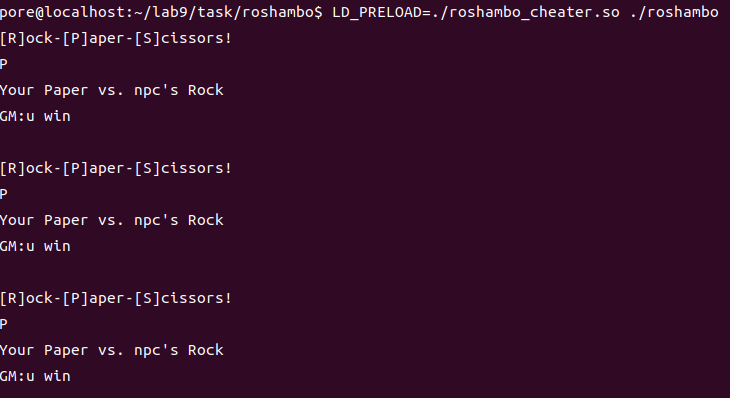
**任务一**

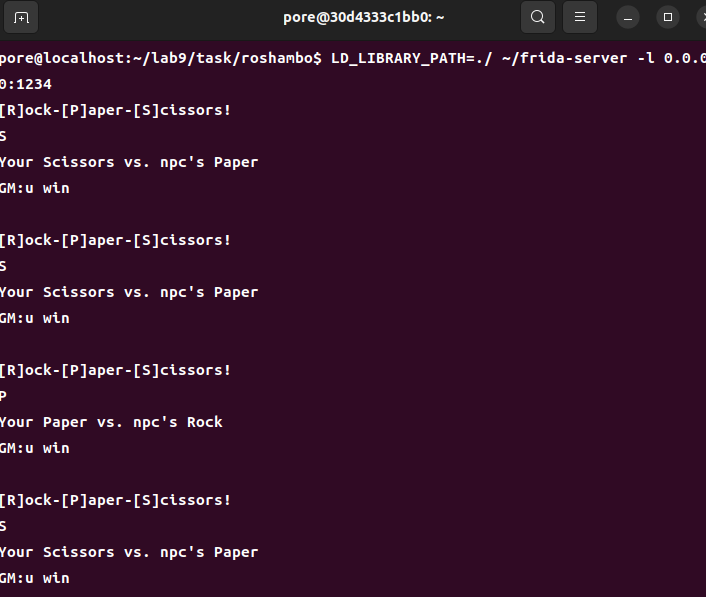
****

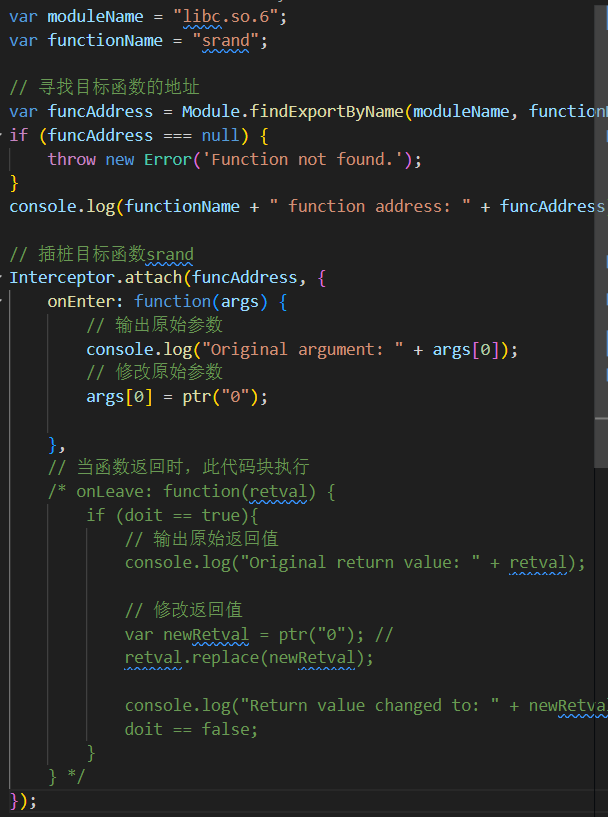
Rand()函数主要用于生成伪随机数，在使用rand()函数之前，通常通过srand()函数来设置随机数生成器的种子值。



将原始的rand函数换成带有辅助功能的函数，让函数直接返回零，那么对方出的一致都是拳头，玩家只要出布就能获胜。

**任务二**

****

****

Srand函数不需要返回值，所以不考虑返回的情况

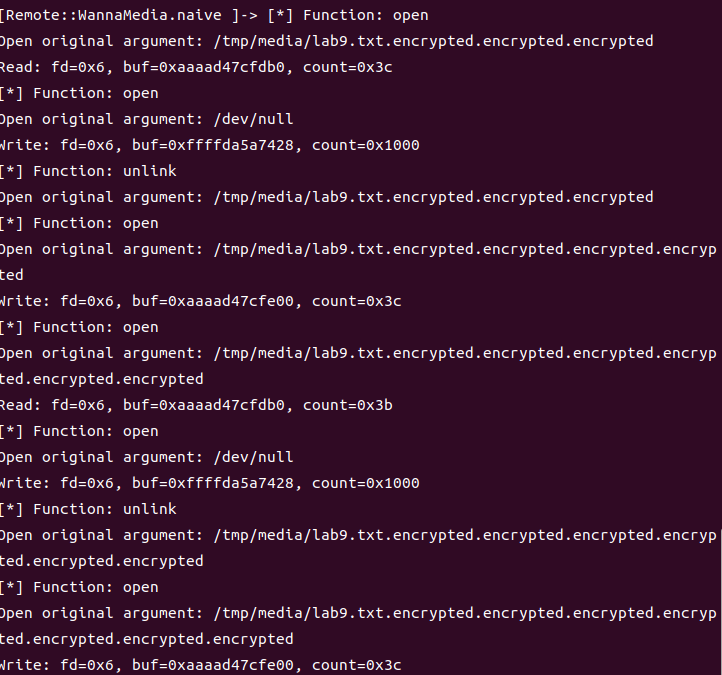
srand的参数实际上是一个种子(seed)，相当于告诉计算机从哪里开始生成随机数序列。如果使用相同的种子，那么每次程序运行时生成的随机数序列都会是相同的。直接指定固定的参数0，使得对手的出法每一轮游戏都会相同。在这个参属下，对手固定出PPRPSPP……玩家只需要依次出SSPSRSS……就能取胜。

**任务三**

因为open、unlink操作需要将参数转换为字符串并输出的功能，所以在一起处理。Write和read单独处理。



脚本输出得到的结果如图：



第一个文件交互阶段：

打开文件 /tmp/media/lab9.txt.encrypted.encrypted.encrypted 并进行读取操作，读取了 0x3c 字节的数据。

第二个文件交互阶段：

打开 /dev/null 这个特殊的设备文件，并向其写入了 0x1000 字节的数据。

第三个文件交互阶段：

使用 unlink 操作删除文件 /tmp/media/lab9.txt.encrypted.encrypted.encrypted。

第四个文件交互阶段：

打开了文件 /tmp/media/lab9.txt.encrypted.encrypted.encrypted.encrypted，并向该文件写入了 0x3c 字节的数据。

……

Wannamedia使用了多个嵌套的加密后缀命名文件来读取，并且多次重复写入数据，可能是为了混淆。

使用 /dev/null 这个特殊的设备文件进行写入操作，这可能是为了隐藏数据。

使用unlink删除文件，可能是为了隐藏操作痕迹。