Chapter 2

流密码

Exercise 3

编程实现流加密算法，其密钥由 32 位 LFSR 生成。32 阶的本源多项式有很多个，为了便于对程序进行测试、验收，本练习要求使用本源多项式：

$$x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$$

并且使用 Fibonacci 配置的方式实现密钥流的生成。

算法对一个文本文件进行加密，加密后的信息存在二进制文件中，也可对加密后的二进制文件进行解密，解密后的明文存在以文本方式存入文件，执行命令时，用户可以指定涉及到的文件名。文件 seed 是存储种子值的二进制文件。**此练习不需要写报告**。

例如:

加密执行的命令: streamcipher -e 1.txt seed c1

解密执行的命令: streamcipher -d c1 seed 2.txt

项目参考初始仓库`https://gitee.com/buuer/streamcipher`。

文件 seed 是一个二进制文件，存的是种子值，初始仓库给的种子值为 AAAAAAAA。

提交的仓库中，要将文件 plain_buu_intr.docx 进行加密，密文以二进制方式存储在 cipher.docx 中，同时将 cipher.docx[1]进行解密，解密后存为文件 decode.docx[2]。

说明

- 密钥是什么？本原多项是什么 (抽头序列是什么？Fibonacci 配置是什么？)，可以查阅相关材料。
- 由于 docx 文件是一个结构性文档，也就是说是一个二进制文档，需要 Word 应用程序来解释的，所以当你加密是出现错误很难调整。建议在编写程序调试时，可以使用一个纯文本文档来

[1]此时文件已经不能被 Word 应用程序正常打卡。

[2]此时文件可以被 Word 应用程序正常打卡。

调试，并且在调试过程中可以构造你需要的原文内容。