第2次软件保护作业

(1) 用汇编写shell.asm;
其中shell.asm的功能是:
①对载入内存的原exe进行解密;
②对原exe进行重定位;
③跳转到原exe的main入口执行;
当shell.asm编译成shell.exe后，为了便于lock引用shell的内容，我们可以把shell.exe 中除文件头外的全部内容保存为shell.bin。
(2) 用C写lock.c;
其中lock.c支持以下命令行方式运行把hello.exe加密成hello2.exe:
lock hello.exe hello2.exe
hello.exe样本下载链接:hello.zip
lock.c的功能是:
①复制hello.exe到hello2.exe;
②读取hello2.exe的文件头添加到shell.bin后面生成shelldat.bin,
③把shelldat.bin添加到hello2.exe末尾;
④对hello2.exe中除了文件头外的全部内容进行加密(使用逐字节xor 33h);
⑤修改hello2.exe文件头+6处的重定位项=0;
⑥修改hello2.exe文件头+2及+4处的文件长度信息;
⑦修改hello2.exe的Δcs:ip;
shell.asm, shell.exe, shell.bin, lock.c,

lock.exe及相关VC6工程文件请全部保存到"学号姓名"文件夹内，再把该文件夹压缩成"学号姓名.zip"，上传到以下ftp:
ftp://bhhreverse:bhhreverse@10.71.45.100/作业02