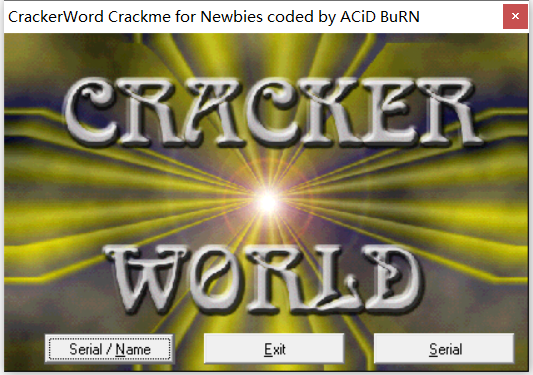
# 逆向分析技术

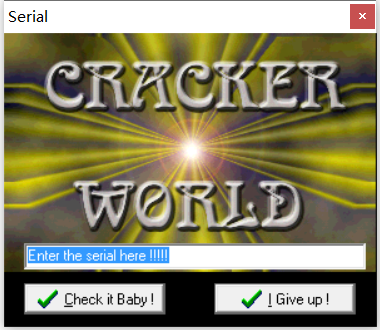
## 实验二程序爆破

实验步骤：

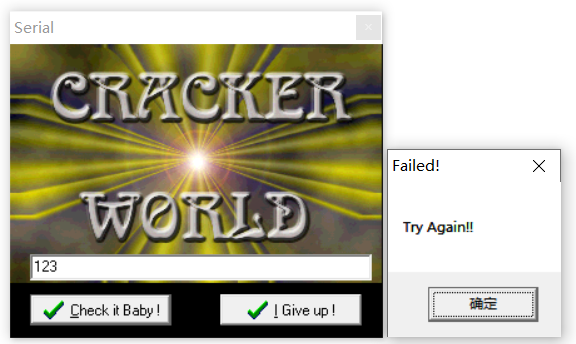
下载并解压缩EXP2.rar。运行EXP2.exe：



点击右边的Serial按钮：



正常情况下，输入一个错误序列号后，点击”Check it Baby!”按钮，会弹出报错信息：

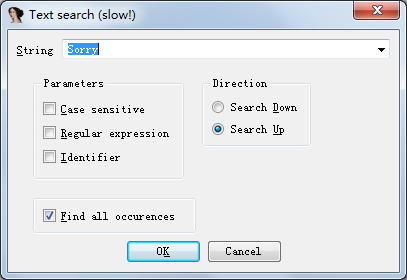


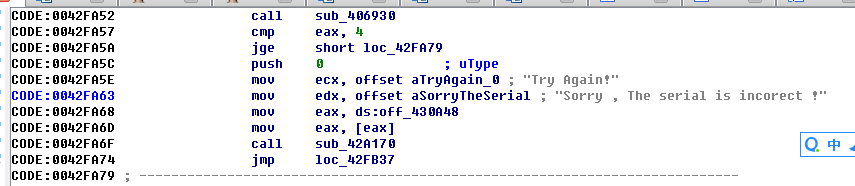
请各位同学利用OllyDbg，参照课程中的爆破示例对该程序中的Serial功能进行爆破，并用爆破后的程序覆盖原程序。爆破成功后，输入任何序列号都会弹出成功信息。提示：1）示例中是如何进行爆破的；2）弹出信息的字符串。

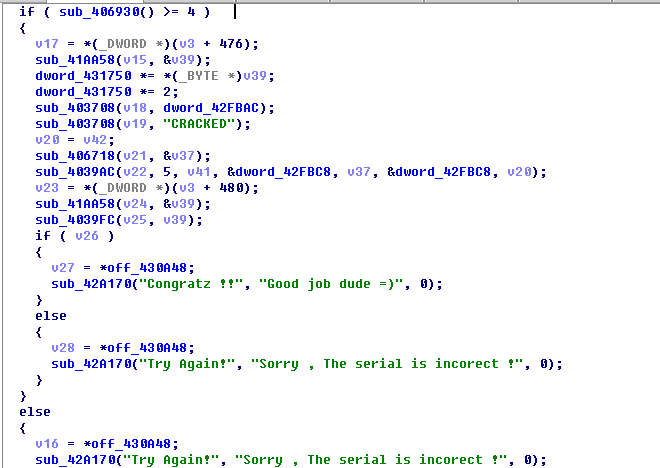
请各位同学通过QQ作业于3月29日前在线提交如下内容：

描述用OllyDbg对EXP2进行爆破的过程（文字+截图）。其中，如何定位到需要爆破的指令，指令的爆破，覆盖原程序以及爆破成功后的运行情况等步骤必须有。

**注意：请不要上传文件，直接在QQ作业中填写。**

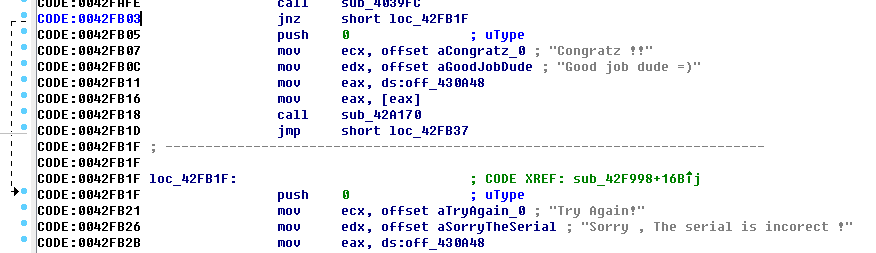
1. **用IDA打开exe文件。ALT+T打开搜索窗口，搜索关键字Sorry**

**2. 得到Sorry , The serial is incorect ! 出现的汇编代码段和地址**

1. **F5反汇编**
2. 看出程序的逻辑是if(v26)，则输出Congratz !!", "Good job dude =。

否则提示错误。

1. 定位汇编代码中的if跳转语句，在0042FB03位置



1. 用NOP填充0042FB03位置的指令，则爆破成功。

OD：ctrl+g 跳转代码