Writeup

1. 检查题目字符串可以发现是Go语言编译的程序，使用IDAGolangHelper可以恢复符号。
2. 从main_main函数入手，结合题目名称、给出的图片等可以发现是一个图片隐写程序，程序解析命令行参数的-i -o 和 -f三个参数，将-f参数中的文件读取后隐写到-i的文件中，保存到-o的输出图片。
3. 整理程序逻辑，首先将隐写文件做16长度的padding，然后送到一个分组加密，分组长度是16，最后对密文做一些调整后插入到图片的lsb中。
4. 首先逆向加密算法，通过搜索加密算法中的常数0x7369f885192c0ef5可以发现是simon加密算法，由于simon加密算法的加密流程比较简单，也可以手动进行还原恢复。
5. 输入文件被加密后，会以随机的顺序被插入到图片一些位置的lsb中（可以在stegsolve的alpha0图层中观察到），逆向发现随机使用了rand.Perm函数，而随机种子与输入图片的像素个数有关，因此随机顺序是固定的，可以通过调试得到。
6. 提取图片的lsb后将解密算法与随机序列结合，解密脚本见dec.go，使用-i steg.png -f flag.7z解密得到一个7z压缩包，打开即可得到flag：